aws

Guida per l'utente

AWSStorage Gateway

Versione API 2013-06-30

AWSStorage Gateway: Guida per l'utente

Table of Contents

Che cos'è Amazon S3 File Gateway

AWSStorage Gateway collega un'appliance software locale allo storage basato sul cloud per fornire un'integrazione perfetta con caratteristiche per la sicurezza dei dati tra l'ambiente IT locale eAWSinfrastruttura di storage. È possibile utilizzare il servizio per memorizzare i dati nelAWSUn cloud per uno storage scalabile e a costi contenuti che contribuisce a mantenere la sicurezza dei dati.AWS Storage Gateway offre soluzioni di storage basato su file, su volumi e su nastro.

Argomenti

Gateway di file Amazon S3

Gateway di file Amazon S3—Amazon S3 File Gateway supporta un'interfaccia file inAmazon Simple Storage Service (Amazon S3)e unisce un servizio e un'appliance software virtuale. Tramite questa combinazione, è possibile archiviare e recuperare oggetti in Amazon S3 utilizzando i protocolli di file standard di settore, ad esempio NFS (Network File System) e SMB (Server Message Block). L'appliance software, o gateway, viene distribuita nell'ambiente locale come macchina virtuale (VM) in esecuzione su hypervisor VMware ESXi, Microsoft Hyper-V o KMV Linux.. Il gateway permette l'accesso a oggetti in S3 come file o punti di montaggio di condivisione file. Con un gateway di file S3, è possibile effettuare le seguenti operazioni:

- Archiviare e recuperare i file direttamente tramite il protocollo NFS versione 3 o 4.1.
- Archiviare e recuperare i file direttamente tramite il protocollo file system SMB versione 2 e 3.
- Accedere ai dati direttamente in Amazon S3 da qualsiasiAWSApplicazione o servizio cloud.
- Gestire i dati S3 tramite policy del ciclo di vita, replica in più regioni e funzione Versioni multiple. Un gateway di file S3 può essere considerato come il montaggio di un file system su Amazon S3.

Un gateway di file S3 semplifica lo storage dei file in Amazon S3, si integra con le applicazioni esistenti tramite i protocolli di file system standard di settore e fornisce un'alternativa conveniente allo storage locale. Fornisce inoltre accesso a bassa latenza ai dati tramite caching locale trasparente. Un File Gateway S3 gestisce il trasferimento di dati da e versoAWS, effettua il buffer delle applicazioni da congestioni di rete, ottimizza i dati e ne esegue lo streaming in parallelo e gestisce il consumo della larghezza di banda. S3 File Gateway si integra conAWSservizi, ad esempio con quanto segue:

- Gestione comune degli accessi tramite AWS Identity and Access Management (IAM)
- Crittografia tramite AWS Key Management Service (AWS KMS)
- Monitoraggio con Amazon CloudWatch (CloudWatch)
- Controllo tramiteAWS CloudTrail(CloudTrail)
- Operazioni tramite AWS Management Console e AWS Command Line Interface (AWS CLI)
- Gestione di costi e fatturazione

Nella documentazione seguente, troverai la sezione Nozioni di base che contiene le informazioni di configurazione comuni a tutti i gateway, nonché sezioni sulla configurazione specifica per gateway. La sezione Nozioni di base illustra come distribuire, attivare e configurare lo storage per un gateway. La sezione sulla gestione illustra come gestire il gateway e le risorse:

- fornisce istruzioni su come creare e utilizzare un gateway di file S3. Mostra come creare una condivisione file, mappare l'unità a un bucket Amazon S3 e caricare file e cartelle su Amazon S3.

- descrive come eseguire le attività di gestione per tutti i tipi di gateway e le risorse.

In questa guida, scoprirai principalmente come utilizzare le operazioni dei gateway tramite la AWS Management Console. Se desideri eseguire queste operazioni in modo programmatico, consultaAWSRiferimento dell'API Storage Gateway.

Come funziona Storage Gateway (architettura)

Di seguito, è fornita una panoramica dell'architettura delle soluzioni Storage Gateway disponibili.

Argomenti

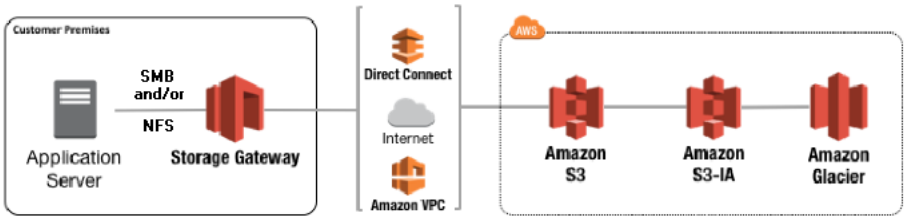
Amazon S3 per i file gateway

Per usare un gateway di file S3, puoi iniziare scaricando un'immagine VM per il gateway. Quindi si attiva il gateway dalAWS Management Consoleo tramite l'API Storage Gateway. Puoi anche creare un gateway di file S3 tramite un'immagine Amazon EC2.

Dopo l'attivazione del gateway di file S3, è necessario creare e configurare la condivisione di file e associare tale condivisione al bucket Simple Storage Service (Amazon S3). In questo modo la condivisione è accessibile dai client che utilizzano il protocollo NFS (Network File System) o SMB (Server Message Block). I file scritti su una condivisione di file diventano oggetti in Amazon S3, con il percorso come chiave. Esiste una mappatura one-to-one tra i file e gli oggetti e il gateway aggiorna gli oggetti in Amazon S3 in modo asincrono man mano che i file vengono modificati. Gli oggetti esistenti nel bucket Amazon S3 vengono visualizzati come file nel file system e la chiave diventa il percorso. Gli oggetti vengono crittografati con chiavi crittografia lato server Amazon S3 (SSE-S3). Tutti i trasferimenti di dati vengono eseguiti tramite HTTPS.

Il servizio ottimizza il trasferimento dei dati tra il gateway eAWSutilizzo di caricamenti paralleli in più parti o download con intervallo di byte per utilizzare meglio la larghezza di banda disponibile. La cache locale viene mantenuta per fornire accesso a bassa latenza ai dati usati di recente e ridurre i costi dell'uscita dei dati. I parametri CloudWatch forniscono informazioni sull'utilizzo delle risorse sulla VM e sul trasferimento dei dati da e versoAWS. CloudTrail monitora tutte le chiamate API.

Con lo storage del gateway di file S3, puoi eseguire attività come l'inserimento di carichi di lavoro cloud in Amazon S3, il backup e l'archiviazione, il tiering e la migrazione dei dati di storage nelAWSNuvola. Il diagramma seguente fornisce una panoramica della distribuzione dello storage di file per Storage Gateway.



S3 File Gateway converte i file in oggetti S3 durante il caricamento di file su Amazon S3. L'interazione tra le operazioni dei file eseguite con le condivisioni di file su oggetti S3 File Gateway e S3 richiede che determinate operazioni siano attentamente considerate durante la conversione tra file e oggetti.

Le operazioni comuni sui file modificano i metadati dei file, il che comporta l'eliminazione dell'oggetto S3 corrente e la creazione di un nuovo oggetto S3. Nella tabella seguente vengono illustrate le operazioni di esempio sui file e l'impatto sugli oggetti S3.

Operazione file	Impatto oggetto S3	Implicazione della classe di storage
Rinomina file	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file	Potrebbero essere applicate commissioni di cancellazione anticipata e costi di recupero
Rinomina cartella	Sostituisce tutti gli oggetti S3 esistenti e crea nuovi oggetti S3 per ogni cartella e file nella struttura delle cartelle	Potrebbero essere applicate commissioni di cancellazione anticipata e costi di recupero
Modifica delle autorizzazioni per file/cartella	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file o cartella	Potrebbero essere applicate commissioni di cancellazione anticipata e costi di recupero
Modificare la proprietà di file/cartelle	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file o cartella	Potrebbero essere applicate commissioni di cancellazione anticipata e costi di recupero

Operazione file	Impatto oggetto S3	Implicazione della classe di storage
Aggiungi a un file	Sostituisce l'oggetto S3 esistente e crea un nuovo oggetto S3 per ogni file	Potrebbero essere applicate commissioni di cancellazione anticipata e costi di recupero

Quando un file viene scritto su S3 File Gateway da un client NFS o SMB, il gateway di file carica i dati del file su Amazon S3 seguito dai relativi metadati (proprietà, timestamp, ecc.). Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto S3. Questo processo crea un'altra versione dell'oggetto, risultando in due versioni di un oggetto. Se il Versioni multiple di S3 è abilitata, entrambe le versioni verranno memorizzate.

Quando un file viene modificato nel Gateway file S3 da un client NFS o SMB dopo che è stato caricato su Amazon S3, S3 File Gateway carica i dati nuovi o modificati invece di caricare l'intero file. La modifica del file comporta la creazione di una nuova versione dell'oggetto S3.

Quando S3 File Gateway carica file di dimensioni maggiori, potrebbe essere necessario caricare pezzi di file più piccoli prima che il client abbia terminato la scrittura su S3 File Gateway. Alcuni motivi di ciò includono la liberazione di spazio nella cache o un elevato tasso di scrittura su una condivisione di file. Ciò può causare più versioni di un oggetto nel bucket S3.

È necessario monitorare il bucket S3 per determinare quante versioni di un oggetto esistono prima di impostare i criteri del ciclo di vita per spostare gli oggetti in classi di storage diverse. È necessario configurare la scadenza del ciclo di vita per le versioni precedenti per ridurre al minimo il numero di versioni disponibili per un oggetto nel bucket S3. L'uso della replica della stessa regione (SRR) o della replica Cross-Region (CRR) tra i bucket S3 aumenterà lo storage utilizzato.

Configurazione di Amazon S3 File Gateway

Questa sezione fornisce istruzioni per iniziare a usare Amazon S3 File Gateway. Per iniziare, devi prima eseguire la registrazioneAWS. Se utilizzi per la prima volta, ti consigliamo di leggere ilRegionieRequisitisezioni.

Argomenti

Registrazione ad Amazon Web Services

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Come registrarsi a un Account AWS

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

   Come parte della procedura di registrazione riceverai una telefonata, durante la quale dovrai inserire un codice di verifica sulla tastiera del telefono.

Creazione di un utente IAM

Dopo aver creato il tuoAWSaccount, utilizza la procedura seguente per creare unAWS Identity and Access Management(IAM) utente per te stesso. Quindi, aggiungi quell'utente a un gruppo con autorizzazioni amministrative.

Per creare un utente amministratore per se stessi e aggiungere l'utente a un gruppo di amministratori (console)

1. Accedi alla console IAM come proprietario dell'account scegliendo Utente root e inserendo l'indirizzo email di Account AWS. Nella pagina successiva, inserisci la password.

> **Note**
>
> È fortemente consigliato rispettare la best practice sull'utilizzo dell'utente IAM **`Administrator`** e conservare in un luogo sicuro le credenziali dell'utente root. Accedere come utente root solo per eseguire alcune attività di gestione dell'account e del servizio.

2. Nel pannello di navigazione seleziona Utenti, quindi seleziona Aggiungi utente.
3. In User name (Nome utente), inserisci **`Administrator`**.
4. Selezionare la casella di controllo accanto a Accesso alla AWS Management Console. Quindi scegli Custom password (Password personalizzata) e inserisci la nuova password nella casella di testo.
5. (Facoltativo) Per impostazione predefinita, AWS richiede al nuovo utente di creare una nuova password al primo accesso. Puoi deselezionare la casella di controllo accanto a User must create a new password at next sign-in (L'utente deve creare una nuova password al prossimo accesso) per consentire al nuovo utente di reimpostare la propria password dopo aver effettuato l'accesso.
6. Seleziona Successivo: Autorizzazioni.
7. In Set permissions (Imposta autorizzazioni), selezionare Add user to group (Aggiungi l'utente al gruppo).
8. Seleziona Create group (Crea gruppo).
9. Nella finestra di dialogo Create group (Crea gruppo), per Group name (Nome gruppo) inserisci **`Administrators`**.
10. Scegli Filtra policy, quindi seleziona Funzione lavorativa gestita da AWS per filtrare i contenuti della tabella.
11. Nell'elenco delle policy, selezionare la casella di controllo accanto ad AdministratorAccess. Seleziona quindi Create group (Crea gruppo).

> **Note**
>
> È necessario attivare l'accesso dell'utente o del ruolo IAM alla fatturazione prima di poter utilizzare le autorizzazioni `AdministratorAccess` per accedere alla console AWS Billing and Cost Management. A questo scopo, seguire le istruzioni nella fase 1 del tutorial sulla delega dell'accesso alla console di fatturazione.

12. Nell'elenco dei gruppi seleziona la casella di controllo per il tuo nuovo gruppo. Se necessario, selezionare Refresh (Aggiorna) per visualizzare il gruppo nell'elenco.
13. Seleziona Successivo: Tag.
14. (Facoltativo) Aggiungere metadati all'utente collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo di tag in IAM, consultare Tagging di utenti e ruoli IAM nella Guida per l'utente di IAM.
15. Seleziona Successivo: Review (Revisione)per visualizzare l'elenco dei membri del gruppo da aggiungere al nuovo utente. Quando sei pronto per continuare, seleziona Create user (Crea utente).

È possibile utilizzare questa stessa procedura per creare altri gruppi e utenti e per concedere agli utenti l'accesso alle risorse del proprio Account AWS. Per ulteriori informazioni sull'utilizzo delle policy per limitare le autorizzazioni degli utenti a risorse AWS specifiche, consulta Gestione degli accessi ed Esempi di policy.

Configurazione del gateway di file

Salvo diversa indicazione, i seguenti requisiti sono comuni a tutti i tipi di gateway di file inAWS Storage Gateway. La configurazione deve soddisfare i requisiti di questa sezione. Controlla i requisiti applicabili alla configurazione del gateway prima di distribuire il gateway.

Argomenti

Prerequisiti richiesti

Prima di utilizzare un Amazon FSx File Gateway (FSx File Gateway), è necessario soddisfare i seguenti requisiti:

- Creare e configurare un file system FSx for Windows File Server. Per istruzioni, consultaFase 1: Creare il file systemnellaGuida dell'utente di Amazon FSx for Windows File Server.
- Configurare Microsoft Active Directory (AD).
- Assicurarsi che vi sia sufficiente larghezza di banda di rete tra il gateway eAWS. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway.
- Configura la tua rete privata, VPN oAWS Direct Connecttra il tuo Amazon Virtual Private Cloud (Amazon VPC) e l'ambiente locale in cui si distribuisce il gateway file FSx.
- Assicurati che il gateway sia in grado di risolvere il nome del 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 Impostazioni di configurazione di rete nella console locale del gateway.

Requisiti storage e hardware

Le sezioni seguenti forniscono informazioni sull'hardware minimo necessario per il gateway e quantità minima di spazio su disco da allocare per lo storage richiesto.

Per informazioni sulle best practice per le prestazioni del gateway di file, consulta Guida alle prestazioni dei gateway di file.

Requisiti hardware per le macchine virtuali (VM) locali

Quando la distribuzione del gateway avviene in locale, verificare che l'hardware sottostante in cui si distribuisce la macchina virtuale gateway (VM) possa usufruire delle 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 dell'immagine della macchina virtuale e dei dati di sistema.

Per ulteriori informazioni, consultare Ottimizzazione delle prestazioni del gateway. Per ulteriori informazioni su come l'hardware influisce sulle prestazioni della macchina virtuale del gateway, vedere Quote per le condivisioni di file.

Requisiti per i tipi di istanza Amazon EC2

Quando la distribuzione del gateway su Amazon Elastic Compute Cloud (Amazon EC2), le dimensioni dell'istanza devono essere almeno**`xlarge`**per il tuo gateway per funzionare. Tuttavia, per la famiglia di istanze ottimizzate per il calcolo, le dimensioni devono essere almeno**`2xlarge`**. Utilizza uno dei seguenti tipi di istanza consigliati per il tuo tipo di gateway.

Consigliati per tipi di gateway di file

- Famiglia di istanze per uso generale — tipo di istanza m4 o m5.
- Famiglia di istanze ottimizzate per il calcolo — tipi di istanza c4 o c5. Selezionare le dimensioni istanza 2xlarge o superiori per soddisfare i requisiti della RAM.
- Famiglia di istanze ottimizzate per la memoria — tipi di istanza r3.
- Famiglia di istanze ottimizzate per lo storage — tipi di istanza i3.

> **Note**
>
> Quando avvii il gateway in Amazon EC2 e il tipo di istanza scelto supporta una quantità di memoria effimera, i dischi vengono elencati automaticamente. Per ulteriori informazioni sullo storage delle istanze Amazon EC2, consultaStorage delle istnellaGuida per l'utente di Amazon EC2.
> Le scritture delle applicazioni vengono archiviate in modo sincrono nella cache, quindi caricate in modo asincrono nello storage durevole in Amazon S3. Se lo storage temporaneo viene perso perché un'istanza si arresta prima che finisca il caricamento, i dati che ancora risiedono nella cache e non sono ancora stati scritti su Amazon Simple Storage Service (Amazon S3) possono andare perduti. Prima di arrestare l'istanza che ospita il gateway, verifica che il`CachePercentDirty`La metrica CloudWatch è`0`. Per informazioni sullo storage temporaneo, consulta Utilizzo di storage effimero con gateway EC2. Per informazioni sul monitoraggio delle metriche per il gateway di storage, consultaMonitoraggio del gateway file.
> Se disponi di più di 5 milioni di oggetti nel bucket S3 e utilizzi un volume General Purposes SSD, è necessario un volume EBS root minimo di 350 GiB per prestazioni accettabili del gateway durante l'avvio. Per informazioni su come aumentare le dimensioni del volume, consultaModifica di un volume EBS tramite volumi elastici (console).

Requisiti di storage

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

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

> **Note**
>
> È possibile configurare una o più unità locali per la cache, fino alla massima capacità. Quando aggiungi 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 allocati in precedenza come cache.

Per informazioni sulle quote del gateway, consulta Quote per le condivisioni di file.

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 di 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 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 certi casi è possibile distribuire FSx File Gateway su Amazon EC2 o utilizzare altri tipi di distribuzione (inclusa quella locale) con policy di sicurezza di rete che limitanoAWSIntervalli

di indirizzi IP. In questi casi, il gateway potrebbe avere problemi di connettività quandoAWSI valori dell'intervallo IP cambiano. LaAWSI valori di intervallo di indirizzi IP che è necessario utilizzare si trovano nel sottoinsieme del servizio Amazon perAWSNella quale attivi il gateway. Per i valori di intervallo IP correnti, consultaAWSIntervalli di indirizzi IPnellaAWSRiferimenti generali.

Argomenti

- Requisiti porta
- Requisiti di rete e di firewall per l'appliance hardware Storage Gateway
- Consentire ad AWS Storage Gateway l'accesso attraverso firewall e router
- Configurazione dei gruppi di sicurezza per l'istanza del gateway Amazon EC2

Requisiti porta

Storage Gateway richiede determinate porte per essere abilitato a questa operazione. Le seguenti illustrazioni mostrano le porte richieste che è necessario consentire per ogni tipo di gateway. Alcune porte sono richieste da tutti i tipi di gateway, mentre altre sono richieste da determinati tipi di gateway. Per ulteriori informazioni sui requisiti relativi alle porte, consulta Requisiti porta.

Porte comuni per tutti i tipi di gateway

Le seguenti porte sono comuni a tutti i tipi di gateway e sono richieste da tutti i tipi di gateway.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP	443 (HTTPS)	In uscita	Storage Gateway	AWS	Per la comunicazione da Storage Gateway alAWSendpoint del servizio. Per informazioni

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					sugli endpoint del servizio, consulta Consentire ad AWS Storage Gateway l'accesso attraverso firewall e router.

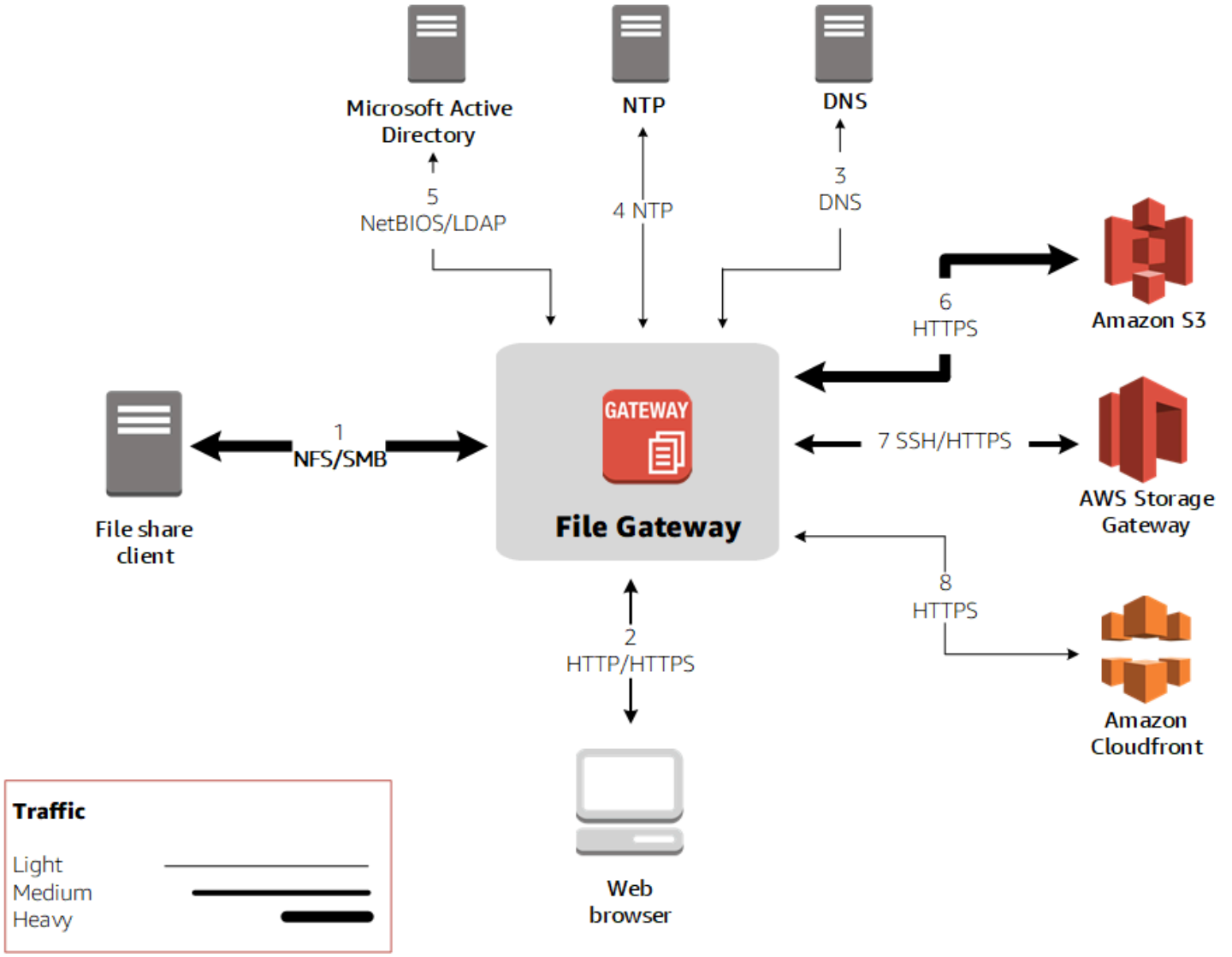
Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP	80 (HTTP)	In entrata	L'host da cui ci si connette alAWS Management Console.	Storage Gateway	Tramite sistemi locali per ottenere la chiave di attivazione del gateway di storage. La porta 80 viene utilizzata solo durante l'attivazione dell'appl iance Storage Gateway. Storage Gateway non richiede l'apertura dell'acce sso pubblico alla porta 80. Il livello di accesso richiesto alla porta 80 dipende dalla configura zione di rete. Se si attiva il gateway dalla console Storage

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					Gateway, l'host da cui ci si collega alla console deve avere accesso alla porta 80 del gateway.
UDP/UDP	53 (DNS)	In uscita	Storage Gateway	Server DNS	Per la comunicazione tra Storage Gateway e il server DNS.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP	22 (Canale di supporto)	In uscita	Storage Gateway	AWS Support	AllowsAWS Supportper accedere 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.
UDP	123 (NTP)	In uscita	Client NTP	Server NTP	Utilizzato dai sistemi locale per sincronizzare l'ora della VM con quella dell'host.

Porte per gateway di file

La figura seguente mostra le porte da aprire per un gateway file S3.



> **Note**
>
> Per requisiti di porta specifici, consultaRequisiti porta.

Per S3 File Gateway, è necessario utilizzare Microsoft Active Directory solo per consentire agli utenti del dominio di accedere a una condivisione file SMB (Server Message Block). È possibile unire il gateway file a qualsiasi dominio di Microsoft Windows valido (risolvibile mediante DNS).

È possibile utilizzare anche l'AWS Directory Serviceper creare unAWS Managed Microsoft ADin Amazon Web Services Cloud. Per la maggior parteAWS Managed Microsoft ADdistribuzioni, è necessario configurare il servizio DHCP (Dynamic Host Configuration Protocol) per il VPC. Per

informazioni sulla creazione di un set di opzioni DHCP, consultaCreazione di un set di opzioni DHCPnellaAWS Directory ServiceGuida di amministrazione.

Oltre alle porte comuni, Amazon S3 File Gateway richiede le seguenti porte.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP/UDP	2049 (NFS)	In entrata	Client NFS	Storage Gateway	Per connettersi ai sistemi locali alle condivisioni NFS esposte dal gateway.
TCP/UDP	111 (NFSv3)	In entrata	client NFSv3	Storage Gateway	Per consentire ai sistemi locali di connettersi al mappatore delle porte esposto dal gateway. **Note** Questa porta è necessaria solo per NFSv3.
TCP/UDP	20048 (NFSv3)	In entrata	client NFSv3	Storage Gateway	Per connettersi ai sistemi locali ai

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					supporti esposti dal gateway. **Note** Questa porta è necessaria solo per NFSv3.

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

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

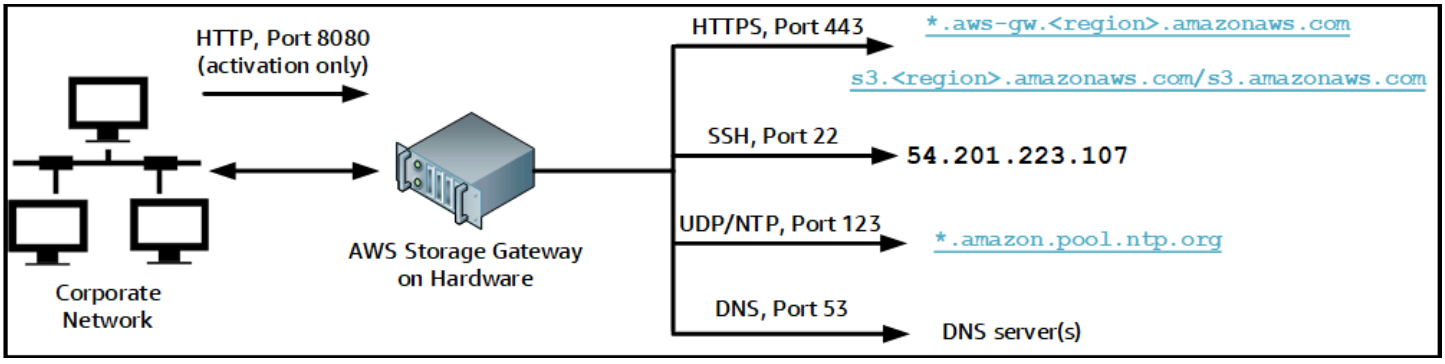
- Accesso a Internet- una connessione di rete a Internet sempre attiva tramite un'interfaccia di rete sul server.
- Servizi DNS— Servizi DNS per la comunicazione tra l'appliance hardware e il server DNS.
- Sincronizzazione oraria— un servizio orario Amazon NTP configurato automaticamente deve essere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

Ci sono cinque porte di rete fisiche nella parte posteriore del server Dell PowerEdge R640. 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	Modalità di 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

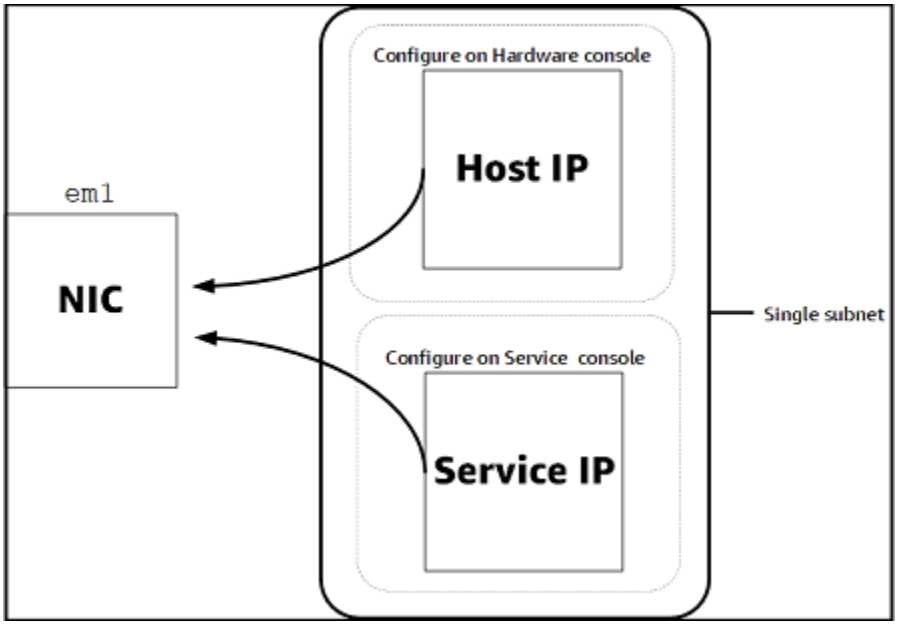
Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					brevemente)

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, consultare Configurazione dei parametri di rete.

> **Note**
>
> Per visualizzare un'illustrazione che mostra la parte posteriore del server con le relative porte, consultaMontaggio su rack dell'apparecchio hardware e collegamento all'alimentazione.

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 appliance hardware, consultaUtilizzo dell'appliance hardware Storage Gateway.

Consentire ad AWS Storage Gateway l'accesso attraverso firewall e router

Il gateway richiede l'accesso ai seguenti endpoint di servizio per comunicare conAWS. 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 abilitino questi endpoint di servizio alle comunicazioni in uscitaAWS.

> **Important**
>
> A seconda del gatewayAWSRegione, sostituisci*regione*nell'endpoint del servizio con la stringa Regione corretta.

Il seguente endpoint del servizio è obbligatorio da tutti i gateway per operazioni head-bucket.

```
s3.amazonaws.com:443
```

I seguenti endpoint di servizio sono richiesti da tutti i gateway per il percorso di controllo (`anon-cp`,`client-cp`,`proxy-app`) e percorso dati (`dp-1`) operazioni.

```
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 del servizio gateway nella regione Stati Uniti occidentali (Oregon) (`us-west-2`).

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

L'endpoint del servizio Amazon S3 mostrato di seguito viene utilizzato solo dai gateway file. Un gateway file richiede questo endpoint per accedere al bucket Amazon S3 su cui è mappata una condivisione file.

```
s3.region.amazonaws.com
```

L'esempio seguente è un endpoint del servizio Amazon S3 nella regione Stati Uniti orientali (Ohio) (Ohio) (`us-east-2`).

```
s3.us-east-2.amazonaws.com
```

> **Note**
>
> Se il gateway non è in grado di determinare ilAWSRegione in cui è ubicato il bucket S3, questo endpoint di servizio è impostato in modo predefinito sus`3.us-east-1.amazonaws.com`. Ti consigliamo di consentire l'accesso alla regione US East (N. Virginia) (`us-east-1`) in aggiunta alle regioni in cui il gateway è attivo e in cui si trova il bucket S3.

Di seguito sono riportati gli endpoint del servizio Amazon S3 perAWS GovCloud (US)Regioni.

```
s3-fips-us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
```

```
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

L'esempio seguente è un endpoint del servizio FIPS per un bucket S3 nelAWSRegione GovCloud (US-West).

```
bucket-name.s3-fips-us-gov-west-1.amazonaws.com
```

L'endpoint Amazon CloudFront seguente è necessario affinché Storage Gateway possa ottenere l'elenco dei prodotti disponibiliAWSRegioni.

```
https://d4kdq0yaxexbo.cloudfront.net/
```

Una macchina virtuale Storage Gateway è configurata in modo che possa utilizzare i seguenti server NTP.

```
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

- Storage Gateway: per supportoAWSRegioni e un elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.
- Storage Gateway Hardware Appliance — Per supportoAWSRegioni che è possibile utilizzare con l'appliance hardware, vedereRegioni dell'appliance hardware Storage GatewaynellaAWSRiferimenti generali.

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

Nello statoAWS Storage Gateway, un gruppo di sicurezza controlla il traffico verso l'istanza del 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.

  Per permettere a delle istanze di connettersi al gateway dall'esterno del gruppo di sicurezza, è consigliabile ammettere connessioni solo sulle porte 3260 (per connessioni iSCSI) e 80 (per 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 utilizzi AWS Support per la risoluzione dei problemi. Per ulteriori informazioni, consultare VuoiAWS Supportper aiutare a risolvere i problemi del gateway EC2.

In certi casi è possibile utilizzare un'istanza Amazon EC2 come iniziatore (ad esempio, per collegarsi alle destinazioni iSCSI su un gateway distribuito su Amazon EC2), consigliamo un approccio in due fasi:

1. Innanzitutto, bisogna avviare l'istanza dell'iniziatore nello stesso gruppo di sicurezza del gateway.
2. Successivamente, occorre configurare l'accesso in modo che l'iniziatore possa comunicare con il gateway.

Per informazioni sulle porte da aprire per il gateway, consulta Requisiti porta.

Hypervisor supportati e requisiti di hosting

È possibile eseguire Storage Gateway in locale sotto forma di appliance di macchina virtuale (VM) o appliance hardware fisica oppure inAWScome istanza Amazon EC2.

Storage Gateway supporta le seguenti versioni di hypervisor e host:

- VMware Hypervisor ESXi (versione 6.0, 6.5 o 6.7) - Una versione gratuita di VMware è disponibile sulla paginaSito Web VMware. Per questa configurazione, è inoltre necessario disporre di un client VMware vSphere per connettersi all'host.
- Microsoft Hyper-V Hyper-V (versione 2012 R2 o 2016) - Una versione standalone gratuita di Hyper-V è disponibile nella paginaCentro download Microsoft. 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 Linux (KVM) - 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, 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.

- Istanza Amazon EC2 - Storage Gateway fornisce un'immagine macchina Amazon (AMI) che contiene l'immagine della macchina virtuale del gateway. Per informazioni su come distribuire un gateway su Amazon EC2, consultaDistribuzione di un gateway di file su un host Amazon EC2.
- Appliance hardware Storage Gateway - Storage Gateway fornisce un'appliance hardware fisica come opzione di distribuzione 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, consultare Ripristino da un arresto imprevisto della macchina virtuale. Storage Gateway non supporta il ballooning di memoria dinamica e memoria virtuale.

Client NFS supportati per un gateway file

I gateway file supportano i seguenti client NFS (Network File System):

- Amazon Linux
- Mac OS X

> **Note**
>
> Consigliamo di impostare l'impostazione`rsize`e`wsize`montare le opzioni su 64 KB per migliorare le prestazioni durante il montaggio di condivisioni di file NFS su Mac OS X.

- RHEL 7
- SUSE Linux Enterprise Server 11 e SUSE Linux Enterprise Server 12
- Ubuntu 14.04
- Microsoft Windows 10 Enterprise, Windows Server 2012 e Windows Server 2016. I client nativi supportano solo NFS versione 3.
- Windows 7 Enterprise e Windows Server 2008.

I client nativi supportano solo NFS versione 3. La dimensione massima supportata di I/O NFS è 32 KB, quindi su queste versioni di Windows si potrebbero registrare prestazioni scadenti.

> **Note**
>
> Ora puoi utilizzare condivisioni di file SMB quando l'accesso è richiesto tramite client SMB Windows anziché tramite client NTF Windows.

Client SMB supportati per un gateway file

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

- Microsoft Windows Server 2008 e versione successiva
- 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 SMB v2.1.

Operazioni del file system supportate per un gateway di file

Il client NFS o SMB può scrivere, leggere, eliminare, rinominare e troncare i file. Quando i client inviano la scrittura aAWS Storage Gateway, scrive sulla cache locale in modo sincrono. Quindi, scrive su Amazon S3 in modo asincrono tramite trasferimenti ottimizzati. Le letture vengono servite automaticamente tramite la cache locale. Se i dati non sono disponibili, vengono recuperati tramite S3 come cache read-through.

Le operazioni di lettura e scrittura sono ottimizzate in modo tale che solo le parti modificate o richieste vengano tramite gateway. Elimina oggetti rimuovi oggetti da Amazon S3. Le directory vengono gestite come oggetti cartella in S3, utilizzando la stessa sintassi della console Amazon S3.

Le operazioni HTTP quali `GET`, `PUT`, `UPDATE` e `DELETE` possono modificare i file in una condivisione file. Queste operazioni sono conformi alle funzioni atomiche di creazione, lettura, aggiornamento ed eliminazione (CRUD).

Accesso a AWS Storage Gateway

Puoi utilizzare il pluginAWS Storage Gatewayplanciaper eseguire diverse attività di gestione e di configurazione del gateway. La sezione Nozioni di base e diverse altre sezioni di questa guida utilizzano la console per illustrare le funzionalità del gateway.

Inoltre, è possibile utilizzare l'API AWS Storage Gateway in modo programmatico per configurare e gestire i gateway. Per ulteriori informazioni sull'API, consulta Riferimento API per Storage Gateway.

È possibile utilizzare anche l'AWSPer sviluppare applicazioni che interagiscono con Storage Gateway. LaAWSGli SDK per Java, .NET e PHP integrano l'API di Storage Gateway sottostante per semplificare le attività di programmazione. Per informazioni sul download delle librerie SDK, consulta la sezioneAWSDeveloper Center.

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

Regioni AWS supportate

- Storage Gateway - Per supportatoAWSRegioni e un elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.
- Storage Gateway Hardware Appliance: per le regioni supportate che è possibile utilizzare con l'appliance hardware, vedereAWS Storage GatewayRegioni dell'appliance hardwarenellaAWSRiferimenti generali.

Utilizzo dell'appliance hardware Storage Gateway

Storage Gateway Hardware Appliance è un'appliance hardware fisica con il software Storage Gateway preinstallato su una configurazione del server convalidata. È possibile gestire l'appliance hardware dallaHardwarepagina sullaAWS Storage Gatewayconsole.

L'appliance hardware è un server 1U ad alte prestazioni che è possibile distribuire nel proprio data center oppure in locale all'interno di un firewall aziendale. Quando si acquista e attiva l'appliance hardware, il processo di attivazione associa l'appliance hardware conAWSconto. Dopo l'attivazione, l'appliance hardware verrà visualizzata nella console come un gateway sull'Hardware(Certificato creato). È possibile configurare l'appliance hardware come gateway di file, gateway di nastri o gateway di volumi. La procedura utilizzata per distribuire e attivare questi tipi di gateway su un'appliance hardware è la stessa da seguire su una piattaforma virtuale.

Lo Storage Gateway Hardware Appliance può essere ordinato direttamente dalAWS Storage Gatewayconsole.

Per ordinare un apparecchio hardware

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/homee scegli ilAWSRegioni in cui si desidera inserire l'appliance.
2. ScegliereHardwaredal riquadro di navigazione.
3. SceglioreOrdinare Appliancee quindi scegliereProcedi. Vieni reindirizzato allaAWSElemental Appliances e Software Management Console per richiedere un preventivo di vendita.
4. Compila le informazioni necessarie e scegliInvia.

Una volta esaminate le informazioni, viene generato un preventivo di vendita e potrai procedere con il processo di ordinazione e inviare un ordine di acquisto o organizzare il pagamento anticipato.

Per visualizzare un preventivo di vendita o la cronologia degli ordini per l'appliance hardware

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. SceglioreHardwaredal riquadro di navigazione.
3. SceglierePreventivi e ordinie quindi scegliereProcedi. Vieni reindirizzato allaAWSElemental Appliances e Software Management Console per esaminare preventivi di vendita e cronologia degli ordini.

Nelle sezioni successive, è possibile trovare le istruzioni su come configurare, attivare, avviare e usare un'appliance hardware Storage Gateway.

Argomenti

Regioni AWS supportate

Storage Gateway Hardware Appliance è disponibile per la spedizione in tutto il mondo dove è legalmente consentito e consentito per l'esportazione da parte del governo degli Stati Uniti. Per informazioni sul supportoAWSRegioni, vediRegioni del Storage Gateway Hardware AppliancenellaAWSRiferimenti generali.

Configurazione dell'appliance hardware

Dopo aver ricevuto l'appliance hardware Storage Gateway, è possibile utilizzare la console dell'appliance hardware per configurare le reti per fornire una connessione sempre attivaAWSe attiva il tuo apparecchio. L'attivazione associa il tuo apparecchio alAWSAccount utilizzato durante il processo di attivazione. Dopo che l'appliance è stata attivata, è possibile avviare un gateway di file, di volumi o nastri dalla console Storage Gateway.

Per installare e configurare l'appliance hardware

1. Montare l'appliance su rack e collegare l'alimentazione e le connessioni di rete. Per ulteriori informazioni, consultare Montaggio su rack dell'apparecchio hardware e collegamento all'alimentazione.

2. Impostare gli indirizzi del protocollo Internet versione 4 (IPv4) sia per l'appliance hardware (l'host) che per Storage Gateway (il servizio). Per ulteriori informazioni, consultare Configurazione dei parametri di rete.
3. Attivare l'apparecchio hardware sulla consoleHardware(Risorsa allaAWSRegioni di tua scelta. Per ulteriori informazioni, consultare Attivazione dell'appliance hardware.
4. Installare lo Storage Gateway sull'appliance hardware. Per ulteriori informazioni, consultare Configurazione del gateway.

   Si configurano i gateway sull'appliance hardware nello stesso modo in cui si configurano i gateway su VMware ESXi, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) 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. Questo fornisce una cache più grande per un accesso a bassa latenza ai dati inAWS. Se si è ordinato il modello da 5 TB, è possibile aumentare lo spazio di archiviazione utilizzabile fino a 12 TB acquistando cinque SSD da 1,92 TB (unità a stato solido), disponibili per l'ordinazione sulla consoleHardware(Certificato creato). È possibile ordinare gli SSD aggiuntivi seguendo lo stesso processo di ordinazione di un accessorio hardware e richiedendo un preventivo di vendita dalla console Storage Gateway.

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

1. Ripristinare l'appliance hardware alle impostazioni predefinite. ContattiAWSSupport per le istruzioni su come eseguire questa operazione.
2. Aggiungere cinque unità SSD da 1,92 TB all'appliance.

Opzioni della scheda di interfaccia di rete

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

- Configurazione NIC 10G-Base-T:
  - Utilizzare cavi CAT6 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 1G-Base-T o 10G-Base-T

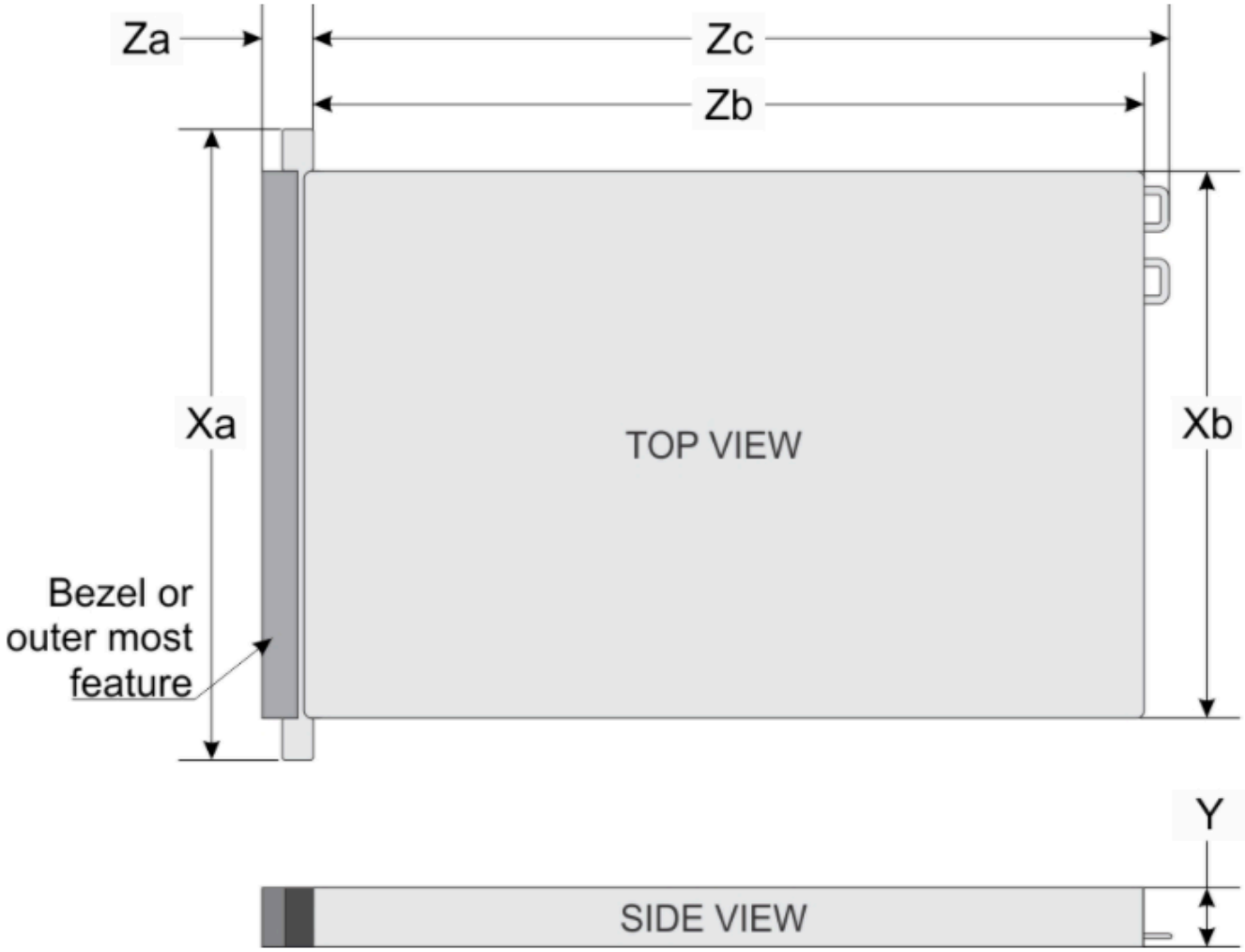
Montaggio su rack dell'apparecchio hardware e collegamento all'alimentazione

Dopo aver disimpallato lo Storage Gateway Hardware Appliance, seguire le istruzioni contenute nella confezione per montare su rack il server. L'appliance dispone di un fattore di forma 1U e può essere installata in un rack da 19" conforme con IEC (International Electrotechnical Commission).

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

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

Dimensioni del dispositivo hardware



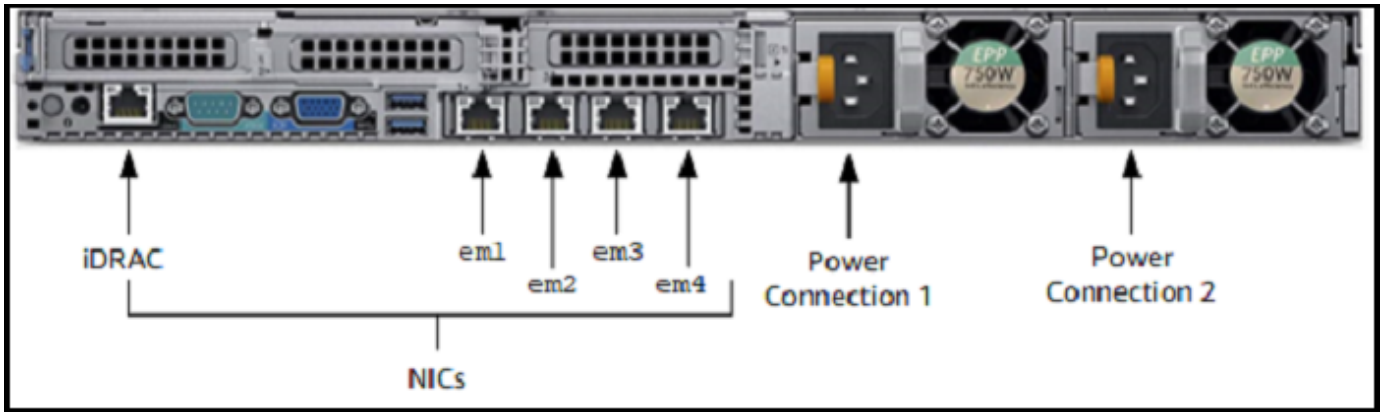
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

Per connettere l'appliance hardware all'alimentazione

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

1. Collegare una connessione all'alimentazione a ciascuno dei due alimentatori. È possibile collegare una sola connessione di alimentazione, ma consigliamo di collegare entrambi gli alimentatori.

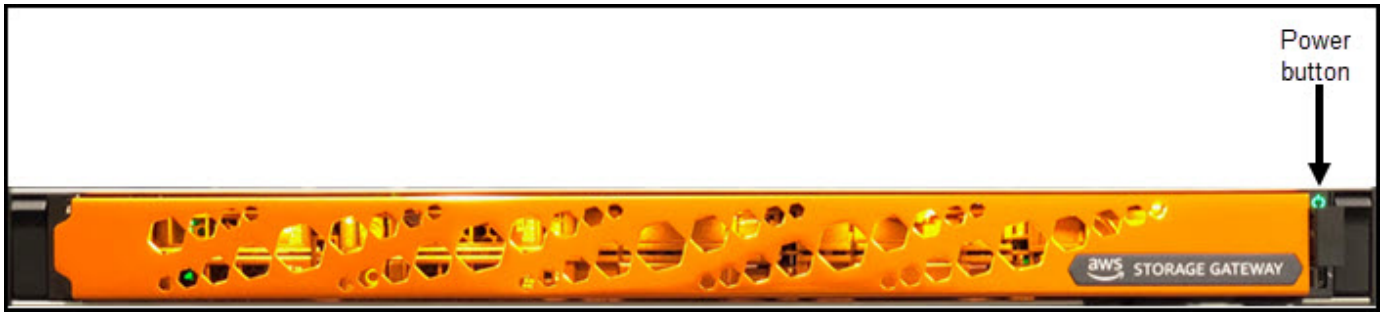
   Nell'immagine seguente è possibile visualizzare l'appliance hardware con le diverse connessioni.

2. Inserire il cavo Ethernet nella porta `em1` per fornire 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.

3. Collegare la tastiera e il monitor.
4. Accendere il server premendo il pulsante Power sul pannello anteriore, come mostrato nell'immagine seguente.



Dopo l'avvio del server, la console hardware viene visualizzata sul monitor. La console hardware offre un'interfaccia utente specifica diAWSche è possibile utilizzare per configurare i parametri di rete iniziali. Si configurano questi parametri per connettere l'applianceAWSe aprire un canale di supporto per la risoluzione dei problemi tramiteAWSSupport.

Per utilizzare la console hardware, immettere il testo con la tastiera e utilizzare i tasti `Up`, `Down`, `Right` e `Left Arrow` per spostarsi 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.

Per impostare una password per la prima volta

1. Per Set Password (Imposta password), immettere una password e premere `Down arrow`.
2. Per Confirm (Conferma), immettere nuovamente la password e quindi scegliere Save Password (Salva password).

A questo punto ci si trova nella console hardware, come mostrato di seguito.

Approfondimenti

[Configurazione dei parametri di rete]

Configurazione dei parametri di rete

Dopo l'avvio del server, è possibile inserire la prima password nella console hardware come descritto in [Montaggio su rack dell'apparecchio hardware e collegamento all'alimentazione].

Quindi, effettuare la procedura seguente nella console hardware per configurare i parametri di rete in modo che l'appliance hardware sia in grado di connettersiAWS.

Per impostare un indirizzo di rete

1. Scegliere Configure Network (Configura rete) e premere il tasto `Enter`. La schermata Configure Network (Configura rete) appare come mostrato di seguito.

2. Per IP Address (Indirizzo IP), immettere un indirizzo IPv4 valido da una delle fonti seguenti:

   - Utilizzare l'indirizzo IPv4 assegnato dal server DHCP (Dynamic Host Configuration Protocol) alla porta di rete fisica.

     In questo caso, annotare questo indirizzo IPv4 per poterlo utilizzare successivamente nella fase di attivazione.

   - Assegnare un indirizzo IPv4 statico. Per farlo, scegliere Static (Statico) nella sezione `em1` e premere `Enter` per visualizzare la schermata di configurazione di un IP statico mostrata di seguito.

     La sezione `em1` è in alto a sinistra nelle impostazioni del gruppo di porte.

   Dopo aver immesso un indirizzo IPv4 valido, premere `Down arrow` oppure `Tab`.

> **Note**
>
> Se si configura qualsiasi altra interfaccia, è necessario fornire la stessa connessione sempre attiva conAWSendpoint elencati nei requisiti.

3. Per Subnet (Sottorete), immettere una maschera di sottorete valida, quindi premere `Down arrow`.
4. Per Gateway, immettere l'indirizzo IPv4 del gateway di rete, quindi premere `Down arrow`.
5. Per DNS1, immettere l'indirizzo IPv4 per il server DNS (Domain Name Service), quindi premere `Down arrow`.
6. (Facoltativo) Per DNS2, immettere un secondo indirizzo IPv4, quindi premere `Down arrow`. Incaricare un secondo server DNS fornirebbe ulteriore ridondanza qualora il primo server DNS non fosse disponibile.
7. Scegliere Save (Salva) quindi premere `Enter` per salvare l'impostazione dell'indirizzo IPv4 statico per l'appliance.

Per disconnettersi dalla console hardware

1. Scegliere Back (Indietro) per tornare alla schermata principale.
2. Scegliere Logout (Esci) per tornare alla schermata di login.

Approfondimenti

Attivazione dell'appliance hardware

Attivazione dell'appliance hardware

Dopo aver configurato l'indirizzo IP, è necessario immettere l'indirizzo IP nella pagina Hardware della console, come descritto di seguito. Il processo di attivazione consente di verificare che l'appliance hardware abbia le opportune credenziali di sicurezza e di registrare l'appliance sull'AWSconto.

È possibile scegliere di attivare l'appliance hardware in uno qualsiasi dei dispositivi supportatiAWSRegioni. Per un elenco di supportateAWSRegioni, vediRegioni del Storage Gateway Hardware AppliancenellaAWSRiferimenti generali.

Per attivare l'appliance per la prima volta oppure in unAWSRegione in cui non sono stati distribuiti gateway

1. Accedi allaAWS Management Consolee apri la console Storage Gateway all'indirizzoAWS Storage GatewayConsole di gestionecon le credenziali dell'account da utilizzare per attivare l'hardware.

   Se questo è il tuo primo gateway in unAWSRegioni, viene visualizzata una schermata iniziale. Dopo aver creato un gateway in questoAWSRegione, lo schermo non viene più visualizzato.

   > **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. Scegliere Get started (Inizia) per visualizzare la procedura guidata di creazione gateway e quindi scegliere Hardware Appliance (Appliance hardware) nella pagina Select host platform (Seleziona piattaforma host), come mostrato di seguito.
3. Scegliere Next (Avanti) per visualizzare la schermata Connect to hardware (Connetti a hardware) mostrata di seguito.
4. PerIndirizzo IPnellaCollegare all'appliance hardware, immettere l'indirizzo IPv4 dell'appliance e quindi scegliereCollegarsiper andare alla schermata Attiva hardware mostrata di seguito.
5. Per Hardware name (Nome hardware), inserire un nome per l'appliance. I nomi possono contenere fino a 255 caratteri e non possono includere una barra.
6. PerFuso orario hardware, inserisci le impostazioni locali.

   Il fuso orario determina quando l'hardware effettua gli aggiornamenti; l'ora per gli aggiornamenti è impostata sulle 2:00 ora locale.

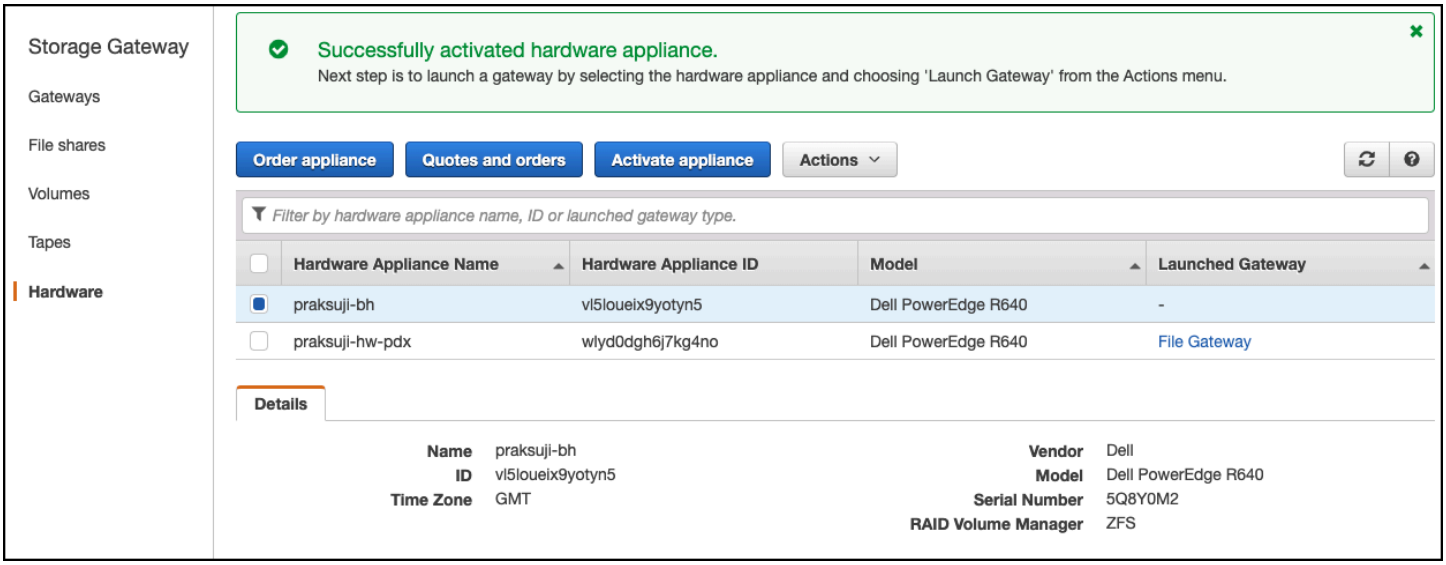
   > **Note**
   >
   > Consigliamo di impostare il fuso orario per l'appliance, in modo che il periodo di aggiornamento standard non corrisponda al normale orario di lavoro.

7. (Facoltativo) Mantenere il RAID Volume Manager (Gestore volumi RAID) impostato su ZFS.

   ZFS viene utilizzato come gestore di volume RAID sull'appliance hardware per fornire prestazioni e protezione dei dati migliori. ZFS è un gestore logico di volumi basato su software con un file system open source. L'appliance hardware è ottimizzata specificatamente per ZFS RAID. Per ulteriori informazioni su ZFS RAID, consulta la pagina di Wikipedia ZFS.
8. Scegliere Next (Avanti) per completare l'attivazione.

Un banner della console verrà visualizzato nella pagina Hardware per indicare che l'appliance hardware è stata attivata correttamente, come mostrato di seguito.

A questo punto, l'appliance è associata all'account. Il passaggio successivo è quello di avviare un gateway di file, di nastri o di volumi nella cache sull'appliance.



Approfondimenti

[Avvio di un gateway]

Avvio di un gateway

È possibile avviare uno qualsiasi dei tre gateway di storage sull'appliance: gateway di file, gateway volume (cache) o gateway a nastro.

Per avviare un gateway sull'appliance hardware.

1. Accedi allaAWS Management Consolee apri la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere Hardware.
3. Per Actions (Operazioni), scegliere Launch Gateway (Avvia gateway).
4. Per Gateway Type (Tipo gateway), scegliere File Gateway (Gateway di file), Tape Gateway (Gateway di nastri) o Volume Gateway (Cached) (Gateway di volumi - nella cache).
5. Per Gateway name (Nome gateway), inserire un nome per il gateway. I nomi possono avere al massimo una lunghezza di 255 caratteri e non possono includere una barra.
6. Scegliere Launch gateway (Avvia gateway).

Il software Storage Gateway per il tipo di gateway scelto verrà installato sull'appliance. Possono essere necessari fino a 5-10 minuti prima che un gateway appaiaonlinenella console.

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 per il gateway

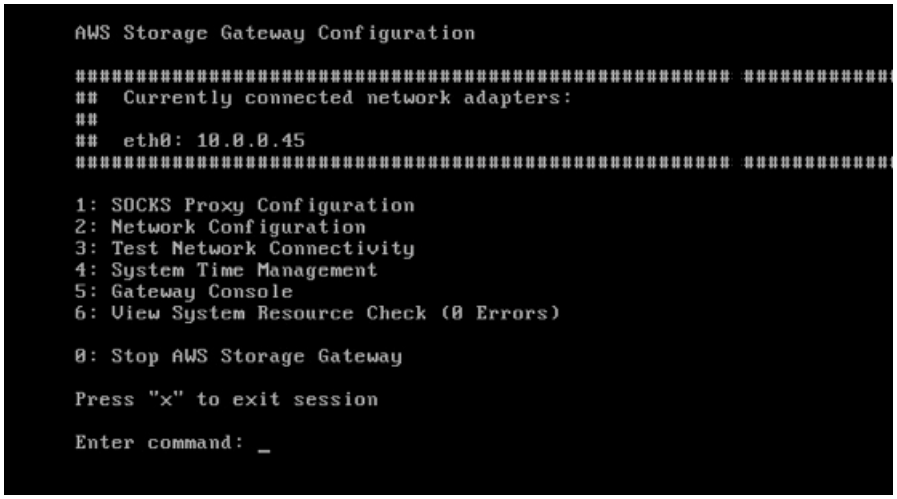
Configurazione di un indirizzo IP per il gateway

Prima di attivare l'appliance hardware, è stato assegnato un indirizzo IP alla sua interfaccia di rete fisica. Dopo aver attivato l'appliance e avviato Storage Gateway su di esso, è necessario assegnare un altro indirizzo IP alla macchina virtuale Storage Gateway che funziona sull'appliance hardware. Per assegnare un indirizzo IP statico a un gateway installato sull'appliance hardware, configurare l'indirizzo IP dalla console locale del gateway. Le applicazioni (come ad esempio il client NFS o SMB, l'iniziatore iSCSI etc.) si connettono a questo indirizzo IP. È possibile accedere alla console locale del gateway dalla console dell'appliance hardware.

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

1. Nella console hardware, scegliere Open Service Console (Apri console di servizio) per aprire una schermata di accesso per la console locale del gateway.
2. Inserire la password di login del localhost, quindi premere `Enter`.

   L'account predefinito è `admin` e la password predefinita è `password`.
3. Modificare la password predefinita. Scegliere Actions (Operazioni) quindi Set Local Password (Imposta password locale) e inserire le nuove credenziali nella finestra di dialogo Set Local Password (Imposta password locale).
4. (Facoltativo) Configurare le impostazioni del proxy. Per istruzioni, consulta Montaggio su rack dell'apparecchio hardware e collegamento all'alimentazione.
5. Passare alla pagina Impostazioni di rete della console locale del gateway, come mostrato di seguito.



6. Digitare 2 per andare alla pagina Network Configuration (Configurazione di rete) mostrata di seguito.

7. Configurare un indirizzo IP statico o DHCP per la porta di rete in modo che l'appliance hardware presenti un gateway di file, di volumi e di nastri per le applicazioni. Questo indirizzo IP deve essere nella stessa sottorete dell'indirizzo IP utilizzato durante l'attivazione dell'appliance.

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.

Approfondimenti

Configurazione del gateway

Configurazione del gateway

Dopo che l'appliance hardware è stata attivata e configurata, l'appliance viene visualizzata nella console. Ora è possibile creare il tipo di gateway che si desidera. Continuare l'installazione per il tipo di gateway. Per istruzioni, consultare Configurare il tuo Amazon S3 File Gateway.

Rimozione di un gateway dall'appliance hardware

Per rimuovere un software del gateway dall'appliance hardware, utilizzare la procedura seguente. Dopo aver completato la procedura, il software del gateway viene disinstallato dall'appliance hardware.

Per rimuovere un gateway da un'appliance hardware

1. Scegliere la casella di controllo per il gateway.
2. Per Actions (Operazioni), selezionare Remove Gateway (Rimuovi gateway).
3. Nella finestra di dialogo Remove gateway from hardware appliance (Rimuovi gateway dall'appliance hardware), scegliere Confirm (Conferma).

> **Note**
>
> Quando si elimina un gateway, non è possibile annullare l'operazione. Per determinati tipi di gateway, è possibile che all'eliminazione si perdano dei dati, soprattutto dati memorizzati nella cache. Per ulteriori informazioni sull'eliminazione di un gateway, consulta Eliminazione del gateway tramite la console AWS Storage Gateway e rimozione delle risorse associate.

L'eliminazione di un gateway non elimina l'appliance hardware dalla console. L'appliance hardware rimane disponibile per future distribuzioni di gateway.

Eliminazione dell'appliance hardware

Dopo aver attivato l'apparecchio hardware nel tuoAWS, è possibile che si debba spostarlo e attivarlo in un altroAWSconto. In questo caso, è necessario eliminare prima l'appliance dallaAWSaccount e attivalo in un altroAWSconto. È inoltre possibile eliminare completamente l'appliance dall'AWSaccount perché non ne hai più bisogno. Seguire queste istruzioni per eliminare l'appliance hardware.

Per eliminare l'appliance hardware

1. Se è stato installato un gateway sull'appliance hardware, è necessario prima rimuovere il gateway per eliminare l'appliance. Per istruzioni su come rimuovere un gateway dall'appliance hardware, consultaRimozione di un gateway dall'appliance hardware.
2. Nella pagina Hardware, scegliere l'appliance hardware da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack).
4. Nella finestra di dialogo Confirm deletion of resource(s) (Conferma eliminazione delle risorse), selezionare la casella di controllo di conferma quindi scegliere Delete (Elimina). Viene visualizzato un messaggio che indica l'avvenuta eliminazione.

   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.

Nozioni di base su AWS Storage Gateway

In questa sezione, puoi trovare le istruzioni su come creare e attivare un gateway di file inAWS Storage Gateway. Prima di iniziare, verificare che la configurazione soddisfi i prerequisiti richiesti e gli altri requisiti descritti inConfigurazione di Amazon S3 File Gateway.

Argomenti

- Creare e attivare un gateway Amazon S3 File Gateway

Creare e attivare un gateway Amazon S3 File Gateway

In questa sezione, puoi trovare le istruzioni su come creare, distribuire e attivare un gateway di file inAWS Storage Gateway.

Argomenti

- Configurazione di un gateway Amazon S3 File Gateway
- Connect il tuo Amazon S3 File Gateway aAWS
- Controlla le impostazioni e attiva il tuo Amazon S3 File Gateway
- Configurare il tuo Amazon S3 File Gateway

Configurazione di un gateway Amazon S3 File Gateway

Per configurare un nuovo gateway S3 File Gateway

1. Apertura dellaAWS Management Consolealhttps://console.aws.amazon.com/storagegateway/home/e scegli ilRegione AWSdove si desidera creare il gateway.
2. ScegliereCreazione gatewayper aprireImpostazione del gateway(Certificato creato).
3. NellaImpostazioni gatewaysezione, eseguire queste operazioni:

    a. Per Gateway name (Nome gateway), inserire un nome per il gateway. Dopo aver creato il gateway, puoi cercare questo nome per trovare il gateway nelle pagine dell'elencoAWS Storage GatewayConsole.

    b. PerFuso orario gateway, scegli il fuso orario locale per la parte del mondo in cui vuoi distribuire il gateway.

4. NellaOpzioni gatewaysezione, perTipo di gateway, scegliGateway dei file Amazon S3.
5. NellaOpzioni della piattaformasezione, eseguire queste operazioni:

   a. PerPiattaforma host, scegliere la piattaforma in cui si desidera distribuire il gateway. Seguire quindi le istruzioni specifiche della piattaforma visualizzate nella pagina della console Storage Gateway per configurare la piattaforma host. Puoi scegliere tra le seguenti opzioni:

      - VMware ESXi— Scaricare, distribuire e configurare la macchina virtuale gateway utilizzando VMware ESXi.
      - Microsoft Hyper-V— Scaricare, distribuire e configurare la macchina virtuale gateway utilizzando Microsoft Hyper-V.
      - KVM Linux— Scaricare, distribuire e configurare la macchina virtuale gateway utilizzando KVM (Linux Kernel-based Virtual Machine).
      - Amazon EC2— Configurare e avviare un'istanza Amazon EC2 per ospitare il gateway.
      - Appliance hardware— Ordina un apparecchio hardware fisico dedicato daAWSper ospitare il gateway.

   b. PerConferma il gateway di configurazione, selezionare la casella di controllo per confermare di aver eseguito i passaggi di distribuzione per la piattaforma host scelta. Questo passaggio non è applicabile alAppliance hardwarepiattaforma host.
6. Una volta configurato il gateway, è necessario scegliere il modo in cui si desidera collegarlo e comunicare conAWS. ScegliereSuccessivoContinua con la.

Connect il tuo Amazon S3 File Gateway aAWS

Per connettere un nuovo file gateway S3 aAWS

1. Se non lo hai già fatto, completa la procedura descritta inConfigurazione di un gateway Amazon S3 File Gateway. Al termine, scegliSuccessivoper aprireConnect to (Connettiti a)AWS(Creare) dellaAWS Storage GatewayConsole.
2. NellaOpzioni endpointsezione, perEndpoint del servizio, scegliere il tipo di endpoint con cui il gateway utilizzerà per comunicareAWS. Puoi scegliere tra le seguenti opzioni:

   - Accessibile pubblicamente— Il gateway comunica conAWSsu Internet pubblico. Se selezioni questa opzione, utilizzaEndpoint abilitato FIPScasella di controllo per specificare se la connessione deve essere conforme agli standard FIPS (Federal Information Processing Standard).

> **Note**
>
> Se richiedi moduli crittografici convalidati FIPS 140-2 quando accediAWStramite un'interfaccia a riga di comando o un'API, utilizzare 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 alcuniAWSRegioni. Per ulteriori informazioni, consultaAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

- Ospitato in VPC— Il gateway comunica conAWStramite una connessione privata con il cloud privato virtuale (VPC), consentendo 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 dell'endpoint VPC (Domain Name System).

3. NellaOpzioni di connessione del gatewaysezione, perOpzioni di connessione, scegli come identificare il tuo gateway perAWS. Puoi scegliere tra le seguenti opzioni:

   - Indirizzo IP— Fornire l'indirizzo IP del gateway nel campo corrispondente. Questo indirizzo IP deve essere pubblico o accessibile dalla rete corrente e devi essere in grado di connetterti dal browser Web.

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

   - Chiave di attivazione— Fornire 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 come vuoi che il tuo gateway si connettaAWS, è necessario attivare il gateway. ScegliereSuccessivoContinua con la.

Controlla le impostazioni e attiva il tuo Amazon S3 File Gateway

Per attivare un nuovo gateway file S3

1. Se non lo hai già fatto, completa le procedure descritte nei seguenti argomenti:

   - Configurazione di un gateway Amazon S3 File Gateway

- Connect il tuo Amazon S3 File Gateway aAWS

Al termine, scegliSuccessivoper aprireEsaminare e attivare(Creare) dellaAWS Storage GatewayConsole.

2. Esamina i dettagli iniziali del gateway per ogni sezione della pagina.
3. Se una sezione contiene errori, scegliereModificareper tornare alla pagina delle impostazioni corrispondente e apportare modifiche.

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

4. Dopo aver attivato il gateway, è necessario eseguire la prima configurazione per allocare i dischi di storage locali e configurare la registrazione. ScegliereSuccessivoContinua con la.

Configurare il tuo Amazon S3 File Gateway

Per eseguire la prima configurazione su un nuovo file gateway S3

1. Se non lo hai già fatto, completa le procedure descritte nei seguenti argomenti:

   - Configurazione di un gateway Amazon S3 File Gateway
   - Connect il tuo Amazon S3 File Gateway aAWS
   - Controlla le impostazioni e attiva il tuo Amazon S3 File Gateway

   Al termine, scegliSuccessivoper aprireImpostazione del gateway(Creare) dellaAWS Storage GatewayConsole.
2. NellaImpostazione dello storage della cachesezione, utilizzare gli elenchi a discesa per allocare almeno un disco locale con una capacità di almeno 150 gibibyte (GiB) aCache. I dischi locali elencati in questa sezione corrispondono allo storage fisico fornito sulla piattaforma host.
3. NellaGruppo di log CloudWatchsezione, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del gateway. Puoi scegliere tra le seguenti opzioni:

   - Creazione di un nuovo gruppo di log— Configura un nuovo gruppo di log per monitorare il gateway.

- Utilizzare un gruppo di log esistente;— Scegli un gruppo di log esistente dall'elenco a discesa corrispondente.
- Disattiva registrazione— Non utilizzare Amazon CloudWatch Logs per monitorare il gateway.

4. NellaAllarmi CloudWatchsezione, scegli come configurare gli allarmi Amazon CloudWatch per avvisarti quando le metriche del gateway si discostano dai limiti definiti. Puoi scegliere tra le seguenti opzioni:

   - Disattiva allarmi— Non utilizzare gli allarmi CloudWatch per ricevere una notifica sulle metriche del gateway.
   - Creare un allarme CloudWatch personalizzato— Configura un nuovo allarme CloudWatch per ricevere una notifica sulle metriche del gateway. ScegliereCreare allarmeper definire le metriche e specificare le operazioni di allarme nella console Amazon CloudWatch. Per istruzioni, consultaUtilizzo degli allarmi Amazon CloudWatchnellaGuida per l'utente di Amazon CloudWatch.

5. (Facoltativo) NelTagsezione, scegliAggiungi nuovo tag, quindi inserisci una coppia chiave-valore che fa distinzione tra maiuscole e minuscole per aiutarti a cercare e filtrare il gateway nelle pagine dell'elencoAWS Storage GatewayConsole. Ripetere questa fase per ogni tag necessario.

6. (Facoltativo) NelVerifica della configurazione VMware High Availabilitysezione, se il gateway viene distribuito su un host VMware come parte di un cluster abilitato per VMware High Availability (HA), sceglie reVerificare VMware HAper verificare se la configurazione HA funziona correttamente.

   > **Note**
   >
   > Questa sezione viene visualizzata solo per i gateway in esecuzione sulla piattaforma host VMware.
   > Questo passaggio non è necessario per completare il processo di configurazione del gateway. Puoi testare la configurazione HA del gateway in qualsiasi momento. La verifica richiede alcuni minuti e riavvia la macchina virtuale (VM) di Storage Gateway.

7. SceglieреConfiguraper completare la creazione del gateway.

   Per verificare lo stato del nuovo gateway, cercatelo nellaGateway(Creare) dellaAWS Storage GatewayConsole.

Una volta creata il gateway, è necessario creare una condivisione di file da utilizzare. Per istruzioni, consultaCreazione di una condivisione file.

Creazione di una condivisione file

Questa sezione include le istruzioni su come creare e utilizzare una condivisione di file. Puoi creare una condivisione file a cui accedere utilizzando il protocollo NFS (Network File System) o SMB (Server Message Block).

> **Note**
>
> Quando un file viene scritto sul gateway di file da un client NFS o SMB, il gateway di file carica i dati del file su Amazon S3 seguito dai relativi metadati (proprietà, timestamp e così via). Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto S3. Questo processo crea un'altra versione dell'oggetto, risultando in due versioni di un oggetto. Se la funzione Versioni multiple di S3 è abilitata, vengono memorizzate entrambe le versioni.
>
> Se si modificano i metadati di un file memorizzato nel gateway di file, viene creato un nuovo oggetto S3 e sostituisce l'oggetto S3 esistente. Questo comportamento è diverso dalla modifica di un file in un file system, in cui la modifica di un file non comporta la creazione di un nuovo file. Verifica tutte le operazioni sui file con cui intendi utilizzareAWSStorage Gateway per capire come ogni operazione di file interagisce con lo storage Amazon S3. Considerate attentamente l'uso di S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 quando carichi dati dal gateway di file. Il caricamento di file dal gateway di file su Amazon S3 quando è abilitato S3 Versioning si traduce in almeno due versioni di un oggetto S3.
>
> Alcuni flussi di lavoro che coinvolgono file di grandi dimensioni e modelli di scrittura di file, come i caricamenti di file eseguiti in diversi passaggi, possono aumentare il numero di versioni di oggetti S3 memorizzati. Se la cache del gateway di file deve liberare spazio a causa dell'elevata velocità di scrittura dei file, è possibile creare più versioni di oggetti S3. Questi scenari aumentano lo storage S3 se il controllo delle versioni di S3 è abilitato e aumentano i costi di trasferimento associati al CRR. Testare tutte le operazioni sui file che prevedi di utilizzare con Storage Gateway in modo da comprendere come ogni operazione di file interagisce con lo storage Amazon S3.
>
> L'utilizzo dell'utilità Rsync con il gateway di file comporta la creazione di file temporanei nella cache e la creazione di oggetti S3 temporanei in Amazon S3. Questa situazione comporta addebiti di cancellazione anticipata nelle classi di storage S3 Standard - Infrequent Access (S3 Standard - accesso infrequente) e S3 Intelligent-Tiering.

Quando crei una condivisione NFS, per impostazione predefinita chiunque possa accedere al server NFS può accedere alla condivisione file NFS. Puoi limitare l'accesso ai client in base all'indirizzo IP.

Per SMB, puoi disporre di uno dei tre diversi modi di autenticazione:

- Una condivisione file con accesso Microsoft Active Directory (AD). Qualsiasi utente Microsoft AD autenticato ottiene l'accesso a questo tipo di condivisione file.
- Una condivisione file SMB con accesso limitato. L'accesso è consentito solo ad alcuni utenti e gruppi di dominio specificati (tramite un elenco consentiti). Agli utenti e ai gruppi può anche essere negato l'accesso (tramite un elenco di negazione).
- Una condivisione file SMB con accesso guest. Qualsiasi utente in grado di fornire la password guest ottiene l'accesso a questa condivisione file.

> **Note**
>
> Le condivisioni di file esportati tramite il gateway per le condivisioni di file NFS supportano le autorizzazioni POSIX. Per la condivisione dei file SMB, è possibile usare liste di controllo accessi (ACL) per gestire le autorizzazioni su file e cartelle nella condivisione di file. Per ulteriori informazioni, consultare Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.

Un gateway di file può ospitare una o più condivisioni di diversi tipi di file. È possibile avere più condivisioni di file NFS e SMB su un gateway di file.

> **Important**
>
> Per creare una condivisione di file, un gateway di file richiede di attivareAWS Security Token Service(AWS STS). Assicurarsi cheAWS STSè attivato nelRegione AWSin cui stai creando il tuo gateway di file. SeAWS STSnon è attivato in questoRegione AWS, attivalo. Per informazioni su come attivareAWS STS, consultaAttivazione e disattivazioneAWS STSin unRegione AWSnellaAWS Identity and Access ManagementGuida per l'utente di.

> **Note**
>
> È possibile utilizzareAWS Key Management Service(AWS KMS) per crittografare gli oggetti che il gateway file memorizza in Amazon S3. Per eseguire

questa operazione utilizzando la console Storage Gateway, consultaCreare una condivisione file NFSoCreare una condivisione file SMB. Puoi anche eseguire questa operazione utilizzando l'API Storage Gateway. Per istruzioni, consultaCreateNFSFileShareoCreateSMBFileSharenellaAWSRiferimento delle API Storage Gateway.

Per impostazione predefinita, un gateway di file utilizza la crittografia lato server gestita con Amazon S3 (SSE-S3) quando scrive dati in un bucket S3. Se esegui la crittografia lato server SSE-KMS (lato server) conAWS KMS—managed keys) la crittografia predefinita per il bucket S3, gli oggetti archiviati da un gateway di file vengono crittografati con SSE-KMS.

Per crittografare utilizzando SSE-KMS con la propria chiave AWS KMS, è necessario abilitare la crittografia SSE-KMS. Per questa operazione, fornisci l'Amazon Resource Name (ARN) della chiave KMS quando crei la condivisione file. È inoltre possibile aggiornare le impostazioni del servizio di gestione delle chiavi per la condivisione file utilizzando l'operazione API UpdateNFSFileShare o UpdateSMBFileShare. Questo aggiornamento si applica agli oggetti archiviati nei bucket Amazon S3 dopo l'aggiornamento.

Se si configura il gateway di file per l'utilizzo di SSE-KMS per la crittografia, è necessario aggiungere manualmente`kms:Encrypt`,`kms:Decrypt`,`kms:ReEncrypt`,`kms:GenerateDataKey`, e`kms:DescribeKey`autorizzazioni per il ruolo IAM associato alla condivisione file Per ulteriori informazioni, consultaUtilizzo di policy basate su identità (policy IAM) per Storage Gateway.

Argomenti

- Creare una condivisione file NFS
- Creare una condivisione file SMB

Creare una condivisione file NFS

Usa la procedura seguente per creare una condivisione di file system (Network File System).

> **Note**
>
> Quando un file viene scritto sul gateway di file da un client NFS, il gateway di file carica i dati del file su Amazon S3 seguito dai relativi metadati (proprietà, timestamp e così via). Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati per il file

aggiorna i metadati per l'oggetto S3. Questo processo crea un'altra versione dell'oggetto, risultando in due versioni di un oggetto. Se la funzione Versioni multiple di S3 è abilitata, vengono memorizzate entrambe le versioni.
Se si modificano i metadati di un file memorizzato nel gateway di file, viene creato un nuovo oggetto S3 e sostituisce l'oggetto S3 esistente. Questo comportamento è diverso dalla modifica di un file in un file system, in cui la modifica di un file non comporta la creazione di un nuovo file. Verifica tutte le operazioni sui file con cui intendi utilizzareAWSStorage Gateway per capire come ogni operazione di file interagisce con lo storage Amazon S3.
Considerate attentamente l'uso di S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 quando carichi dati dal gateway di file. Il caricamento di file dal gateway di file su Amazon S3 quando è abilitato S3 Versioning si traduce in almeno due versioni di un oggetto S3.
Alcuni flussi di lavoro che coinvolgono file di grandi dimensioni e modelli di scrittura di file, come i caricamenti di file eseguiti in diversi passaggi, possono aumentare il numero di versioni di oggetti S3 memorizzati. Se la cache del gateway di file deve liberare spazio a causa dell'elevata velocità di scrittura dei file, è possibile creare più versioni di oggetti S3. Questi scenari aumentano lo storage S3 se il controllo delle versioni di S3 è abilitato e aumentano i costi di trasferimento associati al CRR. Testare tutte le operazioni sui file che prevedi di utilizzare con Storage Gateway in modo da comprendere come ogni operazione di file interagisce con lo storage Amazon S3.
L'utilizzo dell'utilità Rsync con il gateway di file comporta la creazione di file temporanei nella cache e la creazione di oggetti S3 temporanei in Amazon S3. Questa situazione comporta addebiti di cancellazione anticipata nelle classi di storage S3 Standard - Infrequent Access (S3 Standard - accesso infrequente) e S3 Intelligent-Tiering.

Per creare una condivisione file NFS

1. Apertura dellaAWSConsole Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home/.
2. ScegliereCreare una condivisione fileper aprireImpostazioni di condivisione file(Certificato creato).
3. Perportale, scegliere Amazon S3 File Gateway dall'elenco.
4. PerPercorso Amazon S3Effettuare una delle seguenti operazioni:

   - Per collegare la condivisione file direttamente a un bucket S3, scegliereNome bucket S3, quindi immettere il nome del bucket S3 e, facoltativamente, un nome di prefisso per gli oggetti

creati dalla condivisione file. Il gateway utilizza questo bucket per archiviare e recuperare i file. Per ulteriori informazioni sulla creazione di un nuovo bucket, consultaCome creare un bucket S3?nellaGuida per l'utente di Amazon S3.

- Per connettere la condivisione di file a un bucket S3 tramite un access point, selezionareAccess point S3, quindi immettere il nome del punto di accesso S3 e, facoltativamente, un nome di prefisso per gli oggetti creati dalla condivisione file. Il criterio del bucket deve essere configurato per delegare il controllo di accesso all'access point. Per ulteriori informazioni sui punti di accesso, consultaGestione dell'accesso ai dati con access point Amazon S3eDelegazione del controllo di accesso agli access pointnellaGuida per l'utente di Amazon S3.
- Per collegare la condivisione di file a un bucket S3 tramite un alias del punto di accesso, scegliereAlias del punto di accesso S3, quindi immettere il nome dell'alias del punto di accesso S3 e, facoltativamente, un nome di prefisso per gli oggetti creati dalla condivisione file. Se si sceglie questa opzione, il gateway di file non può crearne una nuovaAWS Identity and Access Management(IAM) policy d'accesso e ruolo per conto dell'utente. È necessario selezionare un ruolo IAM esistente e configurare un criterio di accesso nelAccesso al proprio bucket S3sezione che segue. Per ulteriori informazioni sugli alias dell'access point, consultaUtilizzo di un alias in stile bucket per il punto di accessonellaGuida per l'utente di Amazon S3.

> **Note**
>
> - Se si immette un nome di prefisso o si sceglie di connettersi tramite un punto di accesso o un alias del punto di accesso, è necessario immettere un nome di condivisione file.
> - Il nome del prefisso deve terminare con una barra (/).
> - Dopo aver creato la condivisione di file, il nome del prefisso non può essere modificato o eliminato.
> - Per ulteriori informazioni sull'uso di nomi prefissi, consultaOrganizzazione degli oggetti utilizzando i prefissinellaGuida per l'utente di Amazon S3.

5. PerRegione AWS, scegli ilRegione AWSdel bucket S3.
6. PerNome della condivisione file, digitare un nome per la condivisione file. Il nome predefinito è il nome del bucket S3 o il nome del punto di accesso.

> **Note**
>
> - Se si è immesso un nome di prefisso o si è scelto di connettersi tramite un punto di accesso o un alias del punto di accesso, è necessario immettere un nome di condivisione file.
> - Dopo aver creato la condivisione di file, il nome della condivisione file non può essere eliminato.

7. (Opzionale) PerAWS PrivateLinkper S3, eseguire le seguenti operazioni:

   1. Per configurare la condivisione di file per connettersi a S3 tramite un endpoint di interfaccia nel cloud privato virtuale (VPC) basato suAWS PrivateLink, scegliUtilizzo dell'endpoint VPC.
   2. Per identificare l'endpoint dell'interfaccia VPC a cui si desidera connettere la condivisione di file, scegliere unoID endpoint VPCoNome DNS dell'endpoint VPCe quindi fornire le informazioni richieste nel campo corrispondente.

   > **Note**
   >
   > - Questo passaggio è necessario se la condivisione di file si connette a S3 tramite un punto di accesso VPC o tramite un alias associato a un punto di accesso VPC.
   > - Utilizzo delle connessioni di condivisione fileAWS PrivateLinknon sono supportati sui gateway FIPS.
   > - Per informazioni suAWS PrivateLink, consultaAWS PrivateLinkper Amazon S3nellaGuida per l'utente di Amazon S3.

8. Per Access objects using (Accedi agli oggetti utilizzando), selezionare Network File System (NFS).
9. Per Registri di controllo, scegliere una delle opzioni seguenti:

   - Per disattivare la registrazione, scegliereDisabilitare la registrazione.
   - Per creare un nuovo registro di controllo, sceglieCrea un nuovo gruppo di log.
   - Per utilizzare un registro di controllo esistente, sceglieUtilizzare un gruppo di log esistente;, quindi scegliere un log di controllo dall'elenco.

Per ulteriori informazioni sui log di audit, consulta Informazioni sui log di controllo del gateway di file.

10. PerAggiornamento automatico della cache da S3, scegliImpostazione dell'intervallo di aggiornamentoe imposta il tempo in giorni, ore e minuti per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). Il TTL è il periodo di tempo dall'ultimo aggiornamento. Al termine dell'intervallo TTL, l'accesso alla directory fa sì che il gateway di file aggiorni prima il contenuto di quella directory dal bucket Amazon S3.
11. PerNotifica di caricamento file, scegliTempo di liquidazione (secondi)per ricevere una notifica quando un file è stato completamente caricato su S3 dal gateway di file. Impostazione della proprietàOrario di liquidazionein secondi per controllare il numero di secondi da attendere dopo l'ultimo momento in cui un client ha scritto su un file prima di generare un`ObjectUploaded`notifica. Poiché i client possono eseguire molte piccole scritture su file, è meglio impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in un breve periodo di tempo. Per ulteriori informazioni, consultare Ricevere notifica di caricamento file.

    > **Note**
    >
    > Questa impostazione non ha alcun effetto sulla tempistica del caricamento dell'oggetto su S3, solo sulla tempistica della notifica.

12. (Facoltativo) Nella sezione Add tags (Aggiungi tag), immettere una chiave e un valore per aggiungere tag alla condivisione file. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare la condivisione file.
13. Scegli Next (Successivo). LaConfigura come vengono archiviati i file in Amazon S3Viene visualizzata la pagina.
14. PerClasse di storage per nuovi oggetti, selezionare una classe di storage da utilizzare per i nuovi oggetti creati nel bucket Amazon S3:

    - Per archiviare i dati degli oggetti ad accesso frequente in modo ridondante in più zone di disponibilità geograficamente distinte, selezionareS3 Standard. Per ulteriori informazioni sulla classe di storage S3 Standard, consultaClassi di storage per oggetti a cui si accede di frequentenellaDocumentazione su Amazon Simple Storage Service.
    - Per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più conveniente, selezionareS3 Intelligent-Tiering. Per ulteriori informazioni

sulla classe di storage S3 Intelligent-Tiering, consultaLa classe di storage che ottimizza automaticamente gli oggetti con accesso più o meno frequentenellaDocumentazione su Amazon Simple Storage Service.

- Per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte, selezionareS3 Standard - accesso infrequente. Per ulteriori informazioni sulla classe di storage S3 Standard IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione su Amazon Simple Storage Service.
- Per archiviare i dati degli oggetti ad accesso poco frequente in un'unica zona di disponibilità, selezionareS3 One Zone-IA. Per ulteriori informazioni sulla classe di storage S3 One Zone-IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione su Amazon Simple Storage Service.

Per monitorare la fatturazione S3, usaAWS Trusted Advisor. Per ulteriori informazioni, consultaStrumenti di monitoraggionellaDocumentazione su Amazon Simple Storage Service.

15. Per Object metadata (Metadati oggetti), scegliere i metadati da utilizzare:

    - Per abilitare il controllo del tipo MIME per gli oggetti caricati in base alle estensioni di file, selezionareTipo MIME Guess.
    - Per fornire il controllo completo al proprietario del bucket S3 mappato alla condivisione file NFS, selezionareDare il pieno controllo del proprietario della benna. Per ulteriori informazioni sull'uso della condivisione file per accedere agli oggetti in un bucket di proprietà di un altro account, consultaUtilizzo di una condivisione file per l'accesso tra account.
    - Se si sta usando questa condivisione di file su un bucket che richiede il pagamento delle tariffe di accesso da parte del richiedente o del lettore al posto del proprietario del bucket.Abilita il pagamento del richiedente. Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.

16. PerAccesso al proprio bucket S3, scegli ilAWS Identity and Access Management(IAM) ruolo (IAM) che si desidera far utilizzare al gateway di file per accedere al bucket Amazon S3:

    - Per abilitare il gateway file per creare un nuovo ruolo IAM e policy d'accesso per conto dell'utente, selezionareCrea un nuovo ruolo IAM. Questa opzione non è disponibile se la condivisione di file si connette ad Amazon S3 utilizzando un alias del punto di accesso.
    - Per selezionare un ruolo IAM esistente e impostare manualmente i criteri di accesso, selezionareUtilizzare un ruolo IAM esistente. È necessario utilizzare questa opzione se la condivisione di file si connette ad Amazon S3 utilizzando un alias del punto di accesso.

NellaRuolo IAMbox, inserisci l'Amazon Resource Name (ARN) per il ruolo utilizzato per accedere al bucket. Per informazioni sui ruoli IAM, consulta.Ruoli IAMnellaAWS Identity and Access ManagementGuida per l'utente di.

Per ulteriori informazioni sull'accesso al bucket S3, vedere Concessione dell'accesso a un bucket Amazon S3.

17. PerCrittografia, selezionare il tipo di chiavi di crittografia da utilizzare per crittografare gli oggetti archiviati dal gateway di file in Amazon S3:

    - Per utilizzare la crittografia lato server gestita da Amazon S3 (SSE-S3)Chiavi gestite S3 (SSE-S3).
    - Per utilizzare la crittografia lato server gestita daAWS Key Management Service(SSE-KMS), scegliChiavi gestite KMS (SSE-KMS). NellaChiave primarianella casella, scegliere una esistenteAWS KMS keyoppure scegliCreazione di una nuova chiave KMSper creare una nuova chiave KMS nellaAWS Key Management Service(AWS KMS) console. Per ulteriori informazioni suAWS KMS, consultaChe cos'èAWS Key Management Service?nellaAWS Key Management ServiceGuida per gli sviluppatori.

    > **Note**
    >
    > Per specificare unAWS KMSchiave con un alias che non è elencato o per utilizzare unAWS KMSchiave da un altroAccount AWS, devi utilizzareAWS Command Line Interface(AWS CLI). Per ulteriori informazioni, consultaCreateNFSFileSharenellaAWSRiferimento delle API Storage Gateway. Le chiavi asimmetriche KMS non sono supportate.

18. ScegliereSuccessivoper configurare le impostazioni di accesso ai file.

Per configurare le impostazioni di accesso ai file

1. PerClient consentiti, specificare se consentire o limitare l'accesso di ciascun client alla condivisione di file. Fornire l'indirizzo IP o la notazione CIDR per i client che si desidera consentire. Per informazioni sui client NFS supportati, vedere Client NFS supportati per un gateway file.
2. PerOpzioni di montaggio, specificare le opzioni desiderateLivello di squasheEsportazione come.

   Per Squash level (Livello di Squash), scegliere una delle seguenti opzioni:

- Tutte le squash: Tutti gli accessi degli utenti sono mappati all'ID utente (UID) (65534) e all'ID gruppo (GID) (65534).
- Nessuna zucca di root: Il superuser remoto (root) riceve l'accesso come root.
- Squash radice (impostazione predefinita): L'accesso per il superuser remoto (root) è mappato a UID (65534) e GID (65534).

Per Export as (Esporta come), scegliere una delle opzioni seguenti:

- Lettura-scrittura
- Sola lettura

> **Note**
>
> Per le condivisioni di file montate su un client Microsoft Windows, se si sceglieSola lettura, potrebbe venire visualizzato un messaggio di errore relativo a un errore imprevisto che non permette di creare la cartella. Ignorare questo messaggio.

3. Per File metadata defaults (Impostazioni predefinite dei metadati dei file), è possibile modificare i campi Directory permissions (Autorizzazioni directory), File permissions (Autorizzazioni file), User ID (ID utente) e Group ID (ID gruppo). Per ulteriori informazioni, consultare Modifica dei valori predefiniti dei metadati per la condivisione di file NFS.
4. Scegli Next (Successivo).
5. Rivedere le impostazioni di configurazione della condivisione file, quindi selezionareTermina.

   Dopo aver creato la condivisione file NFS, è possibile vedere le impostazioni di condivisione dei file nella scheda Details (Dettagli) della condivisione dei file.

Fase successiva

Montaggio della condivisione file NFS sul client

Creare una condivisione file SMB

Prima di creare una condivisione di file Server Message Block (SMB), configurare le impostazioni di sicurezza SMB per il gateway di file. Per l'autenticazione, è necessario configurare Microsoft Active

Directory (AD) o l'accesso guest per l'autenticazione. Una condivisione di file offre solo un tipo di accesso SMB. Per istruzioni, consultaModifica delle impostazioni SMB per un gateway.

> **Note**
>
> Una condivisione di file SMB non funziona correttamente a meno che le porte richieste non siano aperte nel gruppo di sicurezza. Per ulteriori informazioni, consultare Requisiti porta.

> **Note**
>
> Quando un file viene scritto sul gateway di file da un client SMB, il gateway di file carica i dati del file su Amazon S3 seguito dai relativi metadati (proprietà, timestamp e così via). Il caricamento dei dati del file crea un oggetto S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto S3. Questo processo crea un'altra versione dell'oggetto, risultando in due versioni di un oggetto. Se la funzione Versioni multiple di S3 è abilitata, vengono memorizzate entrambe le versioni.
> Se si modificano i metadati di un file memorizzato nel gateway di file, viene creato un nuovo oggetto S3 e sostituisce l'oggetto S3 esistente. Questo comportamento è diverso dalla modifica di un file in un file system, in cui la modifica di un file non comporta la creazione di un nuovo file. Verifica tutte le operazioni sui file con cui intendi utilizzareAWSStorage Gateway per capire come ogni operazione di file interagisce con lo storage Amazon S3.
> Considerate attentamente l'uso di S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 quando carichi dati dal gateway di file. Il caricamento di file dal gateway di file su Amazon S3 quando è abilitato S3 Versioning si traduce in almeno due versioni di un oggetto S3.
> Alcuni flussi di lavoro che coinvolgono file di grandi dimensioni e modelli di scrittura di file, come i caricamenti di file eseguiti in diversi passaggi, possono aumentare il numero di versioni di oggetti S3 memorizzati. Se la cache del gateway di file deve liberare spazio a causa dell'elevata velocità di scrittura dei file, è possibile creare più versioni di oggetti S3. Questi scenari aumentano lo storage S3 se il controllo delle versioni di S3 è abilitato e aumentano i costi di trasferimento associati al CRR. Testare tutte le operazioni sui file che prevedi di utilizzare con Storage Gateway in modo da comprendere come ogni operazione di file interagisce con lo storage Amazon S3.
> L'utilizzo dell'utilità Rsync con il gateway di file comporta la creazione di file temporanei nella cache e la creazione di oggetti S3 temporanei in Amazon S3. Questa situazione comporta

addebiti di cancellazione anticipata nelle classi di storage S3 Standard - Infrequent Access (S3 Standard - accesso infrequente) e S3 Intelligent-Tiering.

Creazione di una condivisione file SMB

Per creare una condivisione file SMB

1. Apertura dellaAWSConsole Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home/.
2. ScegliereCreare una condivisione fileper aprireImpostazioni di condivisione file(Certificato creato).
3. Perportale, scegliere Amazon S3 File Gateway dall'elenco.
4. PerPercorso Amazon S3Effettuare una delle seguenti operazioni:

   - Per collegare la condivisione file direttamente a un bucket S3, scegliereNome bucket S3, quindi immettere il nome del bucket e, facoltativamente, un nome di prefisso per gli oggetti creati dalla condivisione file. Il gateway utilizza questo bucket per archiviare e recuperare i file. Per ulteriori informazioni sulla creazione di un nuovo bucket, consultaCome creare un bucket S3?nellaGuida per l'utente di Amazon S3.
   - Per connettere la condivisione di file a un bucket S3 tramite un access point, selezionareAccess point S3, quindi immettere il nome del punto di accesso S3 e, facoltativamente, un nome di prefisso per gli oggetti creati dalla condivisione file. Il criterio del bucket deve essere configurato per delegare il controllo di accesso all'access point. Per ulteriori informazioni sui punti di accesso, consultaGestione dell'accesso ai dati con access point Amazon S3eDelegazione del controllo di accesso agli access pointnellaGuida per l'utente di Amazon S3.
   - Per collegare la condivisione di file a un bucket S3 tramite un alias del punto di accesso, sceglieAlias del punto di accesso S3, quindi immettere il nome dell'alias del punto di accesso S3 e, facoltativamente, un nome di prefisso per gli oggetti creati dalla condivisione file. Se si sceglie questa opzione, il gateway di file non può crearne una nuovaAWS Identity and Access Management(IAM) policy d'accesso e ruolo per conto dell'utente. È necessario selezionare un ruolo IAM esistente e configurare un criterio di accesso nelAccesso al proprio bucket S3sezione che segue. Per ulteriori informazioni sugli alias dell'access point, consultaUtilizzo di un alias in stile bucket per il punto di accessonellaGuida per l'utente di Amazon S3.

> **Note**
>
> - Se si immette un nome di prefisso o si sceglie di connettersi tramite un punto di accesso o un alias del punto di accesso, è necessario immettere un nome di condivisione file.
> - Il nome del prefisso deve terminare con una barra (/).
> - Dopo aver creato la condivisione di file, il nome del prefisso non può essere modificato o eliminato.
> - Per ulteriori informazioni sull'uso di nomi prefissi, consultaOrganizzazione degli oggetti utilizzando i prefissinellaGuida per l'utente di Amazon S3.

5. PerRegione AWS, scegli ilRegione AWSdel bucket S3.
6. PerNome della condivisione file, digitare un nome per la condivisione file. Il nome predefinito è il nome del bucket S3 o il nome del punto di accesso.

> **Note**
>
> - Se si è immesso un nome di prefisso o si è scelto di connettersi tramite un punto di accesso o un alias del punto di accesso, è necessario immettere un nome di condivisione file.
> - Dopo aver creato la condivisione di file, il nome della condivisione file non può essere eliminato.

7. (Opzionale) PerAWS PrivateLinkper S3, eseguire le seguenti operazioni:

    1. Per configurare la condivisione di file per connettersi a S3 tramite un endpoint di interfaccia nel cloud privato virtuale (VPC) basato suAWS PrivateLink, scegliUtilizzo dell'endpoint VPC.
    2. Per identificare l'endpoint dell'interfaccia VPC a cui si desidera connettere la condivisione di file, scegliere unoID endpoint VPCoNome DNS dell'endpoint VPCe quindi fornire le informazioni richieste nel campo corrispondente.

> **Note**
>
> - Questo passaggio è necessario se la condivisione di file si connette a S3 tramite un punto di accesso VPC o tramite un alias associato a un punto di accesso VPC.
> - Utilizzo delle connessioni di condivisione fileAWS PrivateLinknon sono supportati sui gateway FIPS.
> - Per informazioni suAWS PrivateLink, consultaAWS PrivateLinkper Amazon S3nellaDocumentazione su Amazon Simple Storage Service.

8. Per Access Objects using (Accedi agli oggetti utilizzando), selezionare Server Message Block (SMB).
9. Per Registri di controllo, scegliere una delle opzioni seguenti:

   - Per disattivare la registrazione, scegliereDisabilitare la registrazione.
   - Per creare un nuovo registro di controllo, sceglieCrea un nuovo gruppo di log.
   - Per utilizzare un gruppo di log esistente, sceglieUtilizzare un gruppo di log esistente;, quindi scegliere un log di controllo dall'elenco.

   Per ulteriori informazioni sui log di audit, consulta Informazioni sui log di controllo del gateway di file.
10. PerAggiornamento automatico della cache da S3, scegliImpostazione dell'intervallo di aggiornamentoe quindi impostare il tempo in giorni, ore e minuti per aggiornare la cache della condivisione di file utilizzando Time To Live (TTL). Il TTL è il periodo di tempo dall'ultimo aggiornamento. Al termine dell'intervallo TTL, l'accesso alla directory fa sì che il gateway di file aggiorni prima il contenuto di quella directory dal bucket Amazon S3.
11. PerNotifica di caricamento file, scegliTempo di liquidazione (secondi)per ricevere una notifica quando un file è stato completamente caricato su S3 dal gateway di file. Impostazione della proprietàOrario di liquidazionein secondi per controllare il numero di secondi da attendere dopo l'ultimo momento in cui un client ha scritto su un file prima di generare un`ObjectUploaded`notifica. Poiché i client possono eseguire molte piccole scritture su file, è meglio impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in un breve periodo di tempo. Per ulteriori informazioni, consultare Ricevere notifica di caricamento file.

> **Note**
>
> Questa impostazione non ha alcun effetto sulla tempistica del caricamento dell'oggetto su S3, solo sulla tempistica della notifica.

12. (Facoltativo) NelTagsezione, scegliAggiungi nuovo tag, quindi immettere una chiave e un valore per aggiungere tag alla condivisione file. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare la condivisione file.
13. Scegli Next (Successivo). LaImpostazioni di storage di Amazon S3Viene visualizzata la pagina.
14. PerClasse di storage per nuovi oggetti, selezionare una classe di storage da utilizzare per i nuovi oggetti creati nel bucket Amazon S3:

    - Per archiviare i dati degli oggetti ad accesso frequente in modo ridondante in più zone di disponibilità geograficamente distinte, selezionareS3 Standard. Per ulteriori informazioni sulla classe di storage S3 Standard, consultaClassi di storage per oggetti a cui si accede di frequentenellaManuale utente di Amazon Simple Storage Service.
    - Per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più conveniente, selezionareS3 Intelligent-Tiering. Per ulteriori informazioni sulla classe di storage S3 Intelligent-Tiering, consultaLa classe di storage che ottimizza automaticamente gli oggetti con accesso più o meno frequentenellaDocumentazione su Amazon Simple Storage Service.
    - Per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte, selezionareS3 Standard - accesso infrequente. Per ulteriori informazioni sulla classe di storage S3 Standard IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione su Amazon Simple Storage Service.
    - Per archiviare i dati degli oggetti ad accesso poco frequente in un'unica zona di disponibilità, selezionareS3 One Zone-IA. Per ulteriori informazioni sulla classe di storage S3 One Zone-IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione su Amazon Simple Storage Service.

    Per monitorare la fatturazione S3, usaAWS Trusted Advisor. Per ulteriori informazioni, consultaStrumenti di monitoraggionellaDocumentazione su Amazon Simple Storage Service.
15. Per Object metadata (Metadati oggetti), scegliere i metadati da utilizzare:

- Per abilitare il controllo del tipo MIME per gli oggetti caricati in base alle estensioni di file, selezionareTipo MIME Guess.
- Per fornire il controllo completo al proprietario del bucket S3 mappato alla condivisione file SMB, selezionareDare il pieno controllo del proprietario della benna. Per ulteriori informazioni sull'uso della condivisione file per accedere agli oggetti in un bucket di proprietà di un altro account, consultaUtilizzo di una condivisione file per l'accesso tra account.
- Per fornire il controllo completo al proprietario del bucket S3 mappato alla condivisione file SMB, selezionareAbilita il pagamento del richiedente. Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.

16. PerAccesso al proprio bucket S3, scegli ilAWS Identity and Access Management(IAM) ruolo (IAM) che si desidera far utilizzare al gateway di file per accedere al bucket Amazon S3:

    - Per abilitare il gateway file per creare un nuovo ruolo IAM e policy d'accesso per conto dell'utente, selezionareCrea un nuovo ruolo IAM. Questa opzione non è disponibile se la condivisione di file si connette ad Amazon S3 utilizzando un alias del punto di accesso.
    - Per selezionare un ruolo IAM esistente e impostare manualmente i criteri di accesso, selezionareUtilizzare un ruolo IAM esistente. È necessario utilizzare questa opzione se la condivisione di file si connette ad Amazon S3 utilizzando un alias del punto di accesso. NellaRuolo IAMbox, inserisci l'Amazon Resource Name (ARN) per il ruolo utilizzato per accedere al bucket. Per informazioni sui ruoli IAM, consulta.Ruoli IAMnellaAWS Identity and Access ManagementGuida per l'utente di.

    Per ulteriori informazioni sull'accesso al bucket S3, vedere Concessione dell'accesso a un bucket Amazon S3.

17. PerCrittografia, selezionare il tipo di chiavi di crittografia da utilizzare per crittografare gli oggetti archiviati dal gateway di file in Amazon S3:

    - Per utilizzare la crittografia lato server gestita da Amazon S3 (SSE-S3)Chiavi gestite S3 (SSE-S3).
    - Per utilizzare la crittografia lato server gestita daAWS Key Management Service(SSE-KMS), scegliChiavi gestite KMS (SSE-KMS). NellaChiave primarianella casella, scegliere una esistenteAWS KMS keyoppure scegliCreazione di una nuova chiave KMSper creare una nuova chiave KMS nellaAWS Key Management Service(AWS KMS) console. Per ulteriori informazioni suAWS KMS, consultaChe cos'èAWS Key Management Service?nellaAWS Key Management ServiceGuida per gli sviluppatori.

> **Note**
>
> Per specificare unAWS KMSchiave con un alias che non è elencato o per utilizzare unAWS KMSchiave da un altroAccount AWS, devi utilizzareAWS Command Line Interface(AWS CLI). Per ulteriori informazioni, consultaCreateNFSFileSharenellaAWSRiferimento delle API Storage Gateway. Le chiavi asimmetriche KMS non sono supportate.

18. Scegli Next (Successivo). LaImpostazioni di accesso ai fileViene visualizzata la pagina.
19. PerMetodo di autenticazione, scegliere il metodo di autenticazione da utilizzare.

    - Per utilizzare Microsoft AD aziendale per l'accesso autenticato degli utenti alla condivisione file SMB, selezionareActive Directory. Il gateway file deve essere aggiunto a un dominio.
    - Per fornire l'accesso solo agli ospiti, scegliAccesso per gli ospiti. Se si seleziona questo metodo di autenticazione, il gateway di file non deve far parte di un dominio Microsoft AD. È anche possibile usare un gateway di file membro di un dominio AD per creare condivisioni di file con accesso guest. È necessario impostare una password guest per il server SMB nel campo corrispondente.

    > **Note**
    >
    > Entrambi i tipi di accesso sono disponibili nello stesso momento.

20. NellaImpostazioni di condivisione SMBsezione, scegli le tue impostazioni.

    Per Export as (Esporta come), scegliere una delle opzioni seguenti:

    - Lettura-scrittura (valore predefinito)
    - Sola lettura

    > **Note**
    >
    > Per le condivisioni di file montate su un client Microsoft Windows, se si sceglieSola lettura, potrebbe venire visualizzato un messaggio di errore relativo a un errore imprevisto che non permette di creare la cartella. Ignorare questo messaggio.

Per File/directory access controlled by (Accesso file/directory controllato da), scegliere una delle opzioni seguenti:

- Per impostare autorizzazioni granulari su file e cartelle nella condivisione di file SMB, selezionareElenco di controllo accessi di Windows. Per ulteriori informazioni, consultare Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.
- Per utilizzare le autorizzazioni POSIX per controllare l'accesso a file e directory che vengono archiviati tramite una condivisione di file NFS o SMB, selezionareAutorizzazioni POSIX.

Se il metodo di autenticazione èActive Directory, perUtenti/gruppi amministrativi, immettere un elenco separato da virgole di utenti e gruppi AD. Questa operazione se si desidera che l'utente amministratore disponga di privilegi per aggiornare gli elenchi di controllo d'accesso (ACL) su tutti i file e le cartelle nella condivisione di file. Questi utenti e gruppi quindi dispongono dei privilegi di amministratore per la condivisione di file. Un gruppo deve avere il prefisso di@personaggio, ad esempio,`@group1`.

PerDistinzione tra lettere maiuscole e minuscolescegliere una delle opzioni seguenti:

- Per consentire al gateway di controllare la sensibilità delle maiuscole e minuscole, scegliereClient specificato.
- Per consentire al client di controllare la sensibilità tra maiuscole e minuscole, scegliereForza la minuscola.

> **Note**
>
> - Se selezionata, questa impostazione si applica immediatamente alle nuove connessioni client SMB. Le connessioni client SMB esistenti devono disconnettersi dalla condivisione di file e riconnettersi affinché l'impostazione abbia effetto.

PerEnumerazione basata sull'accessoscegliere una delle opzioni seguenti:

- Per rendere visibili i file e le cartelle sulla condivisione solo agli utenti che hanno accesso in lettura, sceglieredisabilitato per file e directory.

- Per rendere visibili i file e le cartelle sulla condivisione a tutti gli utenti durante l'enumerazione della directory, scegliereAbilitato per file e directory.

> **Note**
>
> L'enumerazione basata su accesso è un sistema che filtra l'enumerazione di file e cartelle su una condivisione di file SMB in base agli elenchi di controllo d'accesso (ACL) della condivisione.

PerSerratura opportunistica (oplock)scegliere una delle opzioni seguenti:

- Per consentire alla condivisione di file di utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file, sceglieреEnabled (Abilitato). Nella maggior parte dei casi, l'abilitazione del blocco opportunistico migliora le prestazioni, in particolare per quanto riguarda i menu contestuali di Windows.
- Per evitare l'uso di bloccaggio opportunistico, sceglieреDisabilitato. Se più client Windows nell'ambiente modificano frequentemente gli stessi file contemporaneamente, la disattivazione del blocco opportunistico può a volte migliorare le prestazioni.

> **Note**
>
> Non è consigliabile abilitare il blocco opportunistico sulle condivisioni con distinzione tra maiuscole e minuscole per carichi di lavoro che comportano l'accesso a file con lo stesso nome in casi diversi.

21. (Facoltativo) NelAccesso alla condivisione di file di utenti e gruppisezione, scegli le tue impostazioni.

    PerUtenti e gruppi consentiti, scegliAggiunta di un utente autorizzatooAggiunta del gruppo consentitoe inserisci un utente o gruppo AD che si desidera consentire l'accesso alla condivisione file. Ripetere questo processo per consentire il maggior numero di utenti e gruppi necessari.

    PerUtenti e gruppi negati, scegliAggiunta di un utente negatooAggiunta del gruppo negatoe immettere un utente o un gruppo AD che intendi negare l'accesso alla condivisione file. Ripetere questo processo per negare il numero necessario di utenti e gruppi.

> **Note**
>
> LaAccesso alla condivisione di file di utenti e gruppila sezione viene visualizzata solo seActive Directoryè selezionato.
> Immettere solo il nome dell'utente o del gruppo AD. Il nome di dominio è implicito nell'appartenenza del gateway all'AD specifico a cui il gateway è unito.
> Se non si specificano gli utenti o i gruppi consentiti o negati, qualsiasi utente di AD autenticato può esportare la condivisione file.

22. Scegli Next (Successivo).
23. Rivedere le impostazioni di configurazione della condivisione file, quindi selezionareTermina.

    Dopo aver creato la condivisione file SMB, è possibile vedere le impostazioni di condivisione dei file nella scheda Details (Dettagli) della condivisione dei file.

Fase successiva

Montaggio della condivisione file SMB sul client

Monta e usa la condivisione di file

Di seguito sono riportate le istruzioni dedicate all'utilizzo e al montaggio sul client della condivisione file, alla verifica di gateway file e all'eliminazione di risorse in base alle necessità. Per ulteriori informazioni sui client NFS (Network File System) supportati, consulta Client NFS supportati per un gateway file. Per ulteriori informazioni sui client SMB (Service Message Block) supportati, consulta Client SMB supportati per un gateway file.

Puoi trovare i comandi di esempio per il montaggio della condivisione file sull'AWS Management Console. Le istruzioni dedicate all'utilizzo e al montaggio sul client della condivisione file, alla verifica di gateway di file e all'eliminazione di risorse in base alle necessità sono riportate nelle sezioni seguenti.

Argomenti

Montaggio della condivisione file NFS sul client

Ora è possibile montare la condivisione file NFS su un'unità del client e mapparla al bucket Amazon S3.

Montaggio di una condivisione file e mapparla a un bucket Amazon S3

1. Se si sta utilizzando un client di Microsoft Windows, è consigliabile creare una condivisione file SMB e accedervi usando un client SMB già installato sul client di Windows. Se si utilizza NFS, attivare Servizi per NFS in Windows.
2. Montaggio della condivisione file NFS:

   - Per i client Linux, digitare il comando seguente al prompt dei comandi.

     ```
     sudo mount -t nfs -o nolock,hard [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
     ```

- Per i client MacOS, digitare il comando seguente al prompt dei comandi.

  sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v *[Your gateway VM IP address]*:/*[S3 bucket name] [mount path on your client]*

- Per i client Windows, digitare il comando seguente al prompt dei comandi.

  mount -o nolock -o mtype=hard *[Your gateway VM IP address]*:/*[S3 bucket name] [Drive letter on your windows client]*

Supponiamo che ti avvalga di un client Windows con l'indirizzo IP della VM 123.123.1.2 e il nome del bucket Amazon S3 e che`test-bucket`. voglia mappare la condivisione all'unità T. In questo caso, il comando appare come segue.

mount -o nolock -o mtype=hard 123.123.1.2:/test-bucket T:

> **Note**
>
> Durante il montaggio della condivisione file, tieni presente quanto segue:
>
> - Non è da considerarsi che in un bucket Amazon S3 siano presenti una cartella e un oggetto con lo stesso nome. In tal caso, se il nome dell'oggetto non include una barra finale, solo la cartella risulta visibile in un gateway file. Se, ad esempio, un bucket contiene un oggetto denominato`testotest/`e una cartella denominata`test/test1`, solo`test/etest/test1`sono visibili in un gateway di file.
> - Potrebbe essere necessario rimontare la condivisione file dopo il riavvio del client.
> - Per impostazione predefinita, Windows si avvale di un montaggio soft, per la condivisione NFS; montaggio che, però, ha maggiori probabilità di scadere in caso di problemi di connessione. Consigliamo quindi di avvalersi del montaggio hard, più sicuro e affidabile nel preservare i dati. Il comando di montaggio soft omette lo switch **`-o mtype=hard`**. Il comando di montaggio hard di Windows utilizza lo switch `-o mtype=hard`.
> - Se si utilizzano client Windows, verificare le opzioni `mount` dopo il montaggio eseguendo il comando `mount` senza opzioni. La risposta deve confermare che la condivisione file è stata montata utilizzando le ultime opzioni fornite. Inoltre, deve confermare che non si utilizzano voci precedentemente memorizzate nella cache, che richiedono almeno 60 secondi per essere cancellate.

Fase successiva

Prova il tuo gateway file S3

Montaggio della condivisione file SMB sul client

Ora è possibile montare la condivisione file SMB e mapparla a un'unità accessibile sul client. I comandi di montaggio supportati e utilizzabili per il client SMB sono riportati nella sezione del gateway file. Di seguito puoi trovare ulteriori opzioni disponibili.

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

- Prompt dei comandi (`cmdkeyenet use`) — Utilizzare il prompt dei comandi per il montaggio della condivisione file. Memorizza le tue credenziali con`cmdkey`, quindi montare l'unità con`net use`e includere il kit`/persistent:yese/savecred`cambia se si desidera che la connessione persista durante il riavvio del sistema. I comandi specifici utilizzati saranno diversi a seconda che si desideri montare l'unità per l'accesso Microsoft Active Directory (AD) o l'accesso utente guest. Di seguito sono forniti alcuni esempi.
- Esplora file (Mappa unità di rete): utilizzare Esplora file di Windows per montare la condivisione di file. Configurare le impostazioni per specificare se si desidera che la connessione persiste durante il riavvio del sistema e richiedere le credenziali di rete.
- Script PowerShell: creare uno script PowerShell personalizzato per montare la condivisione di file. A seconda dei parametri specificati nello script, la connessione può essere persistente per il riavvio del sistema e la condivisione può essere visibile o invisibile al sistema operativo mentre è montata.

> **Note**
>
> Se sei un utente Microsoft AD, consulta l'amministratore per verificare di avere accesso alla condivisione file SMB prima di montare la condivisione file sul sistema locale.
> Se sei un utente guest, accertati di avere la password dell'account prima di dedicarti al montaggio della condivisione file.

Per montare la condivisione file SMB per gli utenti autorizzati Microsoft AD con il prompt dei comandi:

1. Accertarsi che l'utente Microsoft AD disponga delle autorizzazioni necessarie per la condivisione file SMB prima di montare la condivisione file sul sistema dell'utente.

2. Immettere quanto segue al prompt dei comandi per il montaggio della condivisione file:

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
persistent:yes
```

Per montare la condivisione file SMB con una combinazione specifica nome utente e password utilizzando il prompt dei comandi:

1. Accertarsi che l'account utente abbia accesso alla condivisione file SMB prima di montarla sul sistema.
2. Immettere quanto segue al prompt dei comandi per salvare le credenziali utente in Windows Credential Manager:

```
cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
```

3. Immettere quanto segue al prompt dei comandi per il montaggio della condivisione file:

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
persistent:yes /savecred
```

Per montare la condivisione file SMB per gli utenti guest con il prompt dei comandi:

1. Accertarsi di avere la password dell'account utente guest prima di montare la condivisione file.
2. Digitare quanto segue al prompt dei comandi per salvare le credenziali guest in Windows Credential Manager:

```
cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
```

3. Digitare quanto segue al prompt dei comandi.

```
net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
ID\smbguest /persistent:yes /savecred
```

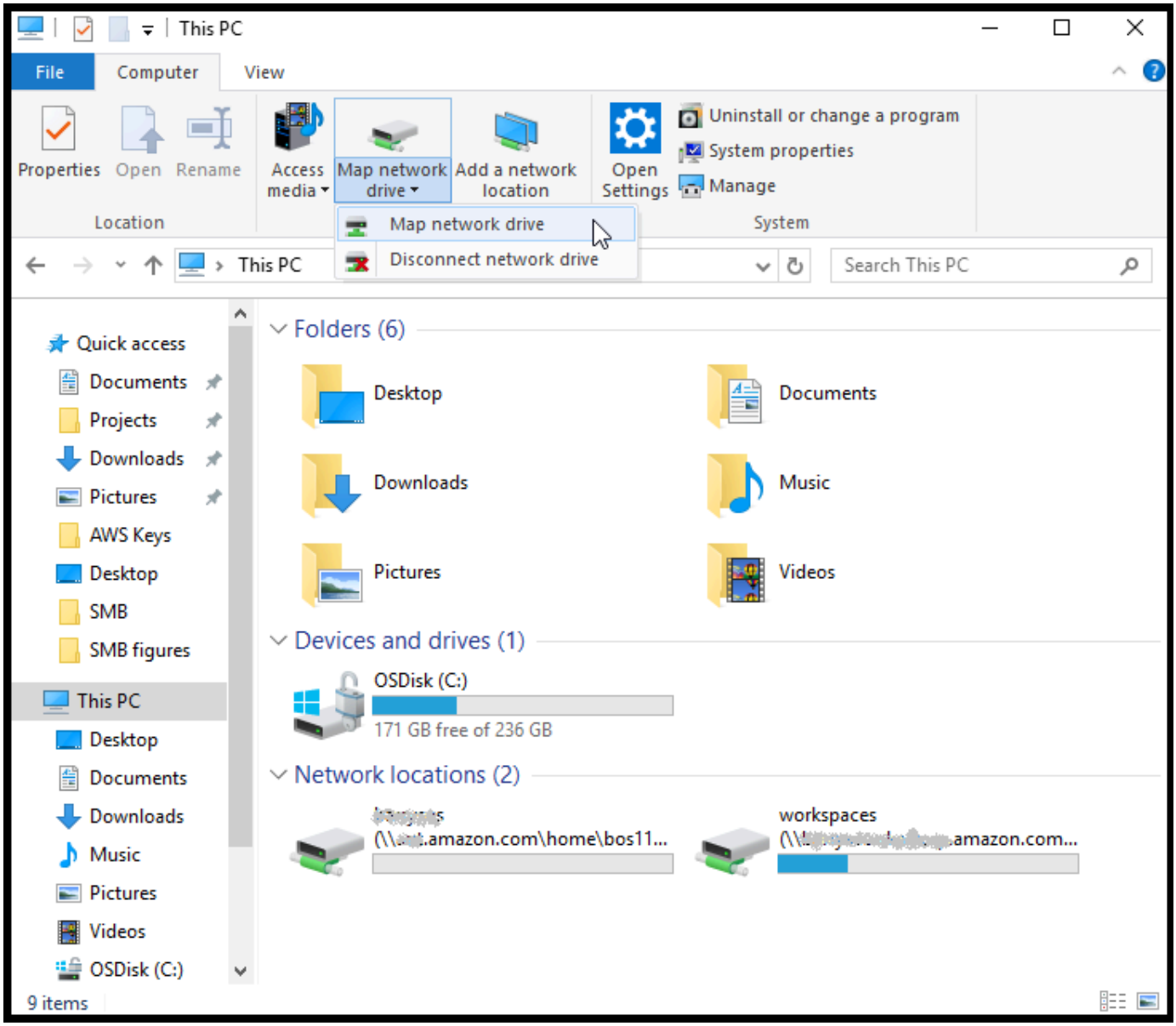
> **Note**
>
> Durante il montaggio della condivisione file, tieni presente quanto segue:
>
> - Non è da considerarsi che in un bucket Amazon S3 siano presenti una cartella e un oggetto con lo stesso nome. In tal caso, se il nome dell'oggetto non include una barra finale, solo

la cartella risulta visibile in un gateway file. Se, ad esempio, un bucket contiene un oggetto denominato`testotest/`e una cartella denominata`test/test1`, solo`test/etest/test1`sono visibili in un gateway di file.

- A meno che non si configuri la connessione di condivisione file per salvare le credenziali utente e persistere durante il riavvio del sistema, potrebbe essere necessario rimuovere la condivisione di file ogni volta che si riavvia il sistema client.

Montaggio di una condivisione file SMB con Esplora file di Windows

1. Premere il tasto Windows e digitare **`File Explorer`** nella casella Cerca in Windows per eseguire la ricerca o premere **`Win+E`**.
2. Nel riquadro di navigazione, selezionare Questo PC; successivamente, scegliere prima Connetti unità di rete e poi, ancora, Connetti unità di rete nella scheda Computer, come mostrato nello screenshot seguente.



3. Nella finestra di dialogo Connetti unità di rete, scegliere una lettera di unità per Unità.
4. Per Cartella, digitare ***[File Gateway IP]**[SMB File Share Name]***, oppure scegliere Sfoglia per selezionare la condivisione 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) Selezionare Connetti con credenziali diverse se si desidera che l'utente immetta la password dell'account guest o di accesso a Microsoft AD.
7. Scegliere Fine per completare il punto di montaggio.

Dalla console di gestione Storage Gateway puoi modificare le impostazioni della condivisione file, gli utenti e i gruppi a cui è consentito o negato l'accesso, nonché la password per l'accesso non autenticato (guest). Inoltre, hai la possibilità di aggiornare i dati nella cache della condivisione file ed eliminare una condivisione file dalla console.

Come modificare le proprietà della condivisione file SMB

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, selezionare File Shares (Condivisioni di file).
3. Nella pagina File Share (Condivisione file), selezionare la casella di controllo della condivisione file SMB da modificare.
4. Tra le Operazioni, scegliere quella desiderata:

   - Selezionare Edit file share settings (Modifica le impostazioni della condivisione file) per modificare l'accesso alla condivisione.
   - Scegliere Edit allowed/denied users (Modifica utenti autorizzati/non autorizzati) per aggiungere o eliminare utenti e gruppi, quindi digitarne i nomi nelle caselle Allowed Users (Utenti autorizzati), Denied Users (Utenti non autorizzati), Allowed Groups (Gruppi autorizzati) e Denied Groups (Gruppi non autorizzati). Utilizzare i pulsanti Add Entry (Aggiungi voce) per concedere nuovi diritti di accesso e la (X) per rimuovere un accesso.
5. Al termine, selezionare Save (Salva).

   Quando specifichi utenti e gruppi autorizzati, crei un elenco di autorizzazioni. Senza un elenco di autorizzazioni, tutti gli utenti autenticati Microsoft AD possono accedere alla condivisione file SMB. Gli utenti e i gruppi contrassegnati come non autorizzati vengono aggiunti a un elenco di negazione e non possono accedere alla condivisione file SMB. Nei casi in cui un utente o un gruppo sia nell'elenco di rifiuto che nell'elenco di autorizzazione, ha la precedenza sull'elenco di negazione.

   È possibile abilitare le liste di controllo degli accessi (ACL) sulla propria condivisione di file SMB. Per informazioni su come abilitare le liste di controllo degli accessi (ACL), consulta Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.

Fase successiva

Prova il tuo gateway file S3

Utilizzo di condivisioni di file su un bucket con oggetti preesistenti

È possibile esportare una condivisione file su un bucket Amazon S3 con oggetti creati all'esterno del gateway file utilizzando NFS o SMB. Quando i client di file system vi accedono, gli oggetti del bucket creati al di fuori del gateway vengono visualizzati come file, sia nel file system NFS sia in quello SMB. Nella condivisione file vengono adoperati l'accesso e le autorizzazioni POSIX (Portable Operating System Interface) standard. I file riscritti in un bucket Amazon S3 acquisiscono le proprietà e i diritti di accesso che assegni loro.

È possibile caricare oggetti in un bucket S3 in qualsiasi momento. Affinché la condivisione file mostri gli oggetti appena aggiunti come file, occorre innanzitutto aggiornare il bucket S3. Per ulteriori informazioni, consultare the section called “Aggiornamento di oggetti nel bucket Amazon S3”.

> **Note**
>
> Avvalersi di più scrittori per un unico bucket Amazon S3 è sconsigliabile. Se comunque intendi farlo, leggi la sezione «Posso avvalermi di più scrittori per il mio bucket Amazon S3?» nellaDomande frequenti su Storage Gateway.

Per assegnare le impostazioni predefinite dei metadati agli oggetti con accesso mediante NFS, consulta Modificare le impostazioni predefinite dei metadati in Gestione di Amazon S3 File Gateway.

Per SMB, è possibile esportare una condivisione utilizzando Microsoft AD o l'accesso guest per un bucket Amazon S3 con oggetti preesistenti. Gli oggetti esportati tramite una condivisione file SMB ereditano la proprietà e le autorizzazioni POSIX dalla directory principale immediatamente superiore. Gli oggetti nella cartella principale ereditano le liste di controllo accessi (ACL) principali. Per l'ACL principale, il proprietario è `smbguest`, le autorizzazioni per i file sono 666 e, infine, le directory sono 777. Quanto scritto si applica a tutte le forme di accesso autenticato (Microsoft AD e guest).

Prova il tuo gateway file S3

Puoi copiare i file e le cartelle sull'unità mappata. I file vengono caricati automaticamente sul bucket Amazon S3.

Caricamento di file da un client Windows su Amazon S3

1. Dal client Windows, accedere all'unità sulla quale è stata montata la condivisione file. Il nome dell'unità è preceduto da quello del bucket S3.

2. Copiare i file o una cartella sull'unità.
3. Nella Console di gestione Amazon S3, accedere al bucket mappato. Le cartelle e i file copiati dovrebbero essere visibili nel bucket Amazon S3 specificato.

   La condivisione file creata può essere visualizzata inCondivisioni filescheda nella schedaAWSConsole di gestione Storage Gateway.

Il client NFS o SMB può scrivere, leggere, eliminare, rinominare e troncare i file.

> **Note**
>
> I gateway di file non supportano la creazione di collegamenti fissi o simbolici in una condivisione file.

In merito al funzionamento dei gateway di file con S3, tieni presente quanto segue:

- Le letture vengono eseguite da una cache read-through, di lettura passante. In altre parole, se non sono disponibili, i dati vengono recuperati da S3 e aggiunti alla cache.
- Le scritture vengono inviate a S3 tramite caricamenti in più parti ottimizzati con l'ausilio di una cache write-back, di riscrittura.
- Le operazioni di lettura e scrittura sono ottimizzate in modo tale che solo le parti richieste o modificate vengano trasferite sulla rete.
- Le eliminazioni rimuovono gli oggetti da S3.
- Le directory vengono gestite come oggetti cartella in S3, utilizzando la stessa sintassi della console Amazon S3. Le directory vuote possono essere rinominate.
- Le prestazioni operative del file system con l'algoritmo ricorsivo (ad esempio, `ls -l`) dipendono dal numero di oggetti nel bucket.

Fase successiva

A questo punto come si può procedere?

A questo punto come si può procedere?

Nelle sezioni precedenti, hai creato e iniziato a utilizzare un gateway di file, dedicandoti, tra l'altro, al montaggio di una condivisione file e alla verifica della configurazione.

Le altre sezioni di questa guida includono informazioni su come eseguire le operazioni seguenti:

- Per la gestione del gateway di file, consulta Gestione di Amazon S3 File Gateway.
- Per l'ottimizzazione del gateway di file, consulta Ottimizzazione delle prestazioni del gateway.
- Per risolvere problemi con il gateway, consulta Risoluzione dei problemi del gateway.
- Per ulteriori informazioni sui parametri Storage Gateway e su come monitorare le prestazioni del gateway, consulta.

Pulizia di risorse non necessarie

Se hai creato un tuo gateway per esercitarti o come test, eliminalo per evitare di incorrere in spese impreviste o non necessarie.

Per eliminare risorse non necessarie

1. Eliminare il gateway, a meno che non si preveda di continuare a utilizzarlo. Per ulteriori informazioni, consultare Eliminazione del gateway tramite la console AWS Storage Gateway e rimozione delle risorse associate.
2. Eliminare la VM Storage Gateway dall'host locale. Se è stato creato un proprio gateway su un'istanza Amazon EC2, terminare l'istanza.

Attivazione di 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. È quindi possibile utilizzare il dispositivo software per il trasferimento dei dati aAWSstorage senza che il gateway comunichiAWSservizi di storage tramite Internet pubblico. Utilizzando il servizio Amazon VPC, è possibile avviareAWSrisorse in una rete virtuale personalizzata. Puoi utilizzare un VPC per controllare le impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni sui VPC, consultaCos'è Amazon VPC?nellaAmazon VPC User Guide.

Per usare un gateway con l'endpoint VPC Storage Gateway nel VPC, è possibile eseguire le operazioni descritte di seguito:

- Utilizzare la console VPC per creare un endpoint VPC per Storage Gateway e per ottenere l'ID endpoint VPC. Specificare questo ID endpoint VPC quando si crea e si attiva il gateway.
- Se attivi un gateway di file, creare un endpoint VPC per Amazon S3. Specificare questo endpoint VPC quando si creano condivisioni di file per il gateway.
- Se attivi un file di gateway, è necessario configurare un proxy HTTP e configurarlo nella console locale della macchina virtuale del gateway. Questo proxy è necessario per i gateway di file locali basati su hypervisor, ad esempio quelli basati su VMware, Microsoft HyperV e KVM (Kernel-based Virtual Machine) Linux. In questi casi, è necessario il proxy per abilitare gli endpoint privati Amazon S3 di accesso al gateway dall'esterno del VPC. Per ulteriori informazioni su come configurare un proxy HTTP, consulta Configurazione di un proxy HTTP

> **Note**
>
> Il gateway deve essere attivato nella stessa regione in cui l'endpoint VPC è stato creato. Per il gateway di file, lo storage Amazon S3 configurato per la condivisione di file deve trovarsi nella stessa regione in cui è stato creato l'endpoint VPC per Amazon S3.

Argomenti

- Creazione di un endpoint VPC per Storage Gateway
- Impostazione e configurazione di un proxy HTTP (solo gateway di file locali)
- Consentire il traffico verso le porte richieste nel proxy HTTP

Creazione di un endpoint VPC per Storage Gateway

Per creare un endpoint VPC, attenersi alle istruzioni seguenti. Se si dispone già di un endpoint VPC per Storage Gateway, è possibile utilizzarlo.

Per creare un endpoint VPC per Storage Gateway

1. Accedere ad AWS Management Console e aprire 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. SulCreazione endpointpagina, scegliereAWSServiziperCategoria dei servizi.
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. Verificare che Enable Private DNS Name (Abilita nome DNS privato) non sia selezionato.
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. Selezionare Create endpoint (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. Trovare la sezione DNS Names (Nomi DNS) e utilizzare il primo nome DNS che non specifica una zona di disponibilità. Il tuo nome DNS sarà come il seguente: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ora che si dispone di un endpoint VPC, è possibile creare il gateway.

> **Important**
>
> Se si crea il gateway di file, è necessario creare un endpoint anche per Amazon S3. Seguire gli stessi passaggi indicati nella sezione Per creare un endpoint VPC per Storage Gateway, ma scegliere`com.amazonaws.us-east-2.s3`invece in Nome servizio. Quindi selezionare la tabella di instradamento a cui si desidera associare l'endpoint S3 invece del gruppo di sicurezza o della sottorete. Per istruzioni, consultaCreazione di un endpoint gateway.

Impostazione e configurazione di un proxy HTTP (solo gateway di file locali)

Se attivi un file di gateway, è necessario impostare un proxy http e configurarlo nella console locale della macchina virtuale del gateway. Questo proxy è necessario affinché il gateway di file locale acceda agli endpoint privati Amazon S3 dall'esterno del VPC. Se si dispone già di un proxy http in Amazon EC2, è possibile utilizzarlo. È necessario, tuttavia, 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

Se non si dispone di un proxy Amazon EC2, utilizzare la procedura seguente per impostare e configurare un proxy HTTP.

Per configurare un server proxy

1. Avvia un'AMI Amazon EC2 Linux. Si consiglia di usare una famiglia di istanze ottimizzate per la rete, ad esempio c5n.large.
2. Utilizzare il comando seguente per installare Squid: **`sudo yum install squid`**. In questo modo viene creato un file di configurazione predefinito in`/etc/squid/squid.conf`.

3. Sostituire i contenuti di questo file config con quanto segue:

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8             # RFC1918 possible internal network
acl localnet src 172.16.0.0/12       # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
```

```
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                    1440       20%        10080
refresh_pattern ^gopher:            1440       0%          1440
refresh_pattern -i (/cgi-bin/|\?) 0             0%          0
refresh_pattern .                              0             20%        4320
```

4. Se non è necessario bloccare il server proxy e non è necessario effettuare alcuna modifica, abilitarlo e avviarlo utilizzando i comandi riportati di seguito. Questi comandi consentono di avviare il server all'accensione.

```
sudo chkconfig squid on
sudo service squid start
```

A questo punto, configurare il proxy http per Storage Gateway affinché venga utilizzato da. Quando si configura il gateway per utilizzare un proxy, utilizzare la porta squid 3128 predefinita. Il file squid.config generato copre tutte le seguenti porte TCP necessarie per impostazione predefinita:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Per utilizzare la console locale della macchina virtuale per configurare il proxy HTTP

1. Accedere alla console locale della VM del gateway. Per ulteriori informazioni su come effettuare l'accesso, consulta Accesso alla console locale del gateway del file.

2. Nel menu principale, scegliere Configurare un proxy HTTP.
3. Nel menu Configuration (Configurazione), scegliere Configure HTTP proxy (Configura proxy HTTP).
4. Fornire il nome host e la porta per il server proxy.

Per informazioni dettagliate su come configurare un proxy HTTP, consulta Configurazione di un proxy HTTP.

Consentire il traffico verso le porte richieste nel proxy HTTP

Se si utilizza un proxy http, assicurarsi di consentire il traffico da Storage Gateway alle destinazioni e alle porte elencate di seguito.

Quando Storage Gateway comunica tramite endpoint pubblici, comunica con i seguenti servizi Storage Gateway.

```
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
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> A seconda del gatewayAWSRegione, sostituiscia *regione* nell'endpoint con la stringa della regione corrispondente. Ad esempio, se si crea un gateway nella regione Stati Uniti occidentali (Oregon), l'endpoint avrà l'aspetto seguente: `storagegateway.us-west-2.amazonaws.com:443`.

Quando Storage Gateway comunica tramite l'endpoint VPC, comunica conAWSservizi tramite più porte sull'endpoint VPC Storage Gateway e sulla porta 443 sull'endpoint privato Amazon S3.

- Porte TCP sull'endpoint VPC dello Storage Gateway.
  - 443, 1026, 1027, 1028, 1031 e 2222
- Porta TCP sull'endpoint S3 privato

- 443

Gestione di Amazon S3 File Gateway

Di seguito sono disponibili informazioni su come gestire le risorse di Amazon S3 File Gateway.

Argomenti

Aggiunta di una condivisione file

Quando il gateway file S3 è attivato e in esecuzione, è possibile aggiungere ulteriori condivisioni file e concedere l'accesso ai bucket Amazon S3. I bucket a cui è possibile concedere l'accesso includono i bucket in un altroAccount AWSrispetto alla condivisione di file. Per ulteriori informazioni su come aggiungere una condivisione file, consulta Creazione di una condivisione file.

Argomenti

Concessione dell'accesso a un bucket Amazon S3

Quando crei una condivisione di file, il gateway di file richiede l'accesso per caricare i file nel bucket Amazon S3 e per eseguire azioni su qualsiasi punto di accesso o endpoint Virtual Private

Cloud (VPC) utilizzato per connettersi al bucket. Per concedere questo accesso, il gateway di file presuppone unAWS Identity and Access Management(IAM) associato a una policy IAM che concede questo accesso.

Il ruolo richiede questa policy IAM e una relazione di trust Security Token Service (STS) per la policy. La policy determina quali operazioni può eseguire il ruolo. Inoltre, il bucket S3 e gli eventuali access point o gli endpoint VPC associati devono includere una policy di accesso che permetta al ruolo IAM di accedervi.

È possibile creare il ruolo e la policy di accesso manualmente oppure possono essere creati per te dal gateway file. Se il gateway file crea la policy per te, la policy contiene un elenco di operazioni S3. Per informazioni su ruoli e autorizzazioni, consultaCreazione di un ruolo per delegare le autorizzazioni a unServizio AWSnellaIAM User Guide.

L'esempio seguente è una policy di trust che consente al gateway file di assumere un ruolo IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se non vuoi che il gateway file crei una policy per conto tuo, puoi creare personalmente la policy e collegarla alla condivisione file. Per ulteriori informazioni su come effettuare tale operazione, consulta Creazione di una condivisione file.

La policy di esempio seguente permette al gateway file di eseguire tutte le operazioni Amazon S3 elencate nella policy. La prima parte dell'istruzione permette l'esecuzione nel bucket S3 denominato `TestBucket` di tutte le operazioni elencate. La seconda parte permette le operazioni elencate su tutti gli oggetti in `TestBucket`.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::TestBucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::TestBucket/*",
            "Effect": "Allow"
        }
    ]
}
```

Il seguente criterio di esempio è simile a quello precedente, ma consente al gateway di file di eseguire le azioni necessarie per accedere a un bucket tramite un punto di accesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
```

```
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:123456789:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Se è necessario collegare la condivisione di file a un bucket S3 tramite un endpoint VPC, vedereLink dell'endpoint per Amazon S3nellaAWS PrivateLinkGuida per l'utente di.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, la rappresentazione cross-service può comportare il problema confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio di chiamata) chiama un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti che ti aiutano a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni che AWS Storage Gateway fornisce un altro servizio alla risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il valore di`aws:SourceArn`deve essere l'ARN dello Storage Gateway a cui è associata la condivisione di file.

Il modo più efficace per proteggersi dal problema confuso dei deputati è quello di utilizzare il`aws:SourceArn`chiave del contesto della condizione globale con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si specificano più risorse, utilizzare la`aws:SourceArn`chiave di condizione del contesto globale con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:servicename::123456789012:*`.

L'esempio seguente mostra come puoi utilizzare la`aws:SourceArn`e`aws:SourceAccount`chiavi di contesto delle condizioni globali in Storage Gateway per prevenire il problema confuso dei deputati.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/
sgw-712345DA"
        }
      }
    }
  ]
}
```

Utilizzo di una condivisione file per l'accesso tra account

Account incrociatoQuando un account Amazon Web Services e gli utenti di tale account dispongono dei diritti di accesso alle risorse che appartengono a un altro account Amazon Web Services. Con i gateway dei file, puoi usare una condivisione file in un account Amazon Web Services per accedere a oggetti in un bucket Amazon S3 appartenente a un account Amazon Web Services differente.

Per usare una condivisione file di proprietà di un account Amazon Web Services per accedere a un bucket S3 in un account Amazon Web Services differente

1. Accertare che il proprietaro del bucket S3 abbia concesso l'accesso al bucket S3 a cui si desidera accedere e agli oggetti nel bucket. Per informazioni su come concedere l'accesso, consultaEsempio 2: Il proprietario del bucket concede autorizzazioni per il bucket multiaccountnellaDocumentazione guida per l'utente di Amazon Simp. Per un elenco delle autorizzazioni richieste, consulta Concessione dell'accesso a un bucket Amazon S3.
2. Accertare che il ruolo IAM utilizzato dalla condivisione file per accedere al bucket S3 includa le autorizzazioni per operazioni quali `s3:GetObjectAcl` e `s3:PutObjectAcl`. Inoltre, verificare che il ruolo IAM includa una policy di attendibilità che consente all'account di assumere quel ruolo IAM. Per un esempio di policy di attendibilità, consulta Concessione dell'accesso a un bucket Amazon S3.

   Se la condivisione file utilizza un ruolo esistente per accedere al bucket S3, è necessario includere le autorizzazioni per le operazioni `s3:GetObjectAcl` e `s3:PutObjectAcl`. Il ruolo richiede inoltre una policy di attendibilità che consente all'account di assumere questo ruolo. Per un esempio di policy di attendibilità, consulta Concessione dell'accesso a un bucket Amazon S3.
3. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
4. Scegliere Give bucket owner full control (Concedi il controllo completo al proprietario del bucket) nelle impostazioni Object metadata (Metadati oggetto) nella finestra di dialogo Configure file share setting (Configura impostazioni di condivisione file).

Una volta creata o aggiornata la condivisione del file per un accesso tra account e una volta caricata la condivisione file in un ambiente locale, è consigliabile testare la configurazione. È possibile eseguire questa operazione elencando contenuti directory o scrivendo file di test e accertando che i file siano visualizzati come oggetti nel bucket S3.

> **Important**
>
> Accertarsi di configurare le policy correttamente per concedere l'accesso a più account all'account utilizzato dalla condivisione file. In caso contrario, gli aggiornamenti ai file mediante le applicazioni nell'ambiente locale non si propagano al bucket Amazon S3 che si sta utilizzando.

Risorse

Per ulteriori informazioni sulle policy d'accesso e sulle liste di controllo accessi, consulta quanto segue:

Linee guida per l'utilizzo delle opzioni disponibili relative alle policy d'accesso predefinitenellaDocumentazione guida per l'utente di Amazon Simp

Panoramica delle liste di controllo accessi (ACL)nellaDocumentazione guida per l'utente di Amazon Simp

Eliminazione di una condivisione file

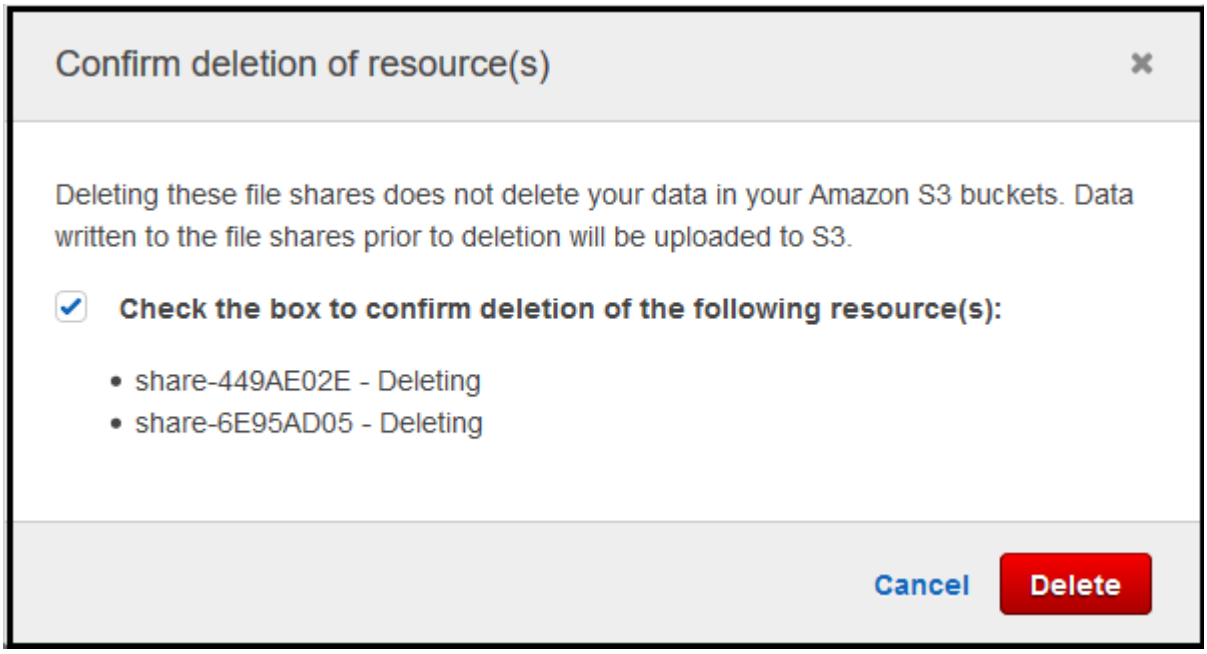
Se una condivisione file non è più necessaria, è possibile eliminarla dalla console di Storage Gateway. Quando elimini una condivisione file, il gateway viene scollegato dal bucket Amazon S3 a cui la condivisione file è mappata. Il bucket S3 e il relativo contenuto non vengono tuttavia eliminati.

Se il gateway sta caricando dati in un bucket S3 quando si elimina una condivisione file, il processo di eliminazione non viene completato finché non sono stati caricati tutti i dati. La condivisione file ha uno stato DELETING (ELIMINAZIONE IN CORSO) fino a quando i dati non sono stati caricati completamente.

Se desideri che i dati vengano caricati completamente, usa la procedura Per eliminare una condivisione file immediatamente seguente. Se non vuoi attendere che i dati vengano caricati completamente, consulta Per forzare l'eliminazione di una condivisione file più avanti in questo argomento.

Per eliminare una condivisione file

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere File shares (Condivisioni di file) e scegliere la condivisione file da eliminare.
3. Per Actions (Operazioni), scegliere Delete file share (Elimina condivisione file). Viene visualizzata la finestra di dialogo di conferma seguente.



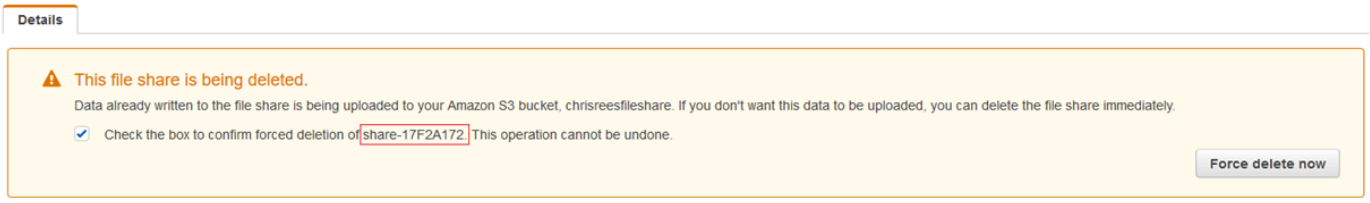
4. Nella finestra di dialogo di conferma selezionare la casella di controllo per la condivisione o le condivisioni di file da eliminare e quindi scegliere Delete (Elimina).

In alcuni casi, è consigliabile non attendere che tutti i dati scritti nei file nella condivisione file NFS (Network File System) vengano caricati prima di eliminare la condivisione file. Ad esempio, potresti voler eliminare intenzionalmente i dati scritti ma non ancora caricati. In un altro esempio, il bucket Amazon S3 o gli oggetti su cui è basata la condivisione file potrebbero essere già stati eliminati, pertanto non è più possibile caricare i dati specificati.

In questi casi, è possibile forzare l'eliminazione della condivisione file utilizzando laAWS Management Consoleo il`DeleteFileShare`Operazione API. Questa operazione interrompe il processo di caricamento dei dati. In tal caso, la condivisione file passa allo stato FORCE_DELETING (ELIMINAZIONE_FORZATA). Per forzare l'eliminazione di una condivisione file dalla console, consulta la procedura seguente.

Per forzare l'eliminazione di una condivisione file

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere File shares (Condivisioni di file), scegliere la condivisione file di cui si vuole forzare l'eliminazione e attendere alcuni secondi. Nella scheda Details (Dettagli) verrà visualizzato un messaggio di eliminazione.



> **Note**
>
> Non è possibile annullare l'operazione di eliminazione forzata.

3. Nel messaggio visualizzato nella scheda Details (Dettagli) verificare l'ID della condivisione file di cui si desidera forzare l'eliminazione, selezionare la casella di conferma e scegliere Force delete now (Forza eliminazione ora).

È anche possibile usare l'operazione API DeleteFileShare per forzare l'eliminazione della condivisione file.

Modifica delle impostazioni per la condivisione file NFS

Puoi modificare la classe di storage per il bucket Amazon S3, il nome della condivisione file, i metadati degli oggetti, il livello di squash, l'esportazione come e le impostazioni di aggiornamento automatico della cache.

> **Note**
>
> Non è possibile modificare una condivisione di file esistente per puntare a un nuovo bucket o punto di accesso o modificare le impostazioni dell'endpoint VPC. È possibile configurare tali impostazioni solo durante la creazione di una nuova condivisione file.

Per modificare le impostazioni della condivisione file

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.
3. PerOperazioni, scegliModifica delle impostazioni di condivisione.
4. Effettuare una o più delle seguenti operazioni:

   - (Opzionale) PerNome della condivisione file, immetti un nuovo nome per la condivisione file.

- Per Registri di controllo, scegliere una delle opzioni seguenti:
  - ScegliereDisabilitare la registrazioneper disattivare la registrazione.
  - ScegliereCrea un nuovo gruppo di logper creare un nuovo registro di controllo.
  - ScegliereUtilizzo di un gruppo di log esistente, poi scegliere un log di controllo esistente dall'elenco.

  Per ulteriori informazioni sui log di audit, consulta Informazioni sui log di controllo del gateway di file.
- (Opzionale) PerAggiornamento automatico della cache da S3, selezionare la casella di controllo e impostare il tempo in giorni, ore e minuti per aggiornare la cache della condivisione file utilizzando Time To Live (TTL). Il TTL è il periodo di tempo dall'ultimo aggiornamento. Dopo che è trascorso l'intervallo TTL, l'accesso alla directory fa sì che il gateway di file venga prima aggiornato il contenuto di quella directory dal bucket Amazon S3.
- (Opzionale) PerNotifica di caricamento file, scegliere la casella di controllo da notificare quando un file è stato completamente caricato su S3 da S3 File Gateway. Impostazione della proprietàPeriodo di liquidazionein secondi per controllare il numero di secondi da attendere dopo l'ultimo momento in cui un client ha scritto su un file prima di generare un`ObjectUploaded`notifica. Poiché i client possono eseguire molte piccole scritture su file, è meglio impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in un breve periodo di tempo. Per ulteriori informazioni, consultare Ricevere notifica di caricamento file.

  > **Note**
  >
  > Questa impostazione non ha alcun effetto sulla tempistica del caricamento dell'oggetto su S3, solo sulla tempistica della notifica.

- PerClasse di storage per nuovi oggetti, selezionare una classe di storage da utilizzare per i nuovi oggetti creati nel bucket Amazon S3:
  - Selezionare S3 Standard per archiviare i dati degli oggetti ad accesso frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Per ulteriori informazioni sulla classe di storage S3 Standard, consultaClassi di storage per oggetti a cui si accede di frequentenellaDocumentazione guida per l'utente di Amazon Simp.
  - Scegli S3 Intelligent-Tiering per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più conveniente. Per ulteriori informazioni sulla classe di storage S3 Intelligent-Tiering, consultaLa classe di storage che ottimizza

automaticamente gli oggetti con accesso più o meno frequentenellaDocumentazione guida per l'utente di Amazon Simp.

- Selezionare S3 Standard-IA per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Per ulteriori informazioni sulla classe di storage S3 Standard IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione guida per l'utente di Amazon Simp.
- Selezionare S3 One Zone-IA per archiviare i dati degli oggetti ad accesso non frequente in una singola zona di disponibilità. Per ulteriori informazioni sulla classe di storage S3 One Zone-IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione guida per l'utente di Amazon Simp.

- Per Object metadata (Metadati oggetti), scegliere i metadati da utilizzare:
  - Scegliere Guess MIME type (Rileva tipo MIME) per abilitare il rilevamento del tipo MIME per gli oggetti caricati in base alle estensioni di file.
  - Scegliere Give bucket owner full control (Concedi il controllo completo al proprietario del bucket) per offrire il controllo al proprietario del bucket S3 mappato alla condivisione file Network File System (NFS) o Server Message Block (SMB) del file. Per ulteriori informazioni sull'uso della condivisione file per accedere agli oggetti in un bucket di proprietà di un altro account, consulta Utilizzo di una condivisione file per l'accesso tra account.
  - Scegliere Enable requester pays (Abilita pagamento a carico del richiedente) se si sta usando la condivisione file in un bucket che richiede il pagamento dei costi di accesso da parte del richiedente o del lettore al posto del proprietario del bucket. Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.
- Per Squash level (Livello squash), scegliere l'impostazione del livello di squash da usare per la condivisione file NFS e quindi scegliere Save (Salva).

> **Note**
>
> È possibile scegliere un'impostazione del livello di squash solo per le condivisioni file NFS. Le condivisioni file SMB non usano le impostazioni di squash.

I valori possibili sono i seguenti:

- Root squash (Squash root) (impostazione predefinita): l'accesso per il superuser remoto (root) è mappato a UID (65534) e GID (65534).

- No root squash (Nessuno squash root): il superuser remoto (root) riceve l'accesso come root.
- All squash (Squash completo): l'accesso di tutti gli utenti è mappato a UID (65534) e GID (65534).

Il valore predefinito per il livello di squash è Root squash (Squash root).

- PerEsporta come, scegliere un'opzione per la condivisione file. Il valore predefinito è Read-write (Lettura-scrittura).

> **Note**
>
> Per le condivisioni di file montate su un client Microsoft Windows, se si seleziona Read-only (Sola lettura) per Export as (Esporta come), potrebbe venire visualizzato un messaggio di errore relativo a un errore imprevisto che non permette di creare la cartella. Questo messaggio di errore è un problema noto di NFS versione 3. È possibile ignorare il messaggio.

5. Scegli Salva.

Modifica dei valori predefiniti dei metadati per la condivisione di file NFS

Se non si impostano i valori dei metadati per i file o le directory nel bucket, il gateway file S3 imposta i valori dei metadati predefiniti. Questi valori includono le autorizzazioni Unix per file e cartelle. È possibile modificare i valori predefiniti dei metadati nella console di Storage Gateway.

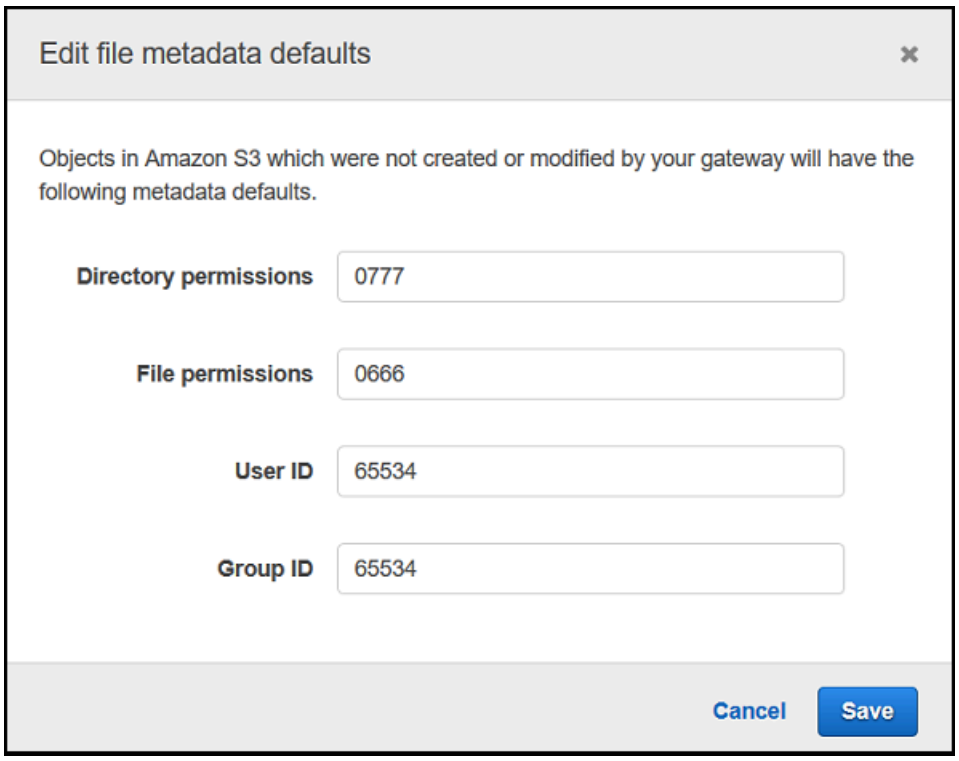
Quando il gateway file S3 archivia i file e le cartelle in Amazon S3, le autorizzazioni dei file Unix vengono archiviate nei metadati degli oggetti. Quando il gateway file S3 individua oggetti che non sono stati archiviati dal gateway file S3, a questi oggetti vengono assegnate le autorizzazioni dei file Unix predefinite. Le autorizzazioni Unix predefinite sono indicate nella tabella seguente.

Metadati	Descrizione
Autorizzazioni directory	Modalità di directory Unix nel formato "nnnn". Ad esempio, "0666" rappresenta la modalità di

Metadati	Descrizione
	accesso per tutte le directory all'interno della condivisione file. Il valore predefinito è 0777.
Autorizzazioni di file	Modalità di file Unix nel formato "nnnn". Ad esempio, "0666" rappresenta la modalità di file all'interno della condivisione file. Il valore predefinito è 0666.
ID utente	ID del proprietario predefinito per i file nella condivisione file. Il valore predefinito è 65534.
ID gruppo	ID del gruppo predefinito per la condivisione file. Il valore predefinito è 65534.

Per modificare le impostazioni predefinite dei metadati

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.
3. Per Actions (Operazioni), scegliere Edit file metadata defaults (Modifica le impostazioni predefinite dei metadati dei file).
4. Nella finestra di dialogo Edit file metadata defaults (Modifica le impostazioni predefinite dei metadati dei file) specificare le informazioni dei metadati e scegliere Save (Salva).



Modifica delle impostazioni di accesso per la condivisione di file NFS

È consigliabile modificare le impostazioni dei client NFS consentiti per la condivisione file NFS. In caso contrario, qualsiasi client nella rete può montare la condivisione file.

Per modificare le impostazioni di accesso NFS

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file NFS da modificare.
3. Per Actions (Operazioni), scegliere Edit share access settings (Modifica impostazioni accesso condivisione).
4. NellaModifica dei client consentitifinestra di dialogo, scegliereAggiungi voce, specificare l'indirizzo IP o la notazione CIDR per i client che si desidera consentire e quindi scegliereSave (Salva).

Modifica delle impostazioni SMB per un gateway

Le impostazioni SMB a livello di gateway consentono di configurare la strategia di sicurezza, l'autenticazione di Active Directory, l'accesso guest, le autorizzazioni dei gruppi locali e la visibilità della condivisione di file per le condivisioni di file SMB su un gateway.

Per modificare le impostazioni SMB a livello gateway

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. ScegliereGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, sceglioreModificare le impostazioni SMBe quindi scegliere le impostazioni da modificare.

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- Impostazione di un livello di sicurezza per il gateway
- Utilizzo di Active Directory per autenticare gli utenti
- Fornire accesso guest alla condivisione di file
- Configurazione di gruppi locali per il gateway
- Impostazione della visibilità della condivisione file

Impostazione di un livello di sicurezza per il gateway

Utilizzando un gateway di file S3, è possibile specificare un livello di sicurezza per il gateway. Specificando questo livello di sicurezza, è possibile indicare se il gateway deve richiedere la firma SMB (Server Message Block) o la crittografia SMB oppure se si desidera abilitare SMB versione 1.

Per configurare il livello di sicurezza

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. SceglieGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, sceglioreModificare le impostazioni SMB, quindi sceglilmpostazioni di sicurezza SMB.
4. Per Security level (Livello di sicurezza), selezionare una delle opzioni seguenti:

> **Note**
>
> Questa impostazione viene chiamata `SMBSecurityStrategy` nel riferimento API. Un più elevato livello di sicurezza può avere ripercussioni sulle prestazioni.

- Applica la crittografia— Se si sceglie questa opzione, S3 File Gateway consente solo connessioni da client SMBv3 con crittografia abilitata. Questa opzione è altamente consigliata per gli ambienti che gestiscono dati sensibili. Questa opzione funziona nei client SMB con Microsoft Windows 8 e Windows Server 2012 o versione più recente.
- Applica la firma— Se si sceglie questa opzione, S3 File Gateway consente solo connessioni da client SMBv2 o SMBv3 con firma abilitata. Questa opzione funziona nei client SMB con Microsoft Windows Vista e Windows Server 2008 o versione più recente.
- Negoziato cliente— Se si sceglie questa opzione, le richieste vengono stabilite in base a ciò che viene negoziato dal client. Questa opzione è consigliata quando si desidera massimizzare la compatibilità tra diversi client nel proprio ambiente.

> **Note**
>
> Per i gateway attivati prima del 20 giugno 2019, il livello di sicurezza predefinito è Client negotiated (Negoziato dal cloud).
> Per i gateway attivati a partire dal 20 giugno 2019, il livello di sicurezza predefinito è Enforce encryption (Applica crittografia).

5. Scegli Salva.

Utilizzo di Active Directory per autenticare gli utenti

Per usare l'istanza di Active Directory aziendale per l'accesso autenticato degli utenti alla condivisione file SMB, modifica le impostazioni SMB per il gateway con le credenziali del dominio Microsoft AD. In questo modo, il gateway può essere aggiunto al dominio di Active Directory e i membri del dominio possono accedere alla condivisione file SMB.

> **Note**
>
> Utilizzo diAWS Directory Service, è possibile creare un servizio di dominio di Active Directory ospitato nellaCloud AWS.

Chiunque fornisca la password corretta, ottiene l'accesso guest alla condivisione file SMB.

È anche possibile abilitare le liste di controllo degli accessi (ACL) sulla propria condivisione di file SMB. Per informazioni su come abilitare le liste di controllo degli accessi (ACL), consulta Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.

Per abilitare l'autenticazione di Active Directory

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. ScegliereGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, sceglieреModificare le impostazioni SMB, quindi scegliImpostazioni di Active Directory.
4. Per Domain name (Nome dominio), specificare il dominio a cui aggiungere il gateway. È possibile partecipare a un dominio utilizzando il suo indirizzo IP o la sua unità organizzativa. Un'unità organizzativa è una suddivisione della Active Directory che può contenere utenti, gruppi, computer e altre unità organizzative.

   > **Note**
   >
   > Se il gateway non è in grado di unirsi a una directory di Active Directory, provare ad aggiungerlo con l'indirizzo IP della directory tramite l'operazione API JoinDomain.

   > **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.

5. Specificare utente di dominio e password di dominio e quindi scegliere Save (Salva).

   Un messaggio nella parte superiore della sezione Gateways (Gateway) della console indica che il gateway è stato aggiunto al dominio AD.

Per limitare l'accesso alla condivisione file a utenti e gruppi AD specifici

1. Nella console Storage Gateway, selezionare la condivisione file a cui si desidera limitare l'accesso.
2. DaOperazionimenu a discesa, scegliereModifica le impostazioni di accesso alla condivisione file.
3. NellaAccesso alla condivisione di file di utenti e gruppisezione, scegli le tue impostazioni.

   PerUtenti e gruppi consentiti, scegliAggiunta di un utente consentitooAggiunta del gruppo consentitoe immettere un utente o un gruppo AD che desideri consentire l'accesso alla condivisione file. Ripetere questo processo per consentire il maggior numero di utenti e gruppi necessari.

   PerUtenti e gruppi negati, scegliAggiunta di un utente negatooAggiunta del gruppo negatoe immettere un utente o un gruppo AD che si desidera negare l'accesso alla condivisione file. Ripetere questo processo per negare il numero necessario di utenti e gruppi.

   > **Note**
   >
   > LaAccesso alla condivisione di file di utenti e gruppila sezione viene visualizzata solo seActive Directoryè selezionato.
   > Immettere solo il nome dell'utente o del gruppo AD. Il nome di dominio è implicito nell'appartenenza del gateway all'AD specifico a cui il gateway è unito.
   > Se non si specificano gli utenti o i gruppi consentiti o negati, qualsiasi utente di AD autenticato può esportare la condivisione file.

4. Una volta completata l'aggiunta di voci, scegliere Save (Salva).

Fornire accesso guest alla condivisione di file

Se si desidera offrire solo l'accesso guest, il gateway file S3 non deve far parte di un dominio di Microsoft AD. È anche possibile usare un gateway file S3 membro di un dominio AD per creare condivisioni file con accesso guest. Prima di creare una condivisione di file con l'accesso guest, è necessario modificare la password predefinita.

Per modificare la password di accesso guest

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.

2. ScegliereGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, sceglieModificare le impostazioni SMB, quindi sceglieImpostazioni di accesso visitatori.
4. PerPassword guest, fornire una password e quindi sceglieSave (Salva).

Configurazione di gruppi locali per il gateway

Le impostazioni del gruppo locale consentono di concedere agli utenti o ai gruppi di Active Directory autorizzazioni speciali per le condivisioni di file SMB sul gateway.

È possibile utilizzare le impostazioni del gruppo locale per assegnare le autorizzazioni di amministrazione del gateway. Gli amministratori gateway possono utilizzare lo snap-in Microsoft Management Console cartelle condivise per chiudere forzatamente i file aperti e bloccati.

> **Note**
>
> È necessario aggiungere almeno un utente o un gruppo Gateway Admin prima di poter unire il gateway a un dominio Active Directory.

Per assegnare Gateway Admins

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. ScegliereGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, sceglieModificare le impostazioni SMB, quindi sceglieImpostazioni gruppo locale.
4. NellaImpostazioni gruppo localesezione, scegli le tue impostazioni. Questa sezione viene visualizzata solo per le condivisioni di file che utilizzano Active Directory.

   PerAmministratori gateway, aggiungere utenti e gruppi di Active Directory a cui si desidera concedere le autorizzazioni locali di amministrazione del gateway. Aggiungi un utente o un gruppo per riga, incluso il nome di dominio. Ad esempio, **`corp\Domain Admins`**. Per creare righe aggiuntive, sceglieAggiungi nuovo amministratore del gateway.

   > **Note**
   >
   > Editing Gateway Admins disconnette e ricollega tutte le condivisioni di file SMB.

5. ScegliereSalva le modifiche, quindi scegliereProcediper riconoscere il messaggio di avviso visualizzato.

Impostazione della visibilità della condivisione file

La visibilità della condivisione file controlla se le condivisioni di un gateway sono visibili quando si elencano le condivisioni agli utenti.

Per impostare la visibilità della condivisione di file

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.
2. ScegliereGateway, poi scegliere il gateway per cui desideri modificare le impostazioni delle PMI.
3. DaOperazionimenu a discesa, scegliereModificare le impostazioni SMB, quindi scegliereImpostazioni di visibilità della condivisione file.
4. PerVisibility status, selezionare la casella di controllo per visualizzare le condivisioni su questo gateway quando elenca le condivisioni agli utenti. Mantieni la casella di controllo deselezionata per far sì che le condivisioni su questo gateway non vengano visualizzate quando elenca le condivisioni agli utenti.

Modifica delle impostazioni per la condivisione file SMB

Dopo aver creato una condivisione di file SMB, puoi modificare la classe di storage per il bucket Amazon S3, i metadati degli oggetti, la distinzione tra maiuscole e minuscole, l'enumerazione basata sull'accesso, i registri di controllo, l'aggiornamento automatico della cache e l'esportazione come impostazioni per la condivisione di file.

> **Note**
>
> Non è possibile modificare una condivisione di file esistente per puntare a un nuovo bucket o punto di accesso o modificare le impostazioni dell'endpoint VPC. È possibile configurare tali impostazioni solo durante la creazione di una nuova condivisione file.

Per modificare le impostazioni di condivisione di file SMB

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.

2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file da aggiornare.
3. PerOperazioni, scegliModifica delle impostazioni di condivisione.
4. Effettuare una o più delle seguenti operazioni:

   - (Opzionale) PerNome della condivisione file, immetti un nuovo nome per la condivisione file.
   - Per Registri di controllo, scegliere una delle opzioni seguenti:
     - ScegliereDisabilitare la registrazioneper disattivare la registrazione.
     - SceglieCrea un nuovo gruppo di logper creare un nuovo registro di controllo.
     - SceglieUtilizzo di un gruppo di log esistente, poi scegliere un log di controllo esistente dall'elenco.

     Per ulteriori informazioni sui log di audit, consulta Informazioni sui log di controllo del gateway di file.
   - (Opzionale) PerAggiornamento automatico della cache da S3 dopo, selezionare la casella di controllo e impostare il tempo in giorni, ore e minuti per aggiornare la cache della condivisione file utilizzando Time To Live (TTL). Il TTL è il periodo di tempo dall'ultimo aggiornamento. Dopo che è trascorso l'intervallo TTL, l'accesso alla directory fa sì che il gateway di file venga prima aggiornato il contenuto di quella directory dal bucket Amazon S3.
   - (Opzionale) PerNotifica di caricamento file, scegliere la casella di controllo da notificare quando un file è stato completamente caricato su S3 da S3 File Gateway. Impostazione della proprietàPeriodo di liquidazionein secondi per controllare il numero di secondi da attendere dopo l'ultimo momento in cui un client ha scritto su un file prima di generare un`ObjectUploaded`notifica. Poiché i client possono eseguire molte piccole scritture su file, è meglio impostare questo parametro il più a lungo possibile per evitare di generare più notifiche per lo stesso file in un breve periodo di tempo. Per ulteriori informazioni, consultare Ricevere notifica di caricamento file.

     > **Note**
     >
     > Questa impostazione non ha alcun effetto sulla tempistica del caricamento dell'oggetto su S3, solo sulla tempistica della notifica.

   - PerClasse di storage per nuovi oggetti, selezionare una classe di storage da utilizzare per i nuovi oggetti creati nel bucket Amazon S3:
     - Selezionare S3 Standard per archiviare i dati degli oggetti ad accesso frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Per ulteriori informazioni

sulla classe di storage S3 Standard, consultaClassi di storage per oggetti a cui si accede di frequentenellaDocumentazione guida per l'utente di Amazon Simp.

- Scegli S3 Intelligent-Tiering per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più conveniente. Per ulteriori informazioni sulla classe di storage S3 Intelligent-Tiering, consultaLa classe di storage che ottimizza automaticamente gli oggetti con accesso più o meno frequentenellaDocumentazione guida per l'utente di Amazon Simp.
- Selezionare S3 Standard-IA per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Per ulteriori informazioni sulla classe di storage S3 Standard IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione guida per l'utente di Amazon Simp.
- Selezionare S3 One Zone-IA per archiviare i dati degli oggetti ad accesso non frequente in una singola zona di disponibilità. Per ulteriori informazioni sulla classe di storage S3 One Zone-IA, consultaClassi di storage per oggetti a cui si accede raramentenellaDocumentazione guida per l'utente di Amazon Simp.

- Per Object metadata (Metadati oggetti), scegliere i metadati da utilizzare:
  - Scegliere Guess MIME type (Rileva tipo MIME) per abilitare il rilevamento del tipo MIME per gli oggetti caricati in base alle estensioni di file.
  - Scegliere Give bucket owner full control (Concedi il controllo completo al proprietario del bucket) per offrire il controllo al proprietario del bucket S3 mappato alla condivisione file Network File System (NFS) o Server Message Block (SMB) del file. Per ulteriori informazioni sull'uso della condivisione file per accedere a oggetti in un bucket di proprietà di un altro account, consultaUtilizzo di una condivisione file per l'accesso tra account.
  - Scegliere Enable requester pays (Abilita pagamento a carico del richiedente) se si sta usando la condivisione file in un bucket che richiede il pagamento dei costi di accesso da parte del richiedente o del lettore al posto del proprietario del bucket. Per ulteriori informazioni, consulta Bucket con pagamento a carico del richiedente.
- PerEsporta come, scegliere un'opzione per la condivisione file. Il valore predefinito è Read-write (Lettura-scrittura).

> **Note**
>
> Per le condivisioni di file montate su un client Microsoft Windows, se si selezionaSola letturaperEsporta come, potrebbe venire visualizzato un messaggio di errore relativo

a un errore imprevisto che non permette di creare la cartella. Questo messaggio di errore è un problema noto di NFS versione 3. È possibile ignorare il messaggio.

- Per File/directory access controlled by (Accesso file/directory controllato da), scegliere una delle opzioni seguenti:
  - Windows Access Control List (Lista di controllo accessi Windows) per impostare autorizzazioni specifiche per i file e le cartelle nella condivisione di file SMB. Per ulteriori informazioni, consultare Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.
  - Selezionare POSIX permissions (Autorizzazioni POSIX) da utilizzare per il controllo dell'accesso ai file e alle directory che vengono archiviati tramite una condivisione di file NFS o SMB.

  Se il metodo di autenticazione èActive Directory, perUtenti/gruppi amministrativi, immettere un elenco separato da virgole di utenti e gruppi AD. Eseguire questa operazione se si desidera che l'utente amministratore disponga di privilegi per aggiornare le ACL su tutti i file e tutte le cartelle nella condivisione file. Questi utenti e gruppi quindi dispongono dei privilegi di amministratore per la condivisione di file. Un gruppo deve avere il prefisso del@personaggio, ad esempio,`@group1`.
- PerDistinzione tra lettere maiuscole e minuscole, selezionare la casella di controllo per consentire al gateway di controllare la distinzione tra maiuscole e minuscole oppure deselezionare la casella di controllo per consentire al client di controllare la maiuscola.

  > **Note**
  >
  > - Se si seleziona questa casella di controllo, questa impostazione si applica immediatamente alle nuove connessioni client SMB. Le connessioni client SMB esistenti devono disconnettersi dalla condivisione di file e riconnettersi affinché l'impostazione abbia effetto.
  > - Se si deseleziona questa casella di controllo, questa impostazione potrebbe causare la perdita dell'accesso ai file con nomi diversi solo nel loro caso.
- PerEnumerazione basata su accesso, selezionare la casella di controllo per rendere visibili i file e le cartelle della condivisione solo agli utenti che hanno accesso in lettura. Mantenere la casella di controllo deselezionata per rendere visibili i file e le cartelle della condivisione a tutti gli utenti durante l'enumerazione della directory.

> **Note**
>
> L'enumerazione basata su accesso è un sistema che filtra l'enumerazione di file e cartelle su una condivisione di file SMB in base agli elenchi di controllo d'accesso (ACL) della condivisione.

- PerSerratura opportunistica (oplock), scegliere una delle opzioni seguenti:
  - ScegliereEnabled (Abilitato)per consentire alla condivisione di file di utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file, migliorando le prestazioni nella maggior parte dei casi, in particolare per quanto riguarda i menu contestuali di Windows.
  - SceglieriDisabilitatoper evitare l'uso di bloccaggio opportunistico. Se più client Windows nell'ambiente modificano frequentemente gli stessi file contemporaneamente, la disattivazione del blocco opportunistico può a volte migliorare le prestazioni.

> **Note**
>
> Non è consigliabile abilitare il blocco opportunistico sulle condivisioni con distinzione tra maiuscole e minuscole per carichi di lavoro che comportano l'accesso a file con lo stesso nome in casi diversi.

5. Scegli Save changes (salva modifiche).

Aggiornamento di oggetti nel bucket Amazon S3

Mentre il client NFS o SMB esegue le operazioni del file system, il gateway gestisce un inventario degli oggetti nel bucket S3 associati alla condivisione file. Il gateway usa questo inventario memorizzato nella cache per ridurre la latenza e la frequenza delle richieste S3. Questa operazione non importa i file nell'archivio cache di S3 File Gateway. Aggiorna solo l'inventario memorizzato nella cache per riflettere le modifiche nell'inventario degli oggetti nel bucket S3.

Per aggiornare il bucket S3 per la condivisione file, è possibile usare la console Storage Gateway, laRefreshCacheoperazione nell'API Storage Gateway o inAWS Lambdafunzione.

Per aggiornare gli oggetti in un bucket S3 dalla console

1. Aprire la console Storage Gateway suhttps://console.aws.amazon.com/storagegateway/home.

2. Scegliere File shares (Condivisioni di file) e quindi scegliere la condivisione file associata al bucket S3 da aggiornare.
3. Per Actions (Operazioni), scegliere Refresh cache (Aggiorna cache).

   Il tempo richiesto dal processo di aggiornamento dipende dal numero di oggetti memorizzati nella cache del gateway e dal numero di oggetti che sono stati aggiunti o rimossi dal bucket S3.

Per aggiornare gli oggetti in un bucket S3 utilizzando unAWS Lambdafunzione

1. Identificare il bucket S3 utilizzato da S3 File Gateway.
2. Controlla che ilEventoLa sezione è vuota. Si compila automaticamente in un secondo momento.
3. Crea un ruolo IAM e consenti di Trust Relationship per Lambda`lambda.amazonaws.com`.
4. Utilizzare la policy seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Creazione di una funzione Lambda dalla console Lambda.
6. Utilizzare la seguente funzione per l'attività Lambda.

```
import json
```

```
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406774878:share/
share-E51FBD9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. PerRuolo di esecuzione, scegliere il ruolo IAM creato.
8. Facoltativo: aggiungi un trigger per Amazon S3 e seleziona l'eventoObjectCreatedoObjectRemoved.

> **Note**
>
> `RefreshCache`deve completare un processo prima di iniziare un altro. Quando crei o elimini molti oggetti in un bucket, le prestazioni potrebbero peggiorare. Pertanto, si consiglia di non utilizzare i trigger S3. Invece, usa la regola Amazon CloudWatch descritta di seguito.

9. Crea una regola CloudWatch sulla console CloudWatch e aggiungi una pianificazione. In generale, raccomandiamo untariffa fissaDi 30 minuti. Tuttavia, è possibile utilizzare 1-2 ore su un grande secchio S3.
10. Aggiungi un nuovo trigger per gli eventi CloudWatch e scegli la regola appena creata.
11. Salva la tua configurazione Lambda. Scegli Test (Esegui test).
12. ScegliereS3 METTEREe personalizza il test in base alle tue esigenze.
13. Il test dovrebbe avere successo. In caso contrario, modificare il JSON in base alle proprie esigenze e ripetere il test.
14. Apri la console Amazon S3 e verifica che l'evento creato e la funzione Lambda ARN siano presenti.
15. Caricamento di un oggetto nel bucket S3 tramite la console Amazon S3 o ilAWS CLI.

    La console CloudWatch genera un output CloudWatch simile al seguente.

```
{
    u'Records': [
```

```
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-
NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}}, u's3SchemaVersion':
 u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

L'invocazione Lambda offre un output simile a quello riportato di seguito.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

La tua condivisione NFS montata sul tuo client rifletterà questo aggiornamento.

> **Note**
>
> Per le cache che aggiornano la creazione o l'eliminazione di oggetti di grandi dimensioni in bucket di grandi dimensioni con milioni di oggetti, gli aggiornamenti potrebbero richiedere ore.

16. Eliminazione manuale dell'oggetto utilizzando la console Amazon S3 oAWS CLI.

17. Visualizza la condivisione NFS montata sul tuo client. Verifica che il tuo oggetto non sia andato (perché la cache è stata aggiornata).
18. Controlla i registri di CloudWatch per vedere il registro della tua eliminazione con l'evento`ObjectRemoved:Delete`.

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> Per i lavori cron o le attività pianificate, il tuo evento di log di CloudWatch è`u'detail-type': u'Scheduled Event'`.

L'aggiornamento della cache avvia solo l'operazione di aggiornamento. Quando l'aggiornamento della cache termina, non significa necessariamente l'aggiornamento dei file sia stato completato. Per stabilire se l'operazione di aggiornamento dei file sia completa prima di verificare la presenza di nuovi file sulla condivisione file del gateway, utilizzare la notifica `refresh-complete`. Per farlo, puoi abbonarti per ricevere una notifica tramite un evento Amazon CloudWatch quando ilRefreshCacheoperazione completata. Per ulteriori informazioni, consultare Ricevere notifiche sulle operazioni di file.

Utilizzo di S3 Object Lock con un gateway di file Amazon S3

Amazon S3 File Gateway supporta l'accesso ai bucket S3 che hanno Amazon S3 Object Lock abilitato. Amazon S3 Object Lock consente di archiviare gli oggetti usando il modello «Write Once Read Many» (WORM). Quando si utilizza il blocco oggetti Amazon S3, puoi impedire che un oggetto nel bucket S3 venga eliminato o sovrascritto. Amazon S3 Object Lock lavora insieme al controllo delle versioni degli oggetti per proteggere i dati.

Se abiliti il blocco oggetti Amazon S3, puoi comunque modificare l'oggetto. Ad esempio, questo può essere scritto, eliminato o rinominato tramite una condivisione file su un gateway file S3. Quando

si modifica un oggetto in questo modo, S3 File Gateway inserisce una nuova versione dell'oggetto senza modificare la versione precedente (ovvero l'oggetto bloccato).

Ad esempio, se si utilizza l'interfaccia NFS o SMB di file S3 per eliminare un file e il corrispondente oggetto S3 è bloccato, il gateway inserisce un contrassegno di eliminazione S3 come versione successiva dell'oggetto e lascia invariata la versione originale. Analogamente, se un gateway file S3 modifica il contenuto o i metadati di un oggetto bloccato, viene caricata una nuova versione dell'oggetto con le modifiche, ma la versione bloccata originale dell'oggetto rimane invariata.

Per ulteriori informazioni sul blocco degli oggetti Amazon S3, consultaBlocco di oggetti tramite il blocco oggetti S3nellaDocumentazione guida per l'utente di Amazon Simp.

Informazioni sullo stato della condivisione file

Ogni condivisione file ha uno stato associato che indica chiaramente l'integrità della condivisione. Nella maggior parte dei casi, lo stato indica che la condivisione file funziona correttamente e che non è richiesta alcuna operazione. In alcuni casi, lo stato indica un problema che potrebbe richiedere un'operazione da parte tua.

È possibile visualizzare lo stato della condivisione file nella console di Storage Gateway. Lo stato della condivisione file è indicato nella colonna Status (Stato) per ogni condivisione file nel gateway. Una condivisione file che funziona normalmente ha lo stato AVAILABLE (DISPONIBILE).

Nella tabella seguente vengono fornite le descrizioni per ciascuno stato della condivisione file e viene indicato se per lo stato specifico è necessario un intervento. Una condivisione deve avere lo stato AVAILABLE (DISPONIBILE) per tutto il tempo in cui è in uso o per la maggior parte del tempo.

Stato	Significato
AVAILABLE (DISPONIBILE)	La condivisione file è configurata correttamente ed è disponibile per l'uso. Lo stato AVAILABLE (DISPONIBILE) è il normale stato di funzionamento per una condivisione file.
CREATING (CREAZIONE IN CORSO)	È in corso la creazione della condivisione file, che non è pronta per l'uso. Lo stato CREATING (CREAZIONE IN CORSO) è transitorio. Nessun'operazione richiesta. Se la condivisione file si blocca in questo stato, probabilmente la macchina virtuale del gateway ha perso la connessione aAWS.

Stato	Significato
UPDATING (AGGIORNAMENTO IN CORSO)	È in corso l'aggiornamento della condivisione file. Se una condivisione file si blocca in questo stato, probabilmente la macchina virtuale del gateway ha perso la connessione aAWS.
ELIMINAZIONE IN CORSO	È in corso l'eliminazione della condivisione file. La condivisione file non viene eliminata fino a quando i dati non sono stati caricatiAWS. Lo stato DELETING (ELIMINAZIONE IN CORSO) è transitorio e non è richiesta alcuna operazione.
FORCE_DEL ETING (ELIMINAZ IONE_FORZATA)	È in corso l'eliminazione forzata della condivisione file. La condivisione file viene eliminata immediatamente e caricata inAWSè stata interrotta. Lo stato FORCE_DELETING (ELIMINAZIONE_FORZATA) è transitorio e non è richiesta alcuna operazione.
UNAVAILABLE (NON DISPONIBILE)	La condivisione file si trova in uno stato non integro. Alcuni problemi possono causare lo stato non integro di una condivisione file. Ad esempio, questo stato può essere dovuto a errori delle policy dei ruoli oppure alla mappatura della condivisione file a un bucket Amazon S3 non esistente. Quando il problema che ha causato lo stato non integro viene risolto, il file torna allo stato AVAILABLE (DISPONIBILE).

Best practice per la condivisione file

In questa sezione vengono fornite informazioni sulle best practice per la creazione di condivisioni file.

Argomenti

- Impedire la scrittura di più condivisioni file nel bucket Amazon S3
- Consentire a client NFS specifici di montare la condivisione di file

Impedire la scrittura di più condivisioni file nel bucket Amazon S3

Quando si crea una condivisione file, è consigliabile configurare il bucket Amazon S3 in modo da permettere la scrittura da parte di una sola condivisione file. Se configuri il bucket S3 per essere scritto da più condivisioni file, potrebbero verificarsi risultati imprevisti. Per impedire che ciò si

verifichi, crea una policy del bucket S3 che impedisce a tutti i ruoli, ad eccezione di quello usato per la condivisione file, di inserire o eliminare oggetti nel bucket. Collega quindi la policy al bucket S3.

La policy di esempio seguente impedisce a tutti i ruoli, ad eccezione di quello che ha creato il bucket, di scrivere nel bucket S3. Le operazioni `s3:DeleteObject` e `s3:PutObject` vengono impedite a tutti i ruoli ad eccezione di `"TestUser"`. La policy si applica a tutti gli oggetti nel bucket `"arn:aws:s3:::TestBucket/*"`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::TestBucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

Consentire a client NFS specifici di montare la condivisione di file

È consigliabile modificare le impostazioni dei client NFS consentiti per la condivisione file. In caso contrario, qualsiasi client nella rete può montare la condivisione file. Per ulteriori informazioni su come modificare le impostazioni dei client NFS, consulta Modifica delle impostazioni di accesso per la condivisione di file NFS.

Monitoraggio del gateway file

È possibile monitorare il gateway di file e le risorse associate inAWS Storage Gatewayutilizzando le metriche di Amazon CloudWatch e i registri di controllo della condivisione di file. Puoi anche utilizzare CloudWatch Events per ricevere notifiche al termine delle operazioni sui file. Per informazioni sui parametri di tipo gateway file, consulta Monitoraggio del gateway file.

Argomenti

Ottenere i log dello stato del gateway di file con i gruppi di log CloudWatch

Puoi utilizzare Amazon CloudWatch Logs per ottenere informazioni sullo stato del gateway file e delle risorse correlate. Puoi utilizzare i log per monitorare il gateway alla ricerca di errori riscontrati. Inoltre, puoi utilizzare i filtri di sottoscrizione Amazon CloudWatch per automatizzare l'elaborazione delle informazioni di log in tempo reale. Per ulteriori informazioni, consultaElaborazione in tempo reale dei dati di log con le sottoscrizioninellaGuida per l'utente di Amazon CloudWatch.

Ad esempio, puoi configurare un gruppo di log CloudWatch per monitorare il gateway e ricevere una notifica quando il gateway di file non riesce a caricare i file in un bucket Amazon S3. È possibile configurare il gruppo quando attivi il gateway o dopo che il gateway è stato attivato ed è operativo. Per informazioni su come configurare un gruppo di log CloudWatch durante l'attivazione di un gateway, consultaConfigurare il tuo Amazon S3 File Gateway. Per informazioni generali sui gruppi di log CloudWatch, consultaUtilizzo di gruppi di log e flussi di lognellaGuida per l'utente di Amazon CloudWatch.

Di seguito è riportato un esempio di errore segnalato da un gateway di file.

```
{
```

```
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Questo errore indica che il gateway di file non è in grado di caricare l'oggetto`myFolder/myFile.text`in Amazon S3 perché è passato dalla classe di storage Amazon S3 Standard alla classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Nel log dello stato del gateway precedente, questi elementi specificano le informazioni fornite:

- `source: share-E1A2B34C` indica la condivisione file che ha riscontrato questo errore.
- `"type": "InaccessibleStorageClass"` indica il tipo di errore che si è verificato. In questo caso, questo errore si è verificato quando il gateway stava tentando di caricare l'oggetto specificato in Amazon S3 o di leggere da Amazon S3. Tuttavia, in questo caso, l'oggetto è passato ad Amazon S3 Glacier. Il valore di `"type"` può essere qualsiasi errore rilevato dal gateway di file. Per un elenco dei possibili errori, consulta Come risolvere i problemi del gateway di file
- `"operation": "S3Upload"`indica che questo errore si è verificato quando il gateway stava tentando di caricare questo oggetto in S3.
- `"key": "myFolder/myFile.text"` indica l'oggetto che ha causato l'errore.
- `gateway": "sgw-B1D123D4` indica il gateway di file che ha riscontrato questo errore.
- `"timestamp": "1565740862516"`indica l'ora in cui l'errore si è verificato.

Per informazioni su come risolvere errori di questo tipo, consulta Come risolvere i problemi del gateway di file.

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

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

Per configurare un gruppo di log di CloudWatch da utilizzare con il gateway di file

1. Accedi allaAWS Management Consolee apri la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, scegliereGatewayquindi scegliere il gateway per il quale si desidera configurare il gruppo di log di CloudWatch.
3. PerOperazioni, scegliModifica delle informazioni sui gateway. Oppure, sulDettaglitab, sottoregistri HealtheNon abilitato, scegliConfigurare gruppo di logper aprireModificareNome del percorso clientefinestra di dialogo.
4. PerGruppo di log dello stato del gatewayscegliere una delle opzioni seguenti:

   - Disabilitare la registrazionese non si desidera monitorare il gateway utilizzando i gruppi di log di CloudWatch.
   - Creare un nuovo gruppo di logper creare un nuovo gruppo di log CloudWatch.
   - Utilizzare un gruppo di log esistente;per utilizzare un gruppo di log CloudWatch già esistente.

     Scegli un gruppo di log dalElenco dei gruppi di log esistenti.
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, sceglieregatewayquindi scegliere il gateway per il quale si è configurato il gruppo di log di CloudWatch.
   2. SelezionaDettaglitab e sottoregistri Health, scegliLog di CloudWatch. LaDettagli gruppo di logla pagina si apre nella console CloudWatch.

Per configurare un gruppo di log di CloudWatch da utilizzare con il gateway di file

1. Accedi allaAWS Management Consolee apri la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. SceglieregatewayquindiScegliere il gateway per il quale si desidera configurare il gruppo di log di CloudWatch.
3. PerOperazioni, scegliModifica delle informazioni sui gateway. Oppure, nelDettaglischeda, accanto aRegistrazione di log, inNon abilitato, scegliConfigurare gruppo di logper aprireModifica delle informazioni sui gatewayfinestra di dialogo.
4. PerGruppo di log del gateway, scegliUtilizzare un gruppo di log esistente;e quindi scegliere il gruppo di log da utilizzare.

Se non si dispone di un gruppo di log, scegliere Create a new log group (Crea un nuovo gruppo di log) per crearne uno. Viene visualizzata la console di CloudWatch Logs, in cui è possibile creare il gruppo di log. Se si crea un nuovo gruppo di log, scegliere il pulsante di aggiornamento per visualizzare il nuovo gruppo di log nell'elenco a discesa.

5. Al termine, scegliere Save (Salva).
6. Per visualizzare i log del gateway, scegliere il gateway, quindi scegliere il gateway, quindi scegliere ilDettaglischeda.

Per informazioni su come risolvere gli errori, consulta Come risolvere i problemi del gateway di file.

Uso di parametri di Amazon CloudWatch

È possibile monitorare i dati per il gateway file utilizzando laAWS Management Consoleo l'API di CloudWatch. La console visualizza una serie di grafici in base ai dati non elaborati dell'API di CloudWatch. L'API CloudWatch può essere utilizzata anche tramite uno deiAWSSDKoAPI di Amazon CloudWatchstrumenti. In base alle tue esigenze, potresti decidere di utilizzare i grafici visualizzati nella console o quelli recuperati dall'API.

Indipendentemente dal metodo utilizzato per utilizzare i parametri, devi specificare le informazioni seguenti.

- Dimensione del parametro da usare. Una dimensione è una coppia nome-valore che consente di identificare un parametro in modo univoco. Le dimensioni per Storage Gateway sono`GatewayId`e`GatewayName`. Nella console CloudWatch è possibile utilizzare il`Gateway Metrics`vista per selezionare le dimensioni specifiche del gateway. Per ulteriori informazioni sulle dimensioni, consulta.DimensioninellaGuida per l'utente di Amazon CloudWatch.
- Il nome del parametro, ad esempio `ReadBytes`.

Nella tabella seguente vengono descritti i tipi di dati dei parametri Storage Gateway disponibili.

Spazio dei nomi Amazon CloudWatch	Dimensione	Descrizione
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Queste dimensioni filtrano in base ai dati dei parametri che descrivono gli aspetti del gateway. Puoi identific

Spazio dei nomi Amazon CloudWatch	Dimensione	Descrizione
		are un gateway file da usare specificando le dimensioni `GatewayId` e `GatewayName` . I dati di throughput e latenza di un gateway si basano su tutte le condivisioni file nel gateway. 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 di parametri disponibili
- Ottenere le statistiche di una parametro
- Creazione di allarmi CloudWatch

Ricevere notifiche sulle operazioni di file

Storage Gateway può avviare CloudWatch Events al termine delle operazioni sui file:

- È possibile ricevere una notifica quando il gateway termina il caricamento asincrono dei file da condivisione file su Amazon S3. Utilizzo dell'`NotificationPolicy`Per richiedere una notifica di caricamento file. In questo modo viene inviata una notifica per ogni caricamento di file completato su Amazon S3. Per ulteriori informazioni, consultare Ricevere notifica di caricamento file.
- È possibile ricevere una notifica quando il gateway termina il caricamento asincrono del set di file di lavoro dalla condivisione file su Amazon S3. Utilizzo dell'NotifyWhenUploadedOperazione API per richiedere una notifica di caricamento del set di file funzionante. Questo invia una notifica quando tutti i file nel set di file di lavoro sono stati caricati su Amazon S3. Per ulteriori informazioni, consultare Ottenere la notifica di caricamento del set di file.
- È possibile ricevere una notifica quando il gateway termina l'aggiornamento della cache per il tuo bucket S3. Quando richiami ilRefreshCacheOperazione tramite la console Storage Gateway o

l'API, effettuare la notifica al termine dell'operazione. Per ulteriori informazioni, consultare Ricevere la notifica di aggiornamento della cache.

Una volta eseguita l'operazione di file richiesta, Storage Gateway invia una notifica tramite CloudWatch Events. Puoi configurare CloudWatch Events per inviare le notifiche tramite destinazioni di eventi, quali Amazon SNS, Amazon SQS o unAWS Lambdafunzione. Ad esempio, puoi configurare un target Amazon SNS per inviare la notifica ai consumatori Amazon SNS, ad esempio un'e-mail o un messaggio di testo. Per informazioni sugli eventi CloudWatch, consultaChe cos'è CloudWatch Events?

Per configurare una notifica CloudWatch Events

1. Creare una destinazione, ad esempio un argomento Amazon SNS o una funzione Lambda, da invocare quando l'evento richiesto in Storage Gateway viene attivato.
2. Creare una regola nella console CloudWatch Events per invocare destinazioni in base a un evento in Storage Gateway.
3. Nella regola, è necessario creare un modello di evento per il tipo di evento. La notifica viene attivata quando l'evento soddisfa questo modello della regola.
4. Selezionare la destinazione e configurare le impostazioni.

L'esempio seguente mostra una regola che avvia il tipo di evento specificato nel gateway specificato e nel parametro specificato.AWSRegione . Ad esempio, è possibile specificare `Storage Gateway File Upload Event` come tipo di evento.

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

Per informazioni su come utilizzare CloudWatch Events per attivare le regole, consultaCreazione di una regola CloudWatch Events che si attiva su un eventonellaGuida per l'utente Amazon CloudWatch Events.

Ricevere notifica di caricamento file

Ci sono due casi d'uso in cui è possibile utilizzare la notifica di caricamento di file:

- Per l'automazione dell'elaborazione nel cloud dei file caricati, si può chiamare il`NotificationPolicy`parametro e recupera un ID di notifica. La notifica che viene attivata quando i file sono stati caricati ha lo stesso ID notifica di quella restituita dall'API. Se si esegue la mappatura di questo ID notifica per monitorare l'elenco dei file in in caricamento, è possibile attivare l'elaborazione del file in.AWSquando viene generato l'evento con lo stesso ID.
- Per i casi d'uso di distribuzione di contenuti, puoi avere due gateway file che sono mappati allo stesso bucket Amazon S3. Il client di condivisione file per Gateway1 può caricare nuovi file in Amazon S3 e i file vengono letti dai client di condivisione file su Gateway2. I file vengono caricati su Amazon S3, ma non sono visibili per il Gateway2 perché utilizza una versione della cache locale dei file in Amazon S3. Per rendere visibili i file in Gateway2, è possibile utilizzare il`NotificationPolicy`parametro per richiedere la notifica di caricamento file da Gateway1 quando il file di caricamento è terminato. È quindi possibile utilizzare CloudWatch Events per emettere automaticamente unRefreshCachePer la condivisione file sul Gateway2. QuandoRefreshCachela richiesta è completa, il nuovo file è visibile in Gateway2.

Example Esempio: notifica di caricamento file

L'esempio seguente mostra una notifica di caricamento file che ti viene inviata tramite CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON. È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway Object Upload Event`.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "my-bucket",
    }
}
```

Nomi di campo	Descrizione
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione dell'evento che ha attivato la notifica inviata.
source	LaAWSservizio che è l'origine della richiesta e della notifica.
account	L'ID delAWSconto da cui la richiesta e la notifica sono state generate.
time	Quando è stata effettuata la richiesta per caricare i file su Amazon S3.
Regione	LaAWSRegione da cui sono state inviate la richiesta e la notifica.
resources	Le risorse di storage gateway a cui si applica la policy.
dimensione oggetti	La dimensione dell'oggetto in byte.
tempo di modifica	Il momento in cui il client ha modificato il file.

Nomi di campo	Descrizione
oggetto-chiave	Il percorso del file.
event-type	CloudWatch Events che hanno attivato la notifica.
prefisso	Nome del prefisso del bucket S3.
bucket-name	Nome del bucket S3.

Ottenere la notifica di caricamento del set di file

Esistono due casi d'uso in cui è possibile utilizzare la notifica di caricamento del set di file di lavoro:

- Per l'automazione dell'elaborazione nel cloud dei file caricati, si può chiamare il`NotifyWhenUploaded`API e recupera un ID di notifica. La notifica che viene attivata quando il set di file è stato caricato ha lo stesso ID notifica di quella restituita dall'API. Se si esegue la mappatura di questo ID notifica per monitorare l'elenco dei file in in caricamento, è possibile attivare l'elaborazione del set di file in.AWSquando viene generato l'evento con lo stesso ID.
- Per i casi d'uso di distribuzione di contenuti, puoi avere due gateway file che sono mappati allo stesso bucket Amazon S3. Il client di condivisione file per Gateway1 può caricare nuovi file in Amazon S3 e i file vengono letti dai client di condivisione file su Gateway2. I file vengono caricati su Amazon S3, ma non sono visibili per il Gateway2 perché utilizza una versione della cache locale dei file in S3. Per rendere visibili i file in Gateway2, utilizzare ilNotifyWhenUploadedOperazione dell'API per richiedere la notifica di caricamento file da Gateway1 quando il caricamento del set di file è terminato. È quindi possibile utilizzare CloudWatch Events per emettere automaticamente unRefreshCachePer la condivisione file sul Gateway2. QuandoRefreshCacheLa richiesta è completa, i nuovi file sono visibili in Gateway2. Questa operazione non importa i file nello storage della cache del gateway di file. Aggiorna solo l'inventario memorizzato nella cache per riflettere le modifiche nell'inventario degli oggetti nel bucket S3.

Example Esempio: notifica di caricamento del set di file di lavoro

L'esempio seguente mostra una notifica di caricamento del set di file che ti viene inviata tramite CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON.

È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Upload Notification Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

Nomi di campo	Descrizione
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione dell'evento che ha attivato la notifica inviata.
source	LaAWSservizio che è l'origine della richiesta e della notifica.
account	L'ID delAWSconto da cui la richiesta e la notifica sono state generate.
time	Quando è stata effettuata la richiesta per caricare i file su Amazon S3.

Nomi di campo	Descrizione
Regione	LaAWSRegione da cui sono state inviate la richiesta e la notifica.
resources	Le risorse di Storage Gateway a cui si applica la policy.
event-type	CloudWatch Events che hanno attivato la notifica.
notification-id	L'ID generato in modo casuale della notifica che è stata inviata. Questo ID è nel formato UUID. Questo è l'ID della notifica che viene restituito quando `NotifyWhenUploaded` viene chiamato.
richiesta-ricevuta	Quando il gateway ha ricevuto la richiesta `NotifyWhenUploaded` .
completed	Quando tutti i file nel set di lavoro sono stati caricati su Amazon S3.

Ricevere la notifica di aggiornamento della cache

Per il caso d'uso della notifica di aggiornamento della cache, è possibile avere due gateway file mappati sullo stesso bucket Amazon S3 e il client NFS per il Gateway1 che carica nuovi file sul bucket S3. I file vengono caricati su Amazon S3, ma non appariranno nel Gateway2 finché non si aggiornerà la cache. Questo perché Gateway2 utilizza una versione della cache locale dei file in Amazon S3. È possibile eseguire un'operazione con i file nel Gateway2 quando l'aggiornamento della cache è terminato. I file di grandi dimensioni potrebbero richiedere alcuni minuti prima di comparire nel gateway2, pertanto potrebbe essere utile ricevere una notifica al termine dell'aggiornamento della cache. È possibile richiedere la notifica di aggiornamento della cache dal Gateway2 per sapere quando tutti i file sono visibili in Gateway2.

Example Esempio: notifica di aggiornamento della cache

L'esempio seguente mostra una notifica di aggiornamento della cache che viene inviata tramite CloudWatch quando l'evento corrisponde alla regola creata. Questa notifica è in formato JSON. È possibile configurare questa notifica in modo che venga in forma di SMS. Il valore del campo `detail-type` è `Storage Gateway Refresh Cache Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

Nomi di campo	Descrizione
versione	La versione corrente della policy IAM.
id	L'ID che identifica la policy IAM.
detail-type (tipo di dettaglio)	Una descrizione del tipo di evento che ha attivato la notifica inviata.
source	LaAWSIl servizio che è l'origine della richiesta e della notifica.

Nomi di campo	Descrizione
account	L'ID delAWSconto da cui la richiesta e la notifica sono state generate.
time	Quando è stata effettuata la richiesta per aggiornare i file nel set di lavoro.
Regione	LaAWSRegione da cui sono state inviate la richiesta e la notifica.
resources	Le risorse di Storage Gateway a cui si applica la policy.
event-type	CloudWatch Events che hanno attivato la notifica.
notification-id	L'ID generato in modo casuale della notifica che è stata inviata. Questo ID è nel formato UUID. Questo è l'ID della notifica che viene restituito quando `RefreshCache` viene chiamato.
started	quando il gateway ha ricevuto il`RefreshCache` La richiesta e l'aggiornamento è stato avviato.
completed	Quando l'aggiornamento del set di lavoro è stato completato.
folderList	Un elenco separato da virgole dei percorsi di cartelle che sono stati aggiornati nella cache. Il valore predefinito è ["/"].

Comprendere i parametri del gateway

Nella tabella seguente vengono descritti parametri che coprono i gateway file S3. Ogni gateway dispone di un set di parametri a esso associati. Alcuni parametri specifici dei gateway hanno lo stesso

nome di certi parametri specifici della condivisione file. Questi parametri rappresentano lo stesso tipo di misure, ma vengono definiti per il gateway piuttosto che per la condivisione file.

Specificare sempre se si desidera utilizzare un gateway o una condivisione file quando si utilizza un parametro specifico. In particolare, quando si utilizza i parametri del gateway, è necessario specificare il`Gateway Name`per il gateway di cui si desidera visualizzare i dati dei parametri. Per ulteriori informazioni, consultare Uso di parametri di Amazon CloudWatch.

Nella tabella seguente vengono descritti i parametri che puoi utilizzare per ottenere informazioni sulGateway file S3s.

Parametro	Descrizione
`AvailabilityNotifications`	Questo parametro segnala il numero di notifiche di stato relative alla disponibilità generate dal gateway durante il periodo di reporting. unità: Conteggio
`CacheFileSize`	Questa parametro monitora le dimensioni dei file nella cache gateway. Usa questa metrica con il`Average`statistic per misurare la dimensione media di un file nella cache del gateway. Usa questa metrica con il`Max`statistic per misurare la dimensione massima di un file nella cache del gateway. unità: Byte
`CacheFree`	Questo parametro indica il numero di byte disponibili nella cache del gateway. unità: Byte
`CacheHitPercent`	Percentuale delle operazioni di lettura dell'appl icazione dal gateway, fornite dalla cache. Il campione si riferisce al termine del periodo di reporting.

Parametro	Descrizione
	In assenza di operazioni di lettura dell'appl icazione dal gateway, questo parametro segnala il 100%. unità: Percentuale
`CachePercentDirty`	Percentuale totale della cache del gateway non conservata inAWS. Il campione si riferisce al termine del periodo di reporting. unità: Percentuale
`CachePercentUsed`	La percentuale complessiva dello storage della cache gateway utilizzato. Il campione si riferisce al termine del periodo di reporting. unità: Percentuale
`CacheUsed`	Questo parametro indica il numero di byte utilizzati nella cache del gateway. unità: Byte
`CloudBytesDownloaded`	Il numero totale di byte che il gateway ha scaricato inAWSdurante il periodo di riferimen to. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni di input/out put al secondo (IOPS). unità: Byte

Parametro	Descrizione
`CloudBytesUploaded`	Il numero totale di byte che il gateway ha scaricato daAWSdurante 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
`FilesFailingUpload`	Questo parametro consente di tenere traccia del numero di file non caricati suAWS. Questi file genereranno notifiche di integrità che contengono ulteriori informazioni sul problema. Usa questa metrica con il`Sum`statistica per mostrare il numero di file che attualmente non vengono caricatiAWS. unità: Conteggio
`FileSharesUnavailable`	Questa metrica fornisce il numero di condivisioni di file su questi gateway che si trovano nellaNon disponibilestato. Se questa metrica segnala che le condivisioni di file non sono disponibili, è probabile che si verifichi un problema con il gateway che potrebbe causare interruzioni del flusso di lavoro. Si consiglia di creare un avviso per quando questa parametro indica un valore diverso da zero. unità: Conteggio

Parametro	Descrizione
`FilesRenamed`	Questo parametro consente di tenere traccia del numero di file rinominati nel periodo di riferimento. unità: Conteggio
`HealthNotifications`	Questa metrica riporta il numero di notifiche di integrità generate da questo gateway nel periodo di riferimento. unità: Conteggio
`IoWaitPercent`	Questo parametro segnala la percentuale di tempo durante la quale 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
`NfsSessions`	Questo parametro indica il numero di sessioni NFS attive sul gateway. unità: Conteggio

Parametro	Descrizione
`RootDiskFreeBytes`	Questo parametro indica il numero di byte disponibili sul disco radice del gateway. Se questa metrica segnala meno di 20 GB sono gratuiti, è necessario aumentare le dimensioni del disco root. unità: Byte
`S3GetObjectRequestTime`	Questa metrica riporta il tempo necessario per il gateway per completare le richieste di oggetti get S3. unità: Millisecondi
`S3PutObjectRequestTime`	Questa metrica riporta il tempo necessario per il gateway per completare le richieste di oggetti put S3. unità: Millisecondi
`S3UploadPartRequestTime`	Questa metrica riporta il tempo necessario per il gateway per completare le richieste di parti di caricamento S3. unità: Millisecondi
`SmbV1Sessions`	Questo parametro indica il numero di sessioni SMBv1 attive sul gateway. unità: Conteggio
`SmbV2Sessions`	Questo parametro indica il numero di sessioni SMBv2 attive sul gateway. unità: Conteggio

Parametro	Descrizione
`SmbV3Sessions`	Questo parametro indica il numero di sessioni SMBv3 attive sul gateway. unità: Conteggio
`TotalCacheSize`	Questa parametro riporta le dimensioni totali della cache. unità: Byte
`UserCpuPercent`	Questa metrica riporta la percentuale di tempo impiegato per l'elaborazione del gateway. unità: Percentuale

Informazioni sulle metriche della condivisione file

Di seguito vengono fornite informazioni sui parametri Storage Gateway che coprono condivisioni file. Ogni condivisione file dispone di un set di parametri a essa associati. Alcuni parametri specifici della condivisione file hanno lo stesso nome di alcuni parametri specifici del gateway. Questi parametri rappresentano lo stesso tipo di misure, ma vengono definiti per la condivisione file.

Specificare sempre se si desidera utilizzare un gateway o un parametro di condivisione dei file prima di utilizzare un parametro. Nello specifico, quando si lavora con i parametri di condivisione file, è necessario specificare `File share ID` che identifica il file per il quale si desidera visualizzare i parametri. Per ulteriori informazioni, consultare Uso di parametri di Amazon CloudWatch.

Nella tabella seguente vengono descritti parametri Storage Gateway che puoi utilizzare per ottenere informazioni sulle condivisioni file.

Parametro	Descrizione
`CacheHitPercent`	Percentuale delle operazioni di lettura dell'appl icazione dalle condivisioni file servite dalla cache. Il campione si riferisce al termine del periodo di reporting.

Parametro	Descrizione
	In assenza di operazioni di lettura dell'appl icazione dalla condivisione file, questo parametro segnala il 100%. unità: Percentuale
`CachePercentDirty`	Contributo della condivisione file alla percentua le totale della cache del gateway non conservat a inAWS. Il campione si riferisce al termine del periodo di reporting. Utilizzo dell'`CachePercentDirty` parametro del gateway per visualizzare la percentuale totale della cache del gateway non conservata inAWS. unità: Percentuale
`CachePercentUsed`	Contributo della condivisione file all'utilizzo della percentuale totale dello storage della cache del gateway. Il campione si riferisce al termine del periodo di reporting. Usa il parametro `CachePercentUsed` del gateway per visualizzare la percentuale totale di utilizzo dello storage della cache del gateway. unità: Percentuale

Parametro	Descrizione
`CloudBytesUploaded`	Il numero totale di byte che il gateway ha scaricato inAWSdurante il periodo di riferimen to. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. unità: Byte
`CloudBytesDownloaded`	Il numero totale di byte che il gateway ha scaricato daAWSdurante il periodo di riferimen to. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni di input/out put al secondo (IOPS). unità: Byte
`ReadBytes`	Numero totale di byte letti dalle applicazioni in locale 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

Parametro	Descrizione
`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 controllo del gateway di file

I log di audit Amazon S3 File Gateway (S3 File Gateway) forniscono dettagli sull'accesso degli utenti a file e cartelle all'interno di una condivisione file. Puoi utilizzarli per monitorare le attività degli utenti e agire se vengono identificati modelli di attività inappropriati.

Operazioni

Nella tabella seguente vengono descritte le operazioni di accesso ai file di log di audit del gateway file.

Nome operazione	Definizione
Leggere i dati	Leggere il contenuto di un file.
Scrivere i dati	Modificare 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.
Delete	Eliminare un file o una cartella.
Attributi di scrittura	Aggiorna i metadati di file o cartelle (ACL, proprietario, gruppo, autorizzazioni).

Attributi

La tabella seguente descrive gli attributi di accesso ai file di log di audit di S3 File Gateway.

Attributo	Definizione
`accessMode`	L'impostazione di autorizzazione per l'oggetto.
`accountDomain` (solo PMI)	Il dominio Active Directory (AD) a cui appartien e l'account client.
`accountName` (solo PMI)	Nome utente Active Directory del client.
`bucket`	Il nome del bucket S3.
`clientGid` (solo NFS)	L'identificatore del gruppo di utenti che accede all'oggetto.
`clientUid` (solo NFS)	Identificatore dell'utente che accede all'oggetto.
`ctime`	L'ora in cui il contenuto o i metadati dell'oggetto sono stati modificato, impostata dal client.
`groupId`	Identificatore per il proprietario del gruppo dell'oggetto.
`fileSizeInBytes`	La dimensione del file in byte, impostata dal client al momento della creazione del file.
`gateway`	L'ID gateway di storage.
`mtime`	Ora in cui il contenuto dell'oggetto è stato modificato, impostata dal client.
`newObjectName`	Il percorso completo del nuovo oggetto dopo che è stato rinominato.
`objectName`	Il percorso completo dell'oggetto.
`objectType`	Definisce se l'oggetto è un file o una cartella.
`operation`	Il nome dell'operazione di accesso dell'oggetto.

Attributo	Definizione
`ownerId`	L'identificatore per il proprietario dell'oggetto.
`securityDescriptor` (solo PMI)	Visualizza l'elenco di controllo di accesso discrezionale (DACL) impostato su un oggetto, in formato SDDL.
`shareName`	Il nome della condivisione a cui si accede.
`source`	L'ID della condivisione file sottoposta ad audit.
`sourceAddress`	L'indirizzo IP del computer client di condivisione file.
`status`	Stato dell'operazione. Vengono registrate solo le operazioni riuscite (gli errori vengono registrati con l'eccezione degli errori derivanti da autorizzazioni negate).
`timestamp`	L'ora in cui si è verificata l'operazione in base al timestamp del sistema operativo del gateway.
`version`	Versione del formato del log di audit.

Attributi registrati per operazione

Nella tabella seguente vengono descritti gli attributi del log di audit del gateway S3 registrati in ogni operazione di accesso ai file.

	Leggere i dati	Scrivere i dati	Create Folder	Creare file	Rinomina e file/ cartella	Elimina file/ cartella	Attributi di scrittura (modifica ACL -Solo SMB)	Attributi di scrittura (chown)	Attributi di scrittura (chmod)	Attributi di scrittura (chgrp)
access			X	X					X	
accoun main (solo PMI)	X	X	X	X	X	X	X	X	X	X
accoun me (solo PMI)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (solo NFS)	X	X	X	X	X	X		X	X	X
client (solo NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						

	Leggere i dati	Scrivere i dati	Create Folder	Creare file	Rinomina e file/ cart ella	Elimina file/ cart ella	Attributi di scrittura (modifica ACL -Solo SMB)	Attributi di scrittura (chown)	Attributi di scrittura (chmod)	Attributi di scrittura (chgrp)
`fileSi nBytes`				X						
`gatewa`	X	X	X	X	X	X	X	X	X	X
`mtime`			X	X						
`newObj Name`					X					
`object e`	X	X	X	X	X	X	X	X	X	X
`object e`	X	X	X	X	X	X	X	X	X	X
`operat`	X	X	X	X	X	X	X	X	X	X
`ownerI`			X	X				X		
`securi escrip` (solo PMI)							X	X		
`shareN`	X	X	X	X	X	X	X	X	X	X
`source`	X	X	X	X	X	X	X	X	X	X

	Leggere i dati	Scrivere i dati	Create Folder	Creare file	Rinomina e file/ cartella	Elimina file/ cartella	Attributi di scrittura (modifica ACL -Solo SMB)	Attributi di scrittura (chown)	Attributi di scrittura (chmod)	Attributi di scrittura (chgrp)
`source ress`	X	X	X	X	X	X	X	X	X	X
`status`	X	X	X	X	X	X	X	X	X	X
`timest`	X	X	X	X	X	X	X	X	X	X
`versic`	X	X	X	X	X	X	X	X	X	X

Gestione del gateway

La gestione del gateway include attività quali la configurazione dello storage della cache e il caricamento dello spazio di buffer ed eseguendo manutenzione generale per le prestazioni del gateway. Queste attività sono comuni a tutti i tipi di gateway.

Argomenti

Spegnimento della macchina virtuale del gateway

Potrebbe essere necessario arrestare o riavviare la macchina virtuale per la manutenzione, ad esempio durante l'applicazione di una patch al tuo hypervisor. Prima di spegnere la macchina virtuale, è necessario arrestare il gateway. Per il gateway file, è sufficiente spegnere la macchina virtuale. Sebbene questa sezione sia incentrata sull'avvio e sull'arresto del gateway utilizzando la console di gestione Storage Gateway, puoi arrestare il gateway anche utilizzando la console locale della macchina virtuale o l'API di Storage Gateway. Quando accendi la macchina virtuale, ricorda di riavviare il gateway.

Potrebbe essere necessario arrestare o riavviare la macchina virtuale per la manutenzione, ad esempio durante l'applicazione di una patch al tuo hypervisor. Per il gateway file, è sufficiente spegnere la macchina virtuale. Non eseguire lo shutdown del gateway. Sebbene questa sezione sia incentrata sull'avvio e sull'arresto del gateway utilizzando la console di gestione Storage Gateway, puoi arrestare il gateway anche utilizzando la console locale della macchina virtuale o l'API di Storage Gateway. Quando accendi la macchina virtuale, ricorda di riavviare il gateway.

- Console locale della VM del gateway: vedereEsecuzione delle operazioni di manutenzione sulla console locale.
- API Storage Gateway: vedereShutdownGateway

Gestione di dischi locali per Storage Gateway

La macchina virtuale (VM) del gateway usa i dischi locali allocati in locale per il buffering e lo storage. I gateway creati nelle istanze Amazon EC2 usano i volumi Amazon EBS come dischi locali.

Argomenti

Decidere la quantità di storage su disco locale

Il numero e la dimensione dei dischi da allocare per il gateway dipende da te. Il gateway richiede il seguente storage aggiuntivo:

I gateway file richiedono almeno un disco da usare come cache. La tabella seguente contiene le dimensioni consigliate per lo storage su disco locale per il gateway distribuito. Puoi aggiungere ulteriore spazio di storage locale dopo la configurazione del gateway, se le richieste dei carichi di lavoro aumentano.

Storage locale	Descrizione	Tipo di gateway
Storage della cache	Lo storage della cache funge da archivio locale durevole per i dati in attesa di essere caricati in Amazon S3 o su file system.	• Gateway file

> **Note**
>
> Le risorse di storage fisiche sottostanti sono rappresentate come datastore in VMware. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando effettui il provisioning di un disco locale (ad esempio, per l'uso come storage della cache), puoi scegliere di 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 lo storage della cache. Un datastore supportato da un solo disco fisico sottostante può offrire prestazioni non soddisfacenti in alcune situazioni, quando viene usato sia per lo storage della cache. Ciò si verifica anche se il backup è costituito da una configurazione RAID a basse prestazioni, come RAID1.

Dopo la configurazione iniziale e la distribuzione del gateway, è possibile modificare lo storage locale aggiungendo dischi per lo storage della cache.

Determinazione della dimensione dello storage cache da allocare

Il gateway usa lo storage della cache per fornire accesso a bassa latenza ai dati usati di recente. Lo storage della cache funge da archivio locale durevole per i dati in attesa di essere caricati in Amazon S3 o su file system. Per ulteriori informazioni su come stimare le dimensioni dello storage della cache, consulta Gestione di dischi locali per Storage Gateway.

Inizialmente, puoi usare questa approssimazione per effettuare il provisioning dei dischi per lo storage della cache. Puoi quindi usare i parametri operativi di Amazon CloudWatch per monitorare l'utilizzo dello storage della cache ed effettuare il provisioning di altro spazio storage, se necessario, usando la console. Per informazioni sull'uso dei parametri e sull'impostazione di allarmi, consulta Prestazioni.

Aggiunta di storage della cache

Quando i requisiti della tua applicazione cambiano, puoi aumentare la capacità di storage della cache del gateway. Puoi aggiungere ulteriore capacità della cache al gateway senza interrompere le funzioni del gateway esistenti. Quando aggiungi ulteriore capacità di storage, esegui l'operazione con la VM del gateway attivata.

Important

Quando aggiungi la cache a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza Amazon EC2). Non modificare la dimensione dei dischi esistenti se i dischi sono stati allocati in precedenza come cache. Non rimuovere i dischi della cache allocati come storage della cache.

La procedura seguente illustra come configurare o memorizzare nella cache lo storage per il gateway.

Per aggiungere e configurare o memorizzare nella cache

1. Effettuare il provisioning di un nuovo disco nell'host (hypervisor o istanza Amazon EC2). Per informazioni su come effettuare il provisioning di un disco in un hypervisor, consulta il manuale utente dell'hypervisor. È possibile configurare il disco come storage della cache.
2. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
3. Nel riquadro di navigazione, scegliere Gateways.
4. Nel menu Actions (Operazioni) scegliere Edit local disks (Modifica dischi locali).
5. Nella finestra di dialogo Edit local disk (Modifica i dischi locali) individuare i dischi allocati e stabilire quali usare per lo storage della cache.

   Se i dischi non vengono visualizzati, fare clic sul pulsante Refresh (Aggiorna).
6. Per salvare le impostazioni di configurazione, selezionare Save (Salva).

Utilizzo di storage effimero con gateway EC2

Questa sezione descrive le operazioni necessarie per evitare la perdita di dati quando si seleziona un disco temporaneo come storage della cache del gateway.

I dischi temporanei forniscono storage a livello di blocchi temporaneo per l'istanza Amazon EC2. I dischi temporanei sono ideali per lo storage temporaneo di dati che cambiano di frequente, come i dati nello storage della cache di un gateway. Quando si avvia il gateway con un'Amazon EC2 Amazon Machine Image e il tipo di istanza selezionato supporta lo storage temporaneo, i dischi sono elencati automaticamente ed è possibile selezionare uno dei dischi per archiviare i dati nella cache del gateway. Per ulteriori informazioni, consultaInstance store Amazon EC2nellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

Le scritture delle applicazioni sui dischi sono archiviate in modo sincrono nella cache e caricate in modo asincrono nello storage durevole in Amazon S3. Se i dati archiviati nello storage temporaneo vengono persi perché un'istanza Amazon EC2 si arresta prima che sia completato il caricamento, i dati nella cache che non sono ancora stati caricati su Amazon S3 potrebbero andare perduti. È possibile evitare la perdita di dati seguendo la procedura prima di riavviare o arrestare l'istanza EC2 che ospita il gateway.

> **Note**
>
> Se utilizzi lo storage temporaneo e arresti e avvii il gateway, il gateway sarà definitivamente offline. Questo accade perché il disco di storage fisico viene sostituito. Non è disponibile alcuna soluzione per questo problema, quindi è necessario eliminare il gateway e attivarne uno nuovo su una nuova istanza EC2.

I passaggi della procedura seguente sono specifici per i gateway di file.

Per prevenire la perdita di dati nei gateway di file che utilizzano dischi temporanei

1. Interrompere tutti i processi che stanno scrivendo sulla condivisione file.
2. Iscriviti per ricevere notifiche da CloudWatch Events. Per informazioni, consultare Ricevere notifiche sulle operazioni di file.
3. Chiama ilNotifica quando l'API caricataper ottenere una notifica quando i dati scritti sono stati archiviati in modo durevole su fino al punto in cui lo storage temporaneo è andato perso.
4. Attendi che l'API si completi e riceverai un id notifica.

   Riceverai un evento CloudWatch con lo stesso id notifica.
5. Verificare che il parametro `CachePercentDirty` per la condivisione file sia 0. Questo conferma che tutti i tuoi dati sono stati scritti su Amazon S3. Per informazioni sui parametri delle condivisioni di file, consulta Informazioni sulle metriche della condivisione file.
6. È ora possibile riavviare o arrestare il gateway di file senza rischio di perdite di dati.

Gestione della larghezza di banda per il gateway di file Amazon S3

È possibile limitare il throughput di caricamento dal gateway aAWSper controllare la quantità di larghezza di banda di rete utilizzata dal gateway. Per impostazione predefinita, un gateway attivato non ha limiti di velocità.

È possibile configurare una pianificazione del limite di larghezza di banda utilizzando ilAWS Management Console, unAWSSoftware Development Kit (SDK) o ilAWS Storage GatewayAPI (vediAggiorna la pianificazione del limite della larghezza della bandanellaAWSRiferimento all'API Storage Gateway.). Utilizzando un programma limite di larghezza di banda, è possibile configurare i limiti in modo che vengano modificati automaticamente durante il giorno o la settimana. Per ulteriori

informazioni, consultare Visualizzare e modificare la pianificazione del limite di larghezza di banda per il gateway utilizzando la console Storage Gateway.

> **Note**
>
> La configurazione dei limiti di velocità di banda e delle pianificazioni non è attualmente supportata per il tipo Amazon FSx File Gateway.

Argomenti

Visualizzare e modificare la pianificazione del limite di larghezza di banda per il gateway utilizzando la console Storage Gateway

Questa sezione descrive come visualizzare e modificare la pianificazione del limite di velocità della larghezza di banda per il gateway.

Per visualizzare e modificare la pianificazione del limite di velocità della larghezza di banda

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione a sinistra, scegliereGatewayquindi scegliere il gateway da gestire.
3. PerOperazioni, scegliModifica la pianificazione del limite della larghezza di banda.

   La pianificazione corrente del limite di larghezza di banda del gateway viene visualizzata sulModifica la pianificazione del limite della larghezza di banda(Certificato creato). Per impostazione predefinita, un nuovo gateway non ha limiti di larghezza di banda definiti.
4. (Facoltativo) ScegliAggiunta di un nuovo limite di velocità di bandaper aggiungere un nuovo intervallo configurabile alla pianificazione. Per ogni intervallo aggiunto, immettere le seguenti informazioni:

- Velocità di caricamento— Immettere il limite di velocità di caricamento, in megabit al secondo (Mbps). Il valore minimo è 100 Mbps.
- Giorni della settimana— Selezionare il giorno o i giorni durante ogni settimana in cui si desidera applicare l'intervallo. È possibile applicare l'intervallo nei giorni feriali (dal lunedì al venerdì), nei fine settimana (sabato e domenica), tutti i giorni della settimana o in un giorno specifico ogni settimana. Per applicare il limite di larghezza di banda in modo uniforme e costante in tutti i giorni e in ogni momento, scegliNessun programma.
- Ora di inizio— Immettere l'ora di inizio per l'intervallo di larghezza di banda, utilizzando il formato HH:MM e l'offset del fuso orario da UTC per il gateway.

  > **Note**
  >
  > L'intervallo limite di larghezza di banda inizia all'inizio del minuto specificato qui.

- Ora di fine— Immettere l'ora di fine dell'intervallo di larghezza di banda, utilizzando il formato HH:MM e l'offset del fuso orario da GMT per il gateway.

  > **Important**
  >
  > L'intervallo limite di larghezza di banda termina alla fine del minuto specificato qui. Per pianificare un intervallo che termina alla fine di un'ora, immettere**59**.
  > Per programmare intervalli continui consecutivi, la transizione all'inizio dell'ora, senza interruzioni tra gli intervalli, inserire**59**per il minuto finale del primo intervallo. Invio**00**per il minuto iniziale dell'intervallo successivo.

5. (Facoltativo) Ripetere la fase precedente finché non è completa la pianificazione del limite di velocità della larghezza di banda. Se devi eliminare un intervallo dalla pianificazione, scegliRemove.

   > **Important**
   >
   > Gli intervalli limite di larghezza di banda non possono sovrapporsi. L'ora di inizio di un intervallo deve avvenire dopo l'ora di fine di un intervallo precedente e prima dell'ora di inizio di un intervallo successivo.

6. Al termine, scegliSalva le modifiche.

Aggiornamento dei limiti di velocità della larghezza di banda del gateway con l'AWS SDK for Java

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare questi limiti automaticamente per un periodo di tempo, ad esempio usando attività pianificate. L'esempio seguente illustra come aggiornare i limiti di velocità della larghezza di banda di un gateway usando l'AWS SDK for Java. Per usare il codice di esempio, devi avere familiarità con l'esecuzione di un'applicazione di console Java. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di AWS SDK for Java.

Example : Aggiornamento dei limiti di velocità della larghezza di banda del gateway utilizzandoAWS SDK for Java

L'esempio di codice Java seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per avvalersi di questo codice di esempio, è necessario fornire l'endpoint del servizio, l'ARN (Amazon Resource Name) del gateway e il limite di caricamento. Per un elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

```
   import java.io.IOException;

   import com.amazonaws.AmazonClientException;
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

       // The gatewayARN
       public static String gatewayARN = "*** provide gateway ARN ***";

       // The endpoint
```

```
        static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

        // Rates
        static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

        public static void main(String[] args) throws IOException {

            // Create a storage gateway client
            sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
            sgClient.setEndpoint(serviceURL);

            UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File gateways

        }

        private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
            try
            {
                BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
```

```
                String returnGatewayARN =
updateBandwidthRateLimitScheduleResponse.getGatewayARN();
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

Aggiornamento dei limiti di velocità della larghezza di banda del gateway con l'AWS SDK for .NET

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare questi limiti automaticamente per un periodo di tempo, ad esempio usando attività pianificate. L'esempio seguente illustra come aggiornare i limiti di velocità della larghezza di banda di un gateway usando l'AWSSoftware Development Kit (SDK) per .NET. Per usare il codice di esempio, devi avere familiarità con l'esecuzione di un'applicazione di console .NET. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di AWS SDK for .NET.

Example : Aggiornamento dei limiti di velocità della larghezza di banda del gateway utilizzandoAWS SDK for .NET

L'esempio di codice C# seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per avvalersi di questo codice di esempio, è necessario fornire l'endpoint del servizio, l'ARN (Amazon Resource Name) del gateway e il limite di caricamento. Per un elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;
```

```
    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

            // The gatewayARN
            public static String gatewayARN = "*** provide gateway ARN ***";

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a storage gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
 BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
 BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
```

```
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

Aggiornamento dei limiti di velocità della larghezza di banda del gateway con l'AWS Tools for Windows PowerShell

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare questi limiti automaticamente per un periodo di tempo, ad esempio usando attività pianificate. L'esempio seguente illustra come aggiornare i limiti di velocità della larghezza di banda di un gateway usando l'AWS Tools for Windows PowerShell. Per usare il codice di esempio, devi avere familiarità con l'esecuzione di uno script di PowerShell. Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS Tools for Windows PowerShell.

Example : Aggiornamento dei limiti di velocità della larghezza di banda del gateway utilizzandoAWS Tools for Windows PowerShell

Lo script di PowerShell seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per utilizzare questo script di esempio, devi specificare l'ARN (Amazon Resource Name) del gateway e il limite di caricamento.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


    .EXAMPLE
        powershell.exe .\SG_UpdateBandwidth.ps1
    #>

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
    $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
 $UploadBandwidthRate

    #Update Bandwidth Rate Limits
    Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                        -BandwidthRateLimitInterval
 @($bandwidthRateLimitInterval)

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN
```

```
    Write-Output("`nGateway: " + $gatewayARN);
    Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Gestione degli aggiornamenti del gateway tramite la console AWS Storage Gateway

Storage Gateway rende periodicamente disponibili importanti aggiornamenti software per il gateway. Puoi applicare manualmente gli aggiornamenti nella Storage Gateway Management Console, altrimenti attendere che gli aggiornamenti vengano applicati automaticamente durante il periodo di manutenzione configurato. Anche se Storage Gateway controlla la presenza di aggiornamenti ogni minuto, esegue la manutenzione e il riavvio solo se sono presenti nuovi aggiornamenti.

Le versioni del software gateway includono regolarmente aggiornamenti del sistema operativo e patch di sicurezza che sono state convalidate daAWS. Questi aggiornamenti vengono generalmente rilasciati ogni sei mesi e vengono applicati come parte del normale processo di aggiornamento del gateway durante le finestre di manutenzione pianificata.

> **Note**
>
> È consigliabile trattare l'appliance Storage Gateway come un dispositivo integrato gestito e non tentare di accedere o modificare in alcun modo l'installazione. Il tentativo di installare o aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del gateway (ad esempio, strumenti SSM o hypervisor) può causare un malfunzionamento del gateway.

Prima di applicare qualsiasi aggiornamento al gateway,AWSinvia una notifica con un messaggio sulla console Storage Gateway e sul tuoAWS Health Dashboard. Per ulteriori informazioni, consultare AWS Health Dashboard. La macchina virtuale non si riavvia, mentre il gateway non è disponibile per un breve periodo mentre viene aggiornato e riavviato.

Quando distribuisci e attivi il gateway, viene impostata una pianificazione di manutenzione settimanale predefinita. Puoi modificare la pianificazione di manutenzione in qualsiasi momento. Quando gli aggiornamenti sono disponibili, nella scheda Details (Dettagli) viene visualizzato un messaggio di manutenzione. Puoi visualizzare la data e l'ora in cui è stato applicato l'ultimo aggiornamento al gateway nella scheda Details (Dettagli).

Per modificare la pianificazione di manutenzione

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere Gateways (Gateway), quindi scegliere il gateway per cui si vuole modificare la pianificazione degli aggiornamenti.
3. Nel menu Actions (Operazioni), scegliere Edit maintenance window (Modifica finestra di manutenzione) per scrivere nella finestra di dialogo Edit maintenance start time (Modifica ora di inizio manutenzione).
4. Per Schedule (Pianificazione), scegliere Weekly (Settimanale) o Monthly (Mensile) per pianificare gli aggiornamenti.
5. Se si sceglie Weekly (Settimanale), modificare i valori per Day of the week (Giorno della settimana) e Time (Ora).

   Se si sceglie Monthly (Mensile), modificare i valori per Day of the month (Giorno del mese) e Time (Ora). Se si sceglie questa opzione e viene visualizzato un errore, significa che il gateway è una versione precedente e non è ancora stato aggiornato a una versione più recente.

   > **Note**
   >
   > Il valore massimo che può essere impostato per il giorno del mese è 28. Se viene selezionato 28, l'orario di inizio della manutenzione sarà il 28° giorno di ogni mese.

   Il tempo di avvio di manutenzione viene visualizzato nella scheda Details (Dettagli) per il gateway la prossima volta che si apre la scheda Details (Dettagli).

Esecuzione delle operazioni di manutenzione sulla console locale

Con la console locale dell'host è possibile svolgere le seguenti operazioni di manutenzione. Le operazioni della console locale possono essere eseguite sull'host della VM o sull'istanza Amazon EC2. Molte operazioni sono comuni ai vari host, ma non mancano delle differenze.

Argomenti

- Esecuzione di attività nella console locale della VM (gateway del file)
- Esecuzione di attività sulla console locale Amazon EC2 (gateway di file)

- Accesso alla console locale del gateway
- Configurazione delle schede di rete per il gateway

Esecuzione di attività nella console locale della VM (gateway del file)

Per un gateway del file distribuito in locale, è possibile eseguire le attività di manutenzione qui elencate, utilizzando la console locale dell'host della VM. Queste attività sono comuni agli hypervisor di VMware, Microsoft Hyper-V e macchine virtuali basate su Kernel (KVM) Linux.

Argomenti

- Accesso alla console locale del gateway del file
- Configurazione di un proxy HTTP
- Configurazione delle impostazioni di rete gateway
- Test della connettività di rete del gateway
- Visualizzazione dello stato delle risorse del sistema gateway
- Configurazione di un server NTP (Network Time Protocol) per il gateway
- Esecuzione di comandi gateway di storage sulla console locale
- Configurazione delle schede di rete per il gateway

Accesso alla console locale del gateway del file

Quando la VM è pronta per l'accesso, è visualizzata la schermata di autenticazione. Per il primo accesso alla console locale, si utilizzano il nome utente e la password predefiniti. Queste credenziali predefinite consentono di accedere a menu in cui è possibile configurare le impostazioni di rete del gateway e modificare la password dalla console locale.AWS Storage Gatewayti consente di impostare una password dalla console Storage Gateway invece di modificarla dalla console locale. Non è necessario conoscere la password predefinita per impostarne una nuova. Per ulteriori informazioni, consultare Accesso alla console locale del gateway del file.

Come accedere alla console locale del gateway

- Per il primo accesso alla console locale, accedere alla VM con le credenziali predefinite. Il nome utente predefinito è `admin` e la password è `password`. Negli altri casi, accedere con le proprie credenziali.

> **Note**
>
> Consigliamo di modificare la password predefinita. A tale scopo, eseguire il comando `passwd` dal menu della console locale (voce 6 del menu principale). Per informazioni su come eseguire il comando, consulta Esecuzione di comandi gateway di storage sulla console locale. È inoltre possibile impostare la password dalla console Storage Gateway. Per ulteriori informazioni, consultare Accesso alla console locale del gateway del file.

Impostazione della password della console locale dalla console Storage Gateway

Per il primo accesso alla console locale, accedere alla VM con le credenziali predefinite. Utilizzare le credenziali predefinite per tutti i tipi di gateway. Il nome utente è `admin` e la password è `password`.

È consigliabile impostare sempre una nuova password immediatamente dopo aver creato il nuovo gateway. A tale scopo, se preferisci, puoi avvalerti della console AWS Storage Gateway anziché di quella locale. Non è necessario conoscere la password predefinita per impostarne una nuova.

Per impostare la password della console locale sulla console Storage Gateway

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, selezionare Gateways (Gateway), poi scegliere il gateway per cui impostare la 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 quella predefinita. Storage Gateway non salva la password, ma la trasmette in modo sicuro alla VM.

> **Note**
>
> La password può includere da 1 a 512 caratteri presenti sulla tastiera.

Configurazione di un proxy HTTP

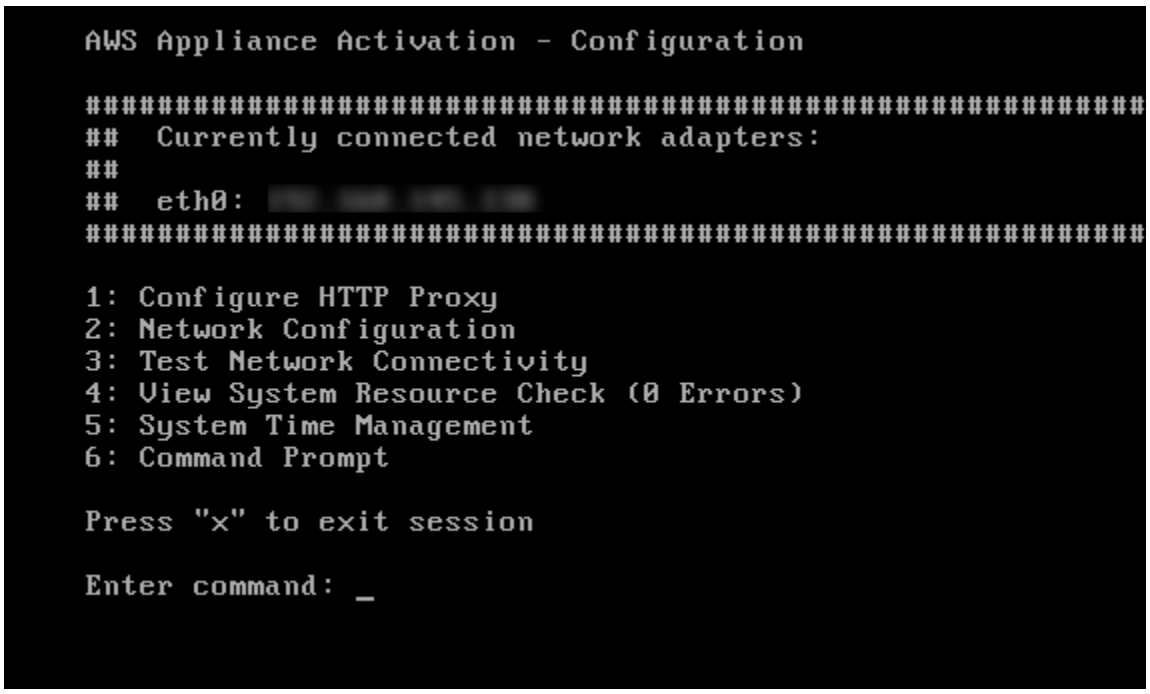
I gateway del file supportano la configurazione di un proxy HTTP.

> **Note**
>
> L'unica configurazione di proxy che i gateway del file supportano è HTTP.

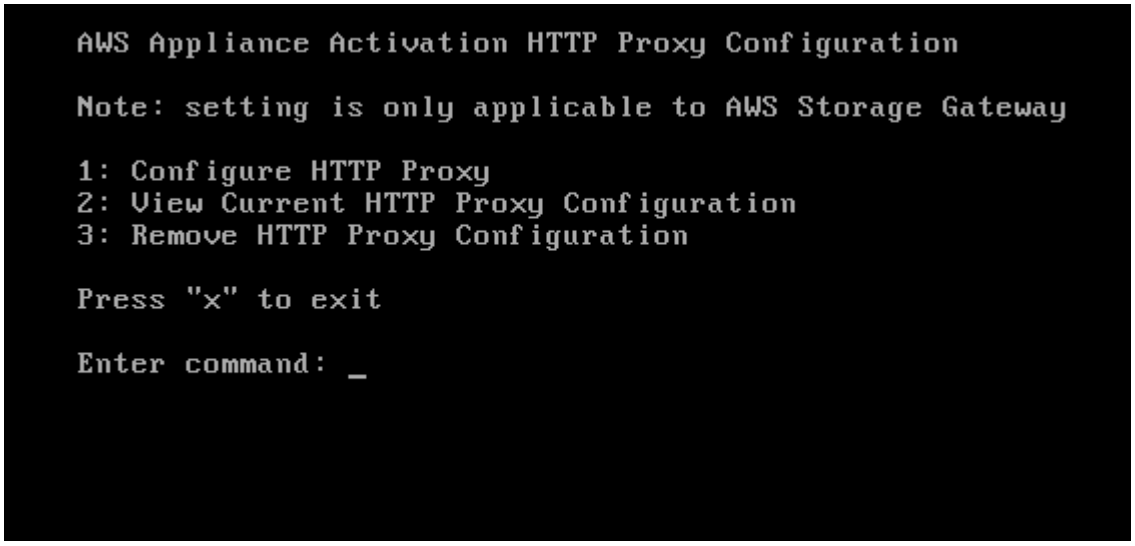
Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopodiché, Storage Gateway instraderà tuttoAWStraffico endpoint tramite 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 gateway di file

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console locale di VMware ESXi, consultare 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 per la macchina virtuale basata su kernel Linux (KVM), consulta Accesso alla console locale del gateway con Linux KVM.
2. SulAWSAttivazione appliance - Configurazionemenu principale, entra**1**per iniziare a configurare il proxy HTTP.



3. Nel menu di configurazione del proxy HTTP, inserire **1** e fornire il nome host per il server proxy HTTP.



Puoi configurare le altre impostazioni HTTP da questo menu come illustrato qui di seguito.

Per	Eseguire questa operazione
Configurare un proxy HTTP	Specificare (sì **1**.

Per	Eseguire questa operazione
	È necessario specificare il nome host e la porta per completare la configurazione.
Visualizzare l'attuale configurazione del proxy HTTP	Specificare (sì **2**. Se un proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured` . In caso contrario, vengono visualizzati il nome host e la porta del proxy HTTP.
Rimuovere la configurazione di un proxy HTTP	Specificare (sì **3**. Viene visualizzato il messaggio `HTTP Proxy Configuration Removed`

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

Configurazione delle impostazioni di rete gateway

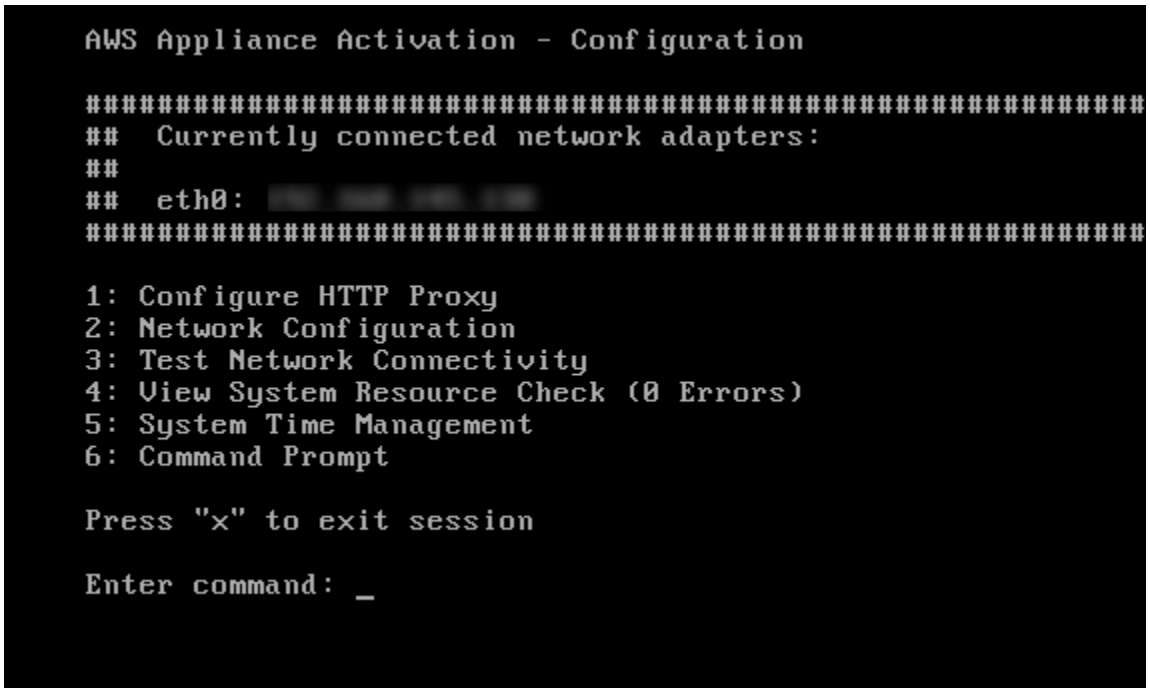
L'impostazione predefinita per la configurazione di rete del gateway è DHCP (Dynamic Host Configuration Protocol). Con DHCP, al gateway viene assegnato automaticamente un indirizzo IP. In alcuni casi, può essere necessario assegnare manualmente un indirizzo IP statico al gateway, come descritto di seguito.

Per configurare il gateway affinché utilizzi indirizzi IP statici

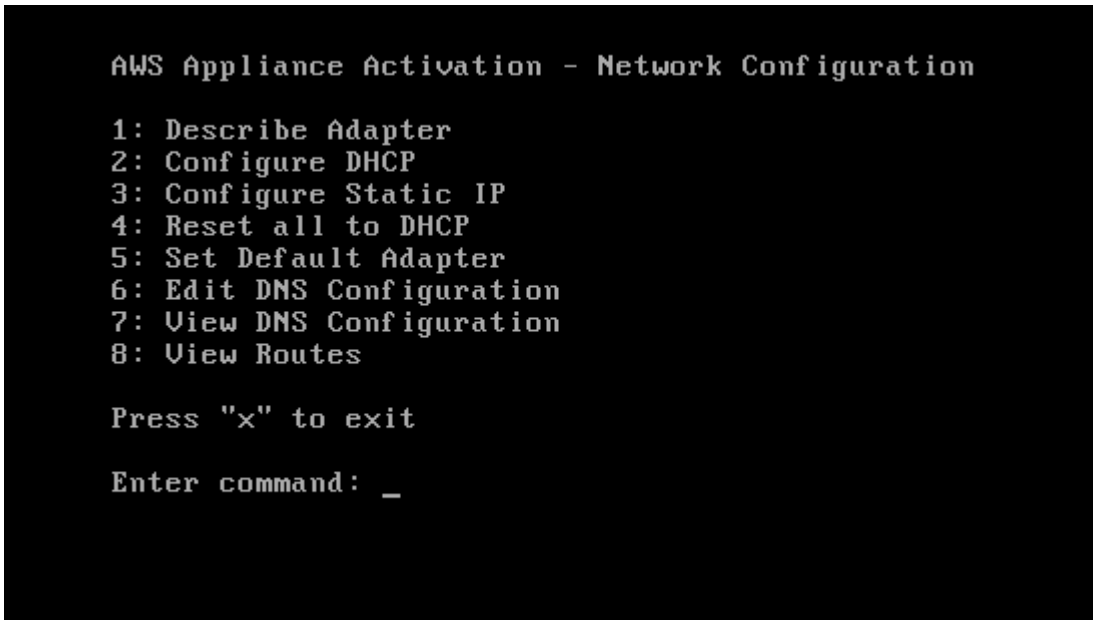
1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla console locale di VMware ESXi, consultare 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. SulAWSAttivazione appliance - Configurazionemenu principale, entra**2**per iniziare a configurare la rete.

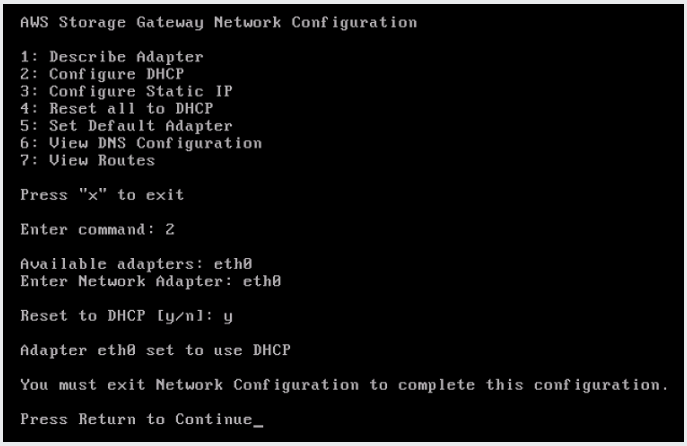


3. Scegliere una delle seguenti opzioni dal menu Network Configuration (Configurazione di rete).



Per	Eseguire questa operazione
Ottenere informazioni sulla scheda di rete	Specificare (sì **1**.

Per	Eseguire questa operazione
	Viene visualizzato un elenco di nomi di schede e viene richiesto di immettere un nome per la scheda, ad esempio**`eth0`**. Se la scheda specificata è in uso, vengono mostrate le seguenti informazioni: • Indirizzo MAC (Media Access Control) • Indirizzo IP • Netmask • Indirizzo IP del gateway • Stato DHCP abilitato È possibile utilizzare lo stesso nome di scheda quando si configura un indirizzo IP statico (opzione 3) e quando si imposta la scheda di routing predefinita del gateway (opzione 5).

Per	Eseguire questa operazione
Configurazione di DHCP	Specificare (sì **2**. Per l'utilizzo di DHCP, viene richiesto di configurare l'interfaccia di rete. 

Per	Eseguire questa operazione
Configurare un indirizzo IP statico per il gateway	Specificare (sì **3**. Per configurare un indirizzo IP statico, viene chiesto di digitare le informazioni riportate di seguito: • Nome scheda di rete • 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, consultare Spegnimento della macchina virtuale del gateway. Se il gateway utilizza più di un'interfaccia di rete, è necessario impostare tutte le interfacc

Per	Eseguire questa operazione
	e abilitate all'utilizzo di DHCP o di 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 disabilitata. Per riabilitarla, 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.
Reimpostare tutte le configurazioni di rete del gateway su DHCP	Specificare (sì **4**. 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 informazi oni, consultare Spegnimento della macchina virtuale del gateway.

Per	Eseguire questa operazione
Impostare l'adattatore di routing predefinito del gateway	Specificare (sì **5**. Sono mostrate le schede disponibili per il gateway e viene richiesto di scegliere una delle schede, ad esempio**`eth0`**.
Modificare la configurazione DNS del gateway	Specificare (sì **6**. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. Viene richiesto di fornire il nuovo indirizzo IP.
Visualizzare la configurazione DNS del gateway	Specificare (sì **7**. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. **Note** Per alcune versioni dell'hypervisor VMware, è possibile modificare la configurazione della scheda in questo menu.
Visualizzare le tabelle di routing	Specificare (sì **8**. Viene visualizzato l'instradamento predefinito del gateway.

Test della connettività di rete del gateway

Avvalendoti della console locale del gateway, puoi testare la connettività di rete. e conseguentemente 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 locale di VMware ESXi, consultare 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. DalAWSAttivazione appliance - Configurazionemenu principale, inserisci il numero corrispondente da selezionareConnettività 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 eRegione AWScome descritto nei seguenti passaggi.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se è stato selezionato il tipo di endpoint pubblico, immettere il numero corrispondente per selezionareRegione AWSche vuoi testare. Per supportatoRegioni AWSe elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

Man mano che il test progredisce, ogni endpoint viene visualizzato[PASSATO]o[FAILED]indicante lo stato della connessione nel modo seguente:

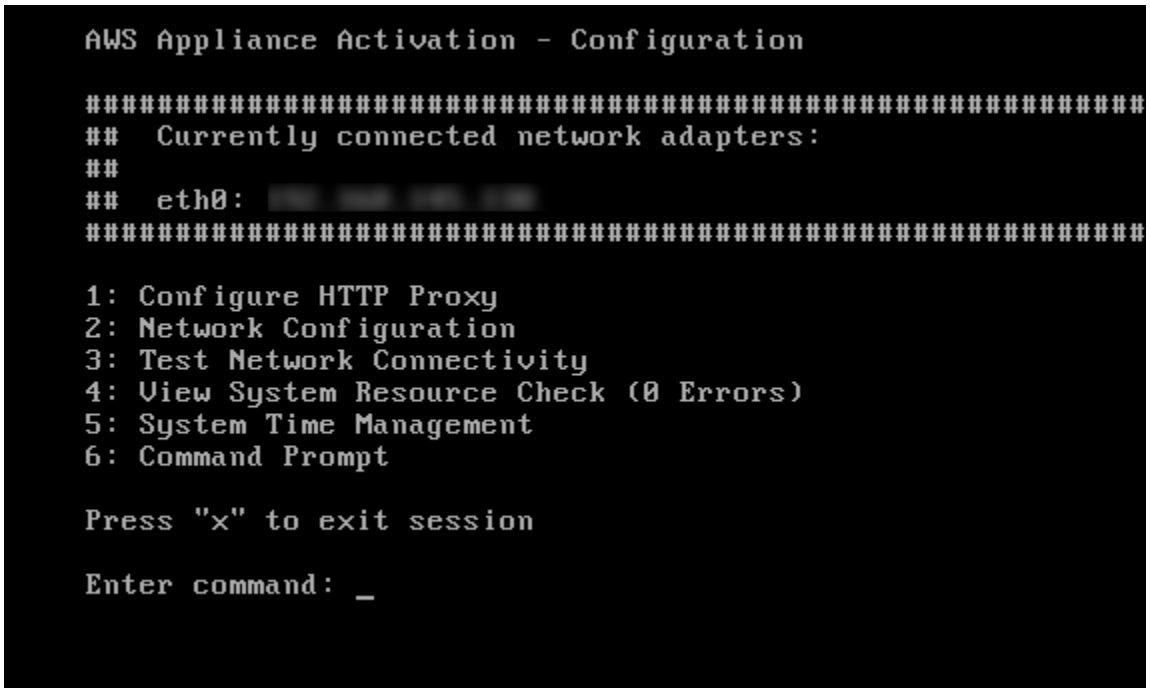
Messaggio	Descrizione
[PASSED]	Storage Gateway ha connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato delle risorse del sistema 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 console di VMware ESXi, consultare 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. NellaAWSAttivazione appliance - Configurazionemenu principale, entra**4**per visualizzare i risultati di un controllo delle risorse di sistema.



La console visualizza un messaggio [OK], [WARNING] ([ATTENZIONE]) o [FAIL] ([ESITO NEGATIVO]) per ogni risorsa, come descritto nella tabella seguente.

Messaggio	Descrizione
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti raccomand ati, ma il gateway continuerà 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 correttam ente. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.

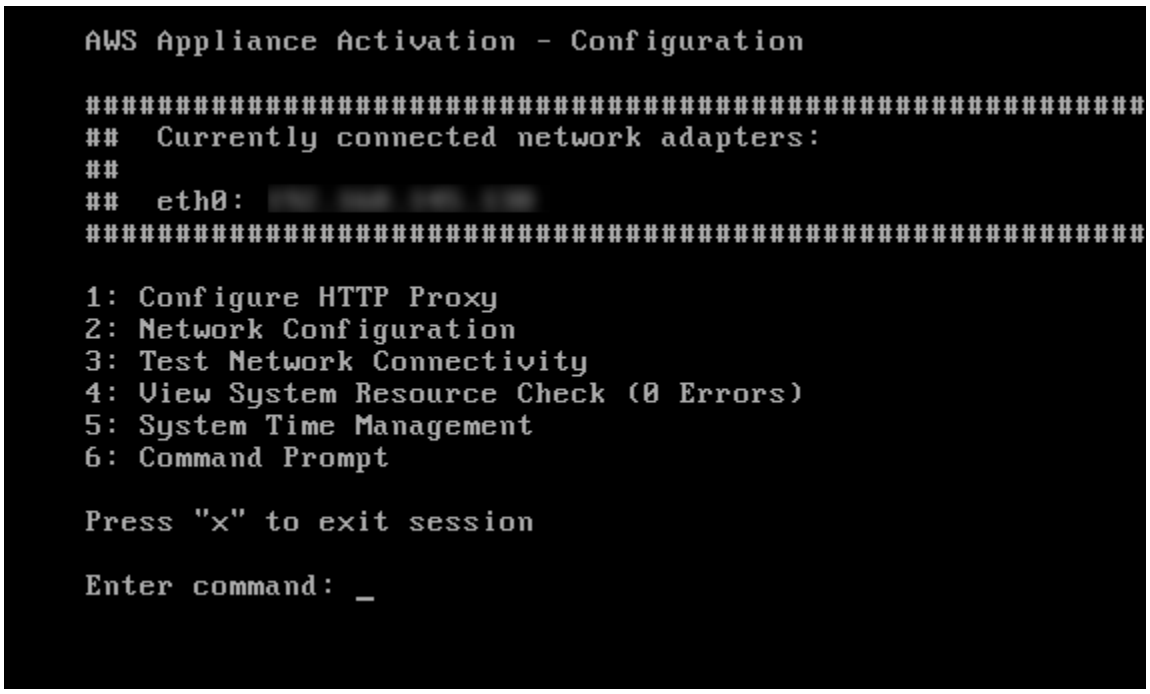
La console visualizza inoltre il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

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

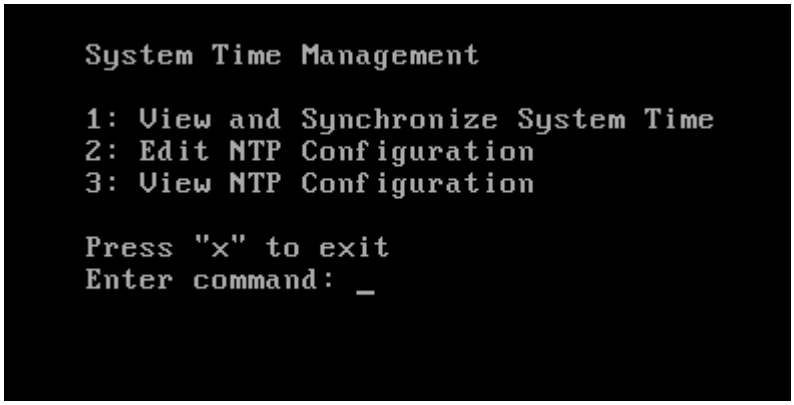
Puoi visualizzare e modificare le configurazioni del server Network Time Protocol (NTP) e sincronizzare l'ora della VM associata al gateway con l'host dell'hypervisor.

Per gestire l'ora di sistema

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console locale di VMware ESXi, consultare 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. NellaAWSAttivazione appliance - Configurazionemenu principale, entra**5**per gestire il tempo del sistema.



3. Nel menu System Time Management (Gestione dell'ora del sistema), selezionare una delle seguenti opzioni.



Per	Eseguire questa operazione
Visualizza e sincronizza l'ora della VM con quella del server NTP.	Specificare (sì **1**. Viene visualizzata l'ora corrente della VM. Il gateway del file stabilisce la differenza temporale rispetto all'ora della VM del gateway e il server NTP ti invita a sincronizzare i due orari (VM e NTP).

Per	Eseguire questa operazione
	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 effettiva alla quale le operazioni vengono eseguite. In caso di gateway distribuito su VMware ESXi, per evitare scostamenti temporali basta impostare l'ora dell'host dell'hypervisor e sincronizzazione l'ora della VM con quella dell'host. Per ulteriori informazioni, consultar e Sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host. In caso, invece, di gateway distribuito su Microsoft Hyper-V, è necessario controllare periodicamente l'ora impostata sulla VM. Per ulteriori informazioni, consultare Sincroniz zazione dell'ora della VM associata al gateway. 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.

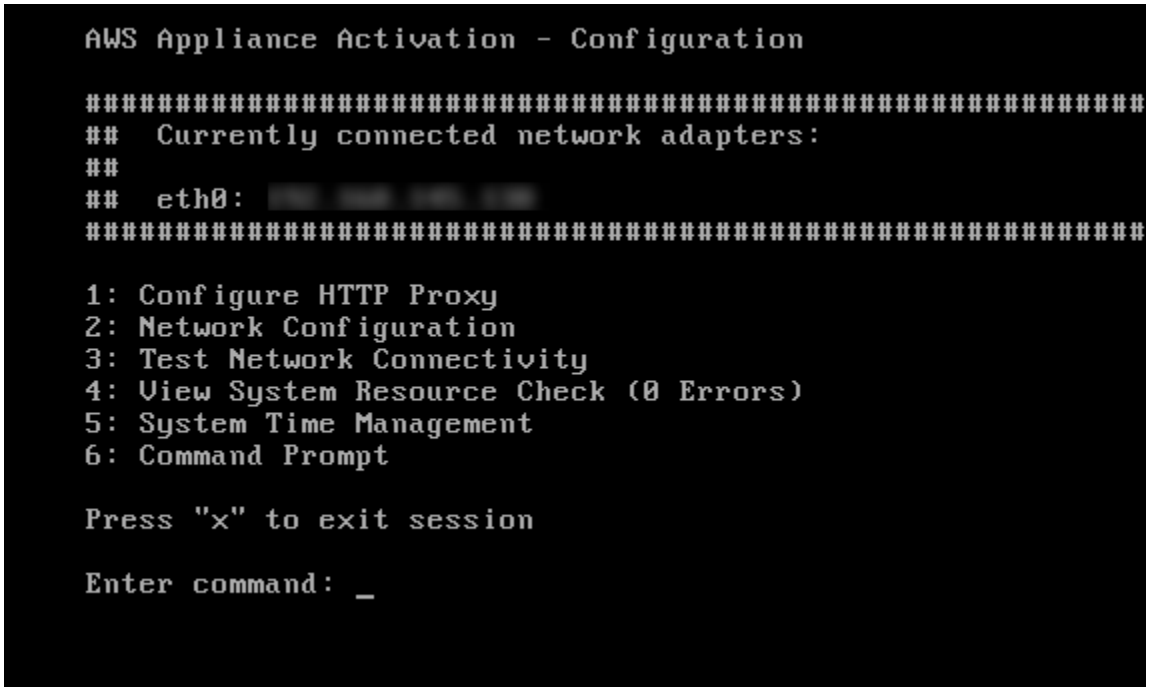
Per	Eseguire questa operazione
Modifica della configurazione del server NTP	Specificare (sì **2**. Ti viene richiesto di fornire un server NTP preferito e un server secondario.
Visualizzazione della configurazione del server NTP	Specificare (sì **3**. Viene visualizzata la configurazione del server NTP.

Esecuzione di comandi gateway di storage 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 operazioni di manutenzione come ad esempio il salvataggio delle tabelle di routing, la connessione al Support Amazon Web Services e così via.

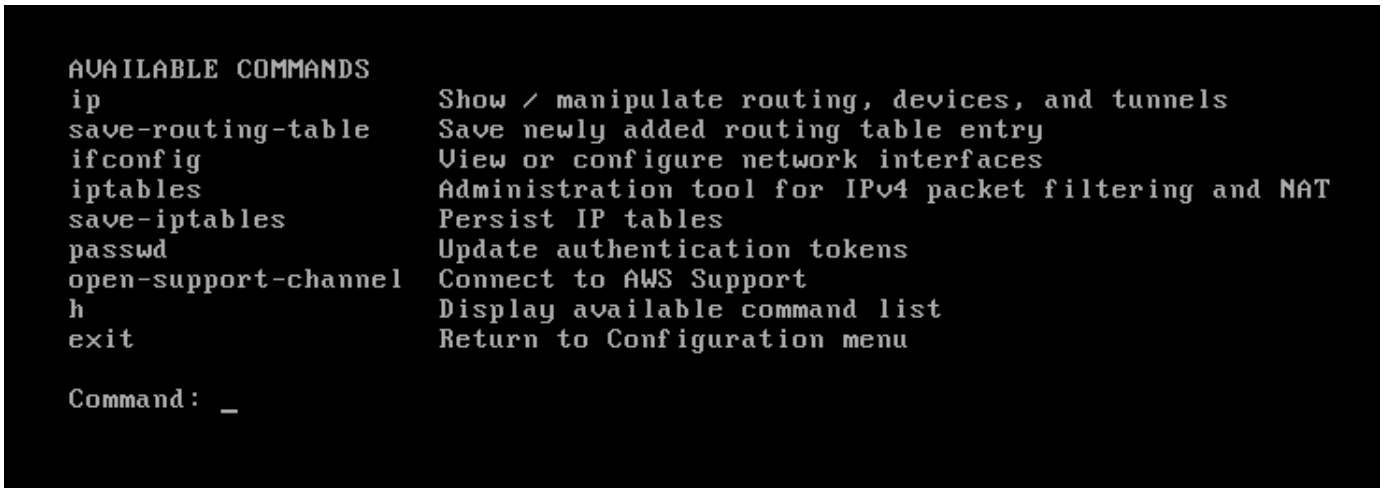
Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console locale di VMware ESXi, consultare 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. SulAWSAttivazione appliance - Configurazionemenu principale, entra**6**perPrompt dei comandi.



3. SulAWSAttivazione appliance - prompt dei comandiconsole, entra**h**, quindi premere il pulsanteRestituiscichiave.

   La console mostra il menu AVAILABLE COMMANDS (COMANDI DISPONIBILI) con ciò che fanno i comandi, come illustrato nella schermata seguente.



4. Al prompt dei comandi, inserire il comando che desideri utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitare il nome del comando nel prompt di comando.

Configurazione delle schede di rete per il gateway

La configurazione predefinita di Storage Gateway prevede l'utilizzo della scheda di rete E1000, ma è possibile riconfigurare il gateway per avvalersi della scheda di rete VMXNET3 (10 GbE). È anche possibile configurare Storage Gateway per accedervi da più di un indirizzo IP. A tale scopo, configura il gateway per l'utilizzo di più schede di rete.

Argomenti

Configurazione del gateway per l'utilizzo della scheda di rete VMXNET3

Storage Gateway supporta la scheda di rete di tipo E1000 negli host degli hypervisor VMware ESXi e Microsoft Hyper-V. Tuttavia, la scheda VMXNET3 (10 GbE) è supportata solo dall'hypervisor VMware ESXi. Se il gateway è in hosting su un hypervisor VMware ESXi, puoi riconfigurarlo affinché utilizzi la scheda VMXNET3 (10 GbE). Per ulteriori informazioni su questa scheda, consulta il sito web di VMware.

Per gli host hypervisor KVM, Storage Gateway supporta l'utilizzo di`virtio`driver di dispositivi di rete. L'utilizzo del tipo di scheda di rete E1000 per gli host KVM non è supportato.

> **Important**
>
> Per selezionare VMXNET3, il sistema operativo guest deve essere di tipo Other Linux64 (Altro Linux64).

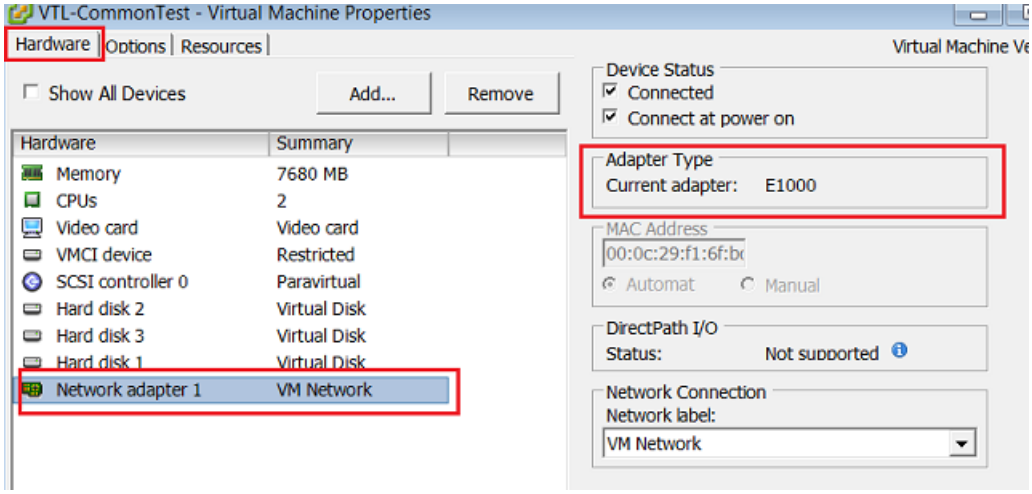
Passaggi necessari per configurare il gateway affinché utilizzi la scheda VMXNET3:

1. Rimuovere la scheda E1000 predefinita.
2. Aggiungere la rete VMXNET3.
3. Riavviare il gateway.
4. Configurare la scheda per la rete.

Seguono informazioni dettagliate su ogni passaggio.

Per rimuovere la scheda E1000 predefinita e configurare il gateway affinché utilizzi la scheda VMXNET3

1. In VMware, aprire il menu contestuale (con il pulsante destro del mouse) per il gateway e scegliere Edit Settings (Modifica impostazioni).
2. Nella finestra Virtual Machine Properties (Proprietà macchina virtuale), selezionare la scheda Hardware (Hardware).
3. Per Hardware, scegliere Network adapter (Scheda di rete). Nella sezione Adapter Enter (Tipo di scheda) è riportata l'attuale scheda E1000. Questa scheda deve essere sostituita con la VMXNET3.



4. Selezionare prima la scheda di rete E1000 e poi Remove (Rimuovi). In questo esempio, la scheda di rete E1000 è la Network adapter 1 (Scheda di rete 1).

> **Note**
>
> Sebbene sia possibile, è preferibile non eseguire contemporaneamente entrambe le schede di rete (E1000 e VMXNET3) nel gateway, per evitare problemi di rete.

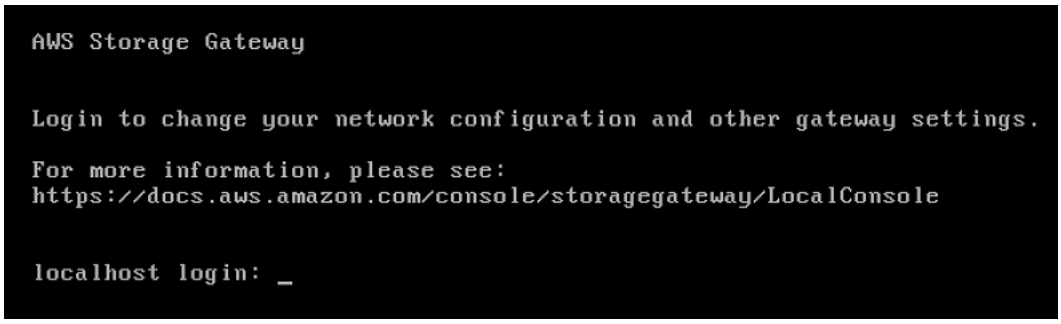
5. Scegliere Add (Aggiungi) per avviare la procedura guidata di aggiunta dell'hardware.
6. Selezionare prima Ethernet Adapter (Scheda Ethernet) e poi Next (Avanti).
7. Nel corso della procedura guidata, scegliere **`VMXNET3`** come Adapter Enter (Tipo di scheda), quindi selezionare Next (Avanti).
8. Nel corso della procedura guidata dedicata alle proprietà della macchina virtuale, verificare che, nella sezione Adapter Enter (Tipo di rete), il parametro Current Adapter (Rete attuale) sia impostato su VMXNET3 (VMXNET3), poi selezionare OK (OK).

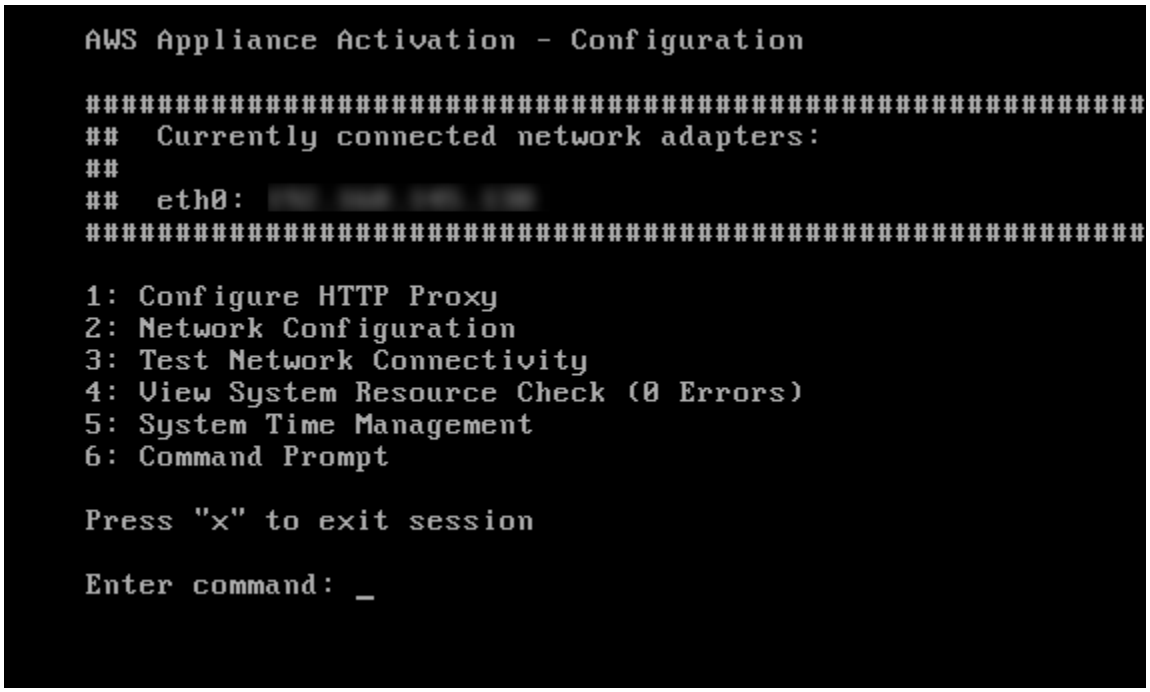
9. Nel client VMware VSphere, arrestare il gateway.
10. Nel client VMware VSphere, riavviare il gateway.

Dopo il riavvio del gateway, riconfigurare la scheda appena aggiunta per accertarsi della connettività di rete a Internet.

Come configurare la scheda di rete

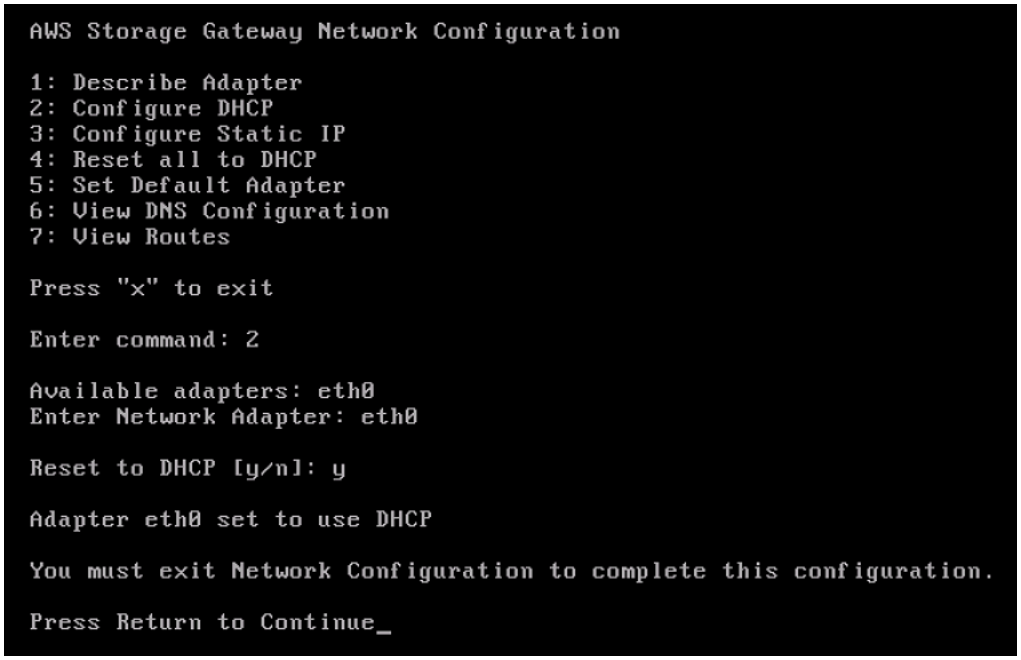
1. Nel client VSphere, scegliere la scheda Console per avviare la console locale. Per eseguire la configurazione basta accedere alla console locale del gateway con le credenziali predefinite. Per ulteriori informazioni su come accedere con le credenziali predefinite, consulta Accesso alla console locale del gateway del file.





2. Al prompt, digitare **2** per selezionare Network Configuration (Configurazione di rete), poi premere **`Enter`** (Invio) per aprire il menu della configurazione di rete.

3. Al prompt, digitare **4** per selezionare Reset all to DHCP (Reimposta tutto su DHCP), quindi digitare **y** (ossia "yes", sì) al prompt successivo affinché tutte le schede utilizzino il protocollo DHCP (Dynamic Host Configuration Protocol). Tutte le schede disponibili sono impostate per l'utilizzo di DHCP.



   Se il gateway è già stato attivato, è necessario arrestarlo e riavviarlo dalla Storage Gateway Management Console. Dopo il riavvio del gateway, bisogna testare la connettività di rete a Internet. Per informazioni su come testare la connettività di rete, consulta Test della connettività di rete del gateway.

Esecuzione di attività sulla console locale Amazon EC2 (gateway di file)

Alcune attività di manutenzione richiedono di effettuare l'accesso alla console locale durante l'esecuzione di un gateway distribuito in un'istanza Amazon EC2. Questa sezione include informazioni su come effettuare l'accesso alla console locale ed eseguire attività di manutenzione.

Argomenti

- Accesso alla console locale del gateway Amazon EC2
- Instradamento del gateway distribuito su EC2 tramite un proxy HTTP
- Configurazione delle impostazioni di rete gateway
- Test della connettività di rete del gateway
- Visualizzazione dello stato delle risorse del sistema gateway

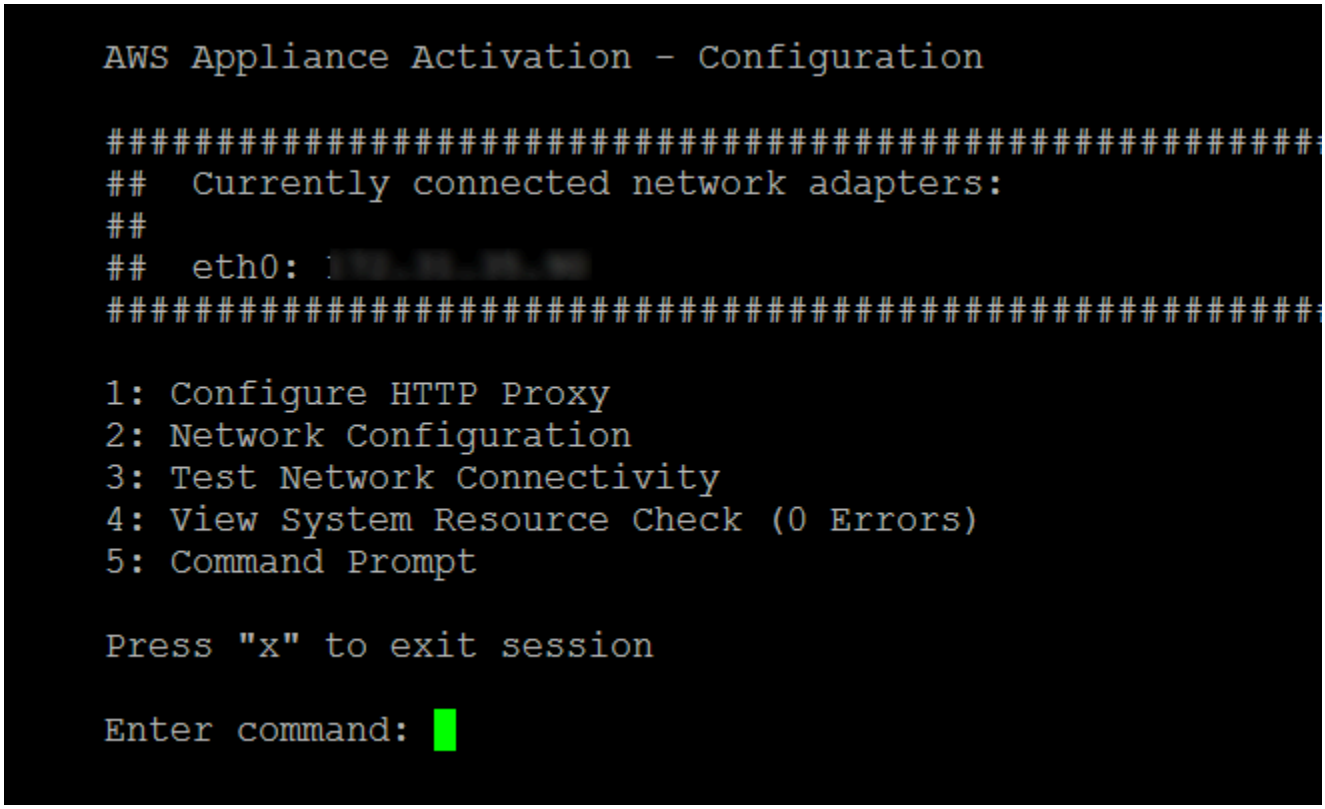
- Esecuzione di comandi Storage Gateway sulla console locale

Accesso alla console locale del gateway Amazon EC2

Puoi connetterti all'istanza Amazon EC2 usando un client SSH (Secure Shell). Per informazioni dettagliate, consultaConnessione all'istanzanellaGuida per l'utente di Amazon EC2. 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, consultaCoppia di chiavi Amazon EC2nellaGuida per l'utente di Amazon EC2.

Per accedere alla console locale del gateway

1. Accedere alla console locale. Se ci si connette all'istanza EC2 da un computer Windows, accedere come amministratore.
2. Dopo aver eseguito il login, viene visualizzato ilAWSAttivazione appliance - Configurazionemenu principale, come mostrato nello screenshot seguente.



Per ulteriori informazioni	vedere questo argomento
Configurare un proxy HTTP per il gateway	Instradamento del gateway distribuito su EC2 tramite un proxy HTTP
Configurazione delle impostazioni di rete per il gateway	Test della connettività di rete del gateway
Verificare la connettività di rete	Test della connettività di rete del gateway
Visualizzare un controllo delle risorse di sistema	Accesso alla console locale del gateway Amazon EC2.
Esegui comandi della console Storage Gateway	Esecuzione di comandi Storage Gateway sulla console locale

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

Per uscire dalla sessione di configurazione, digitare **x** per chiudere il menu.

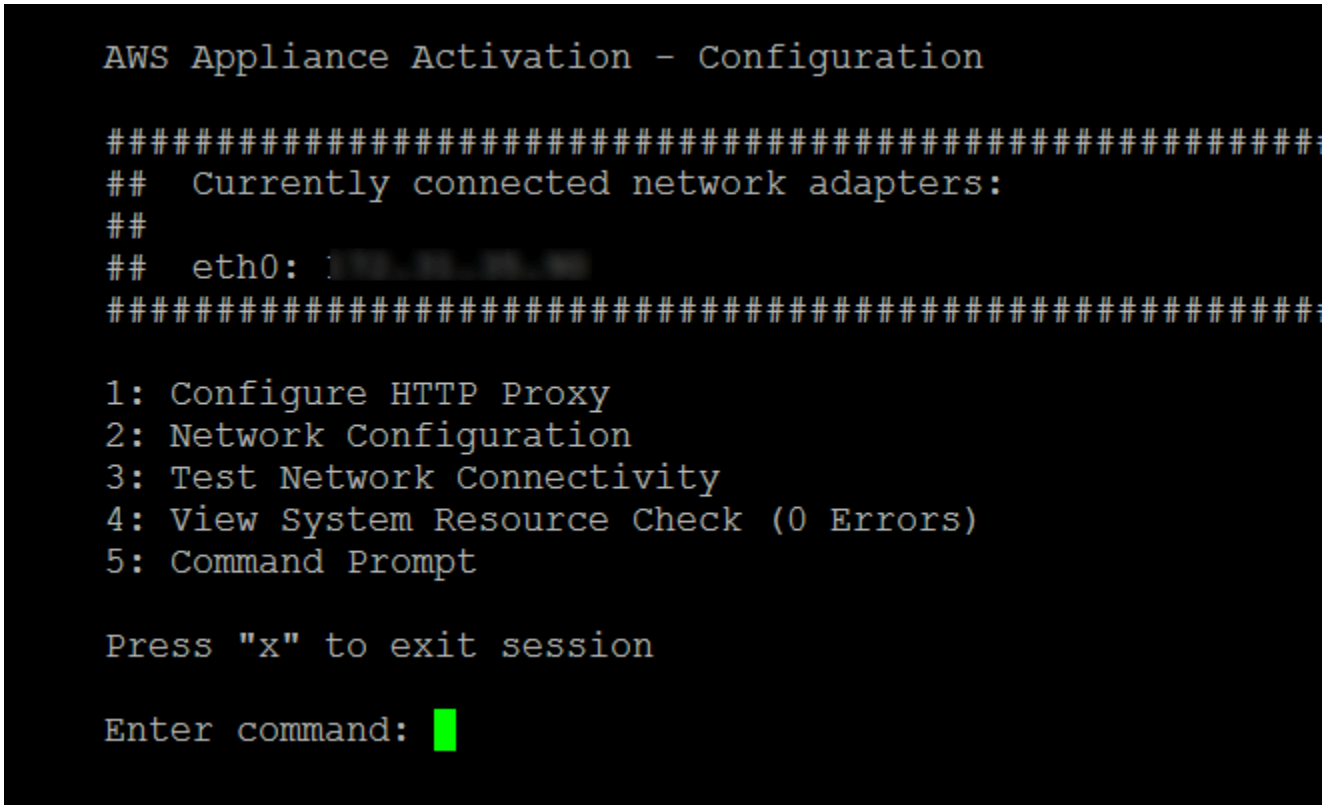
Instradamento del gateway distribuito su EC2 tramite un proxy HTTP

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

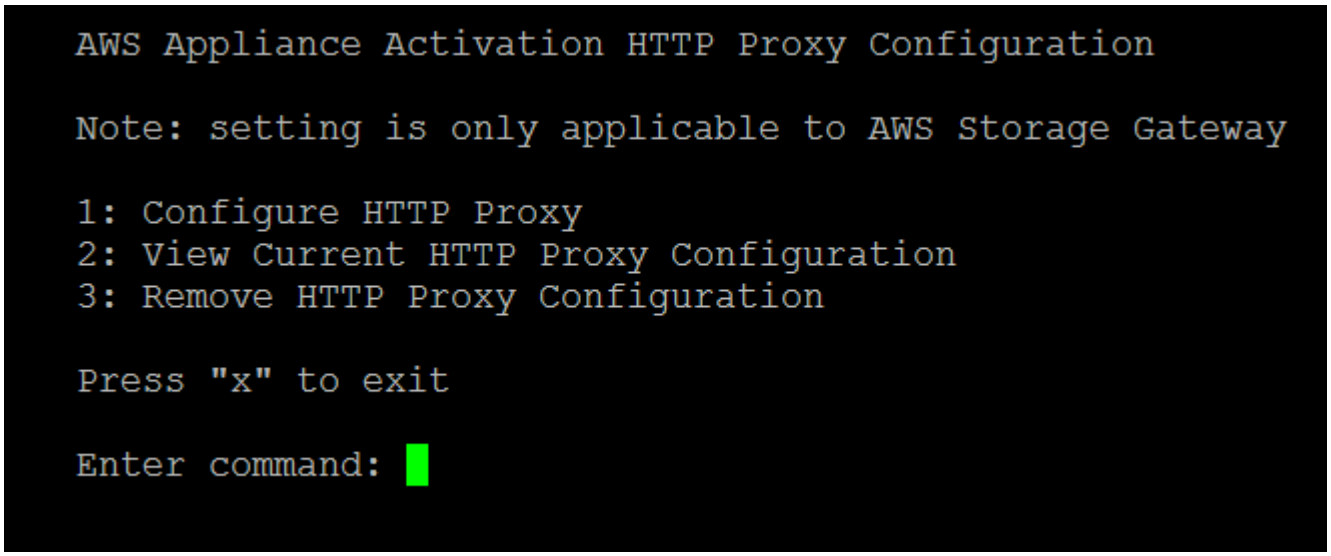
Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopodiché, Storage Gateway instraderà tuttoAWStraffico endpoint tramite 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, consultare Accesso alla console locale del gateway Amazon EC2.
2. SulAWSAttivazione appliance - Configurazionemenu principale, entra**1**per iniziare a configurare il proxy HTTP.



3. Seleziona una delle seguenti opzioni nellaAWSAttivazione appliance - ConfigurazioneConfigurazione di un proxy HTTPmenu.



Per	eseguire questa operazione
Configurare un proxy HTTP	Specificare (sì **1**.

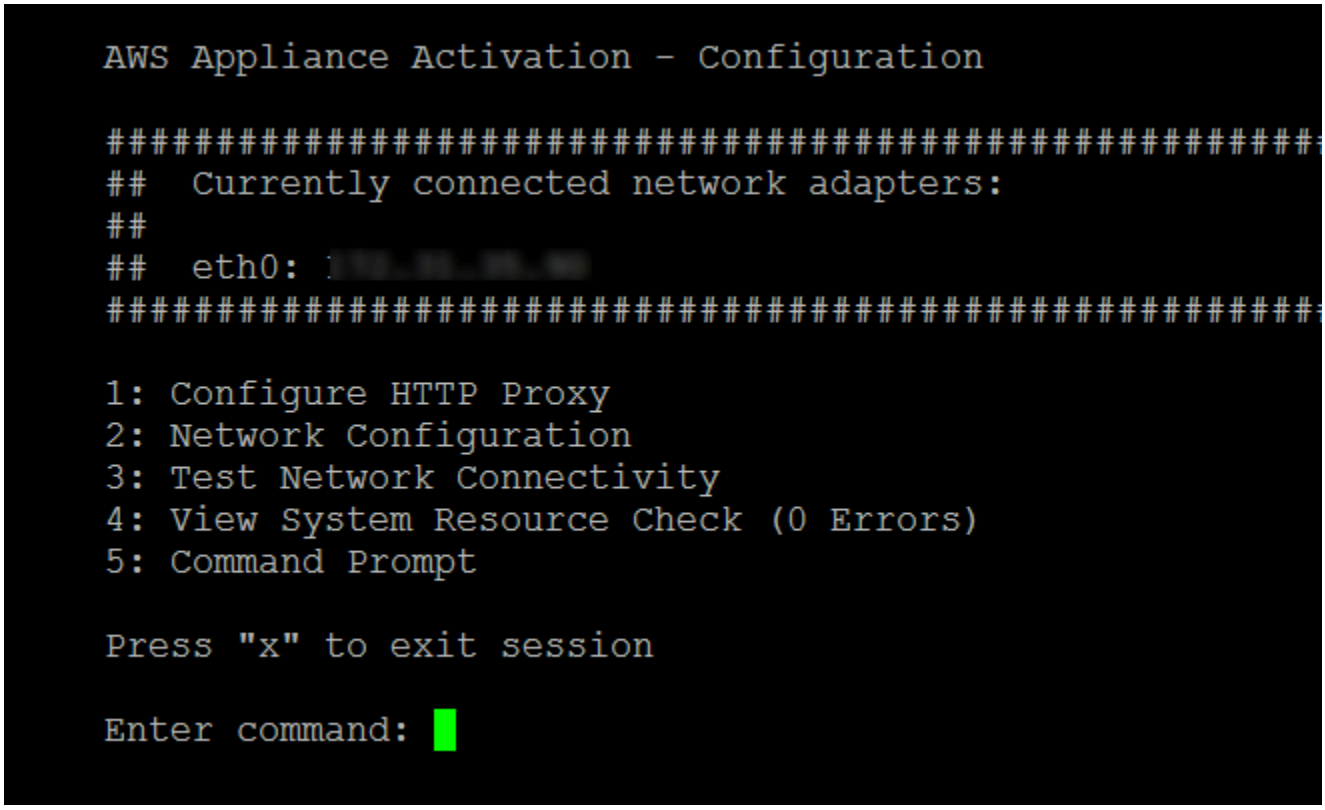
Per	eseguire questa operazione
	È necessario specificare il nome host e la porta per completare la configurazione.
Visualizzare l'attuale configurazione del proxy HTTP	Specificare (sì **2**. Se un proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured` . In caso contrario, vengono visualizzati il nome host e la porta del proxy HTTP.
Rimuovere la configurazione di un proxy HTTP	Specificare (sì **3**. Viene visualizzato il messaggio `HTTP Proxy Configuration Removed`

Configurazione delle impostazioni di rete gateway

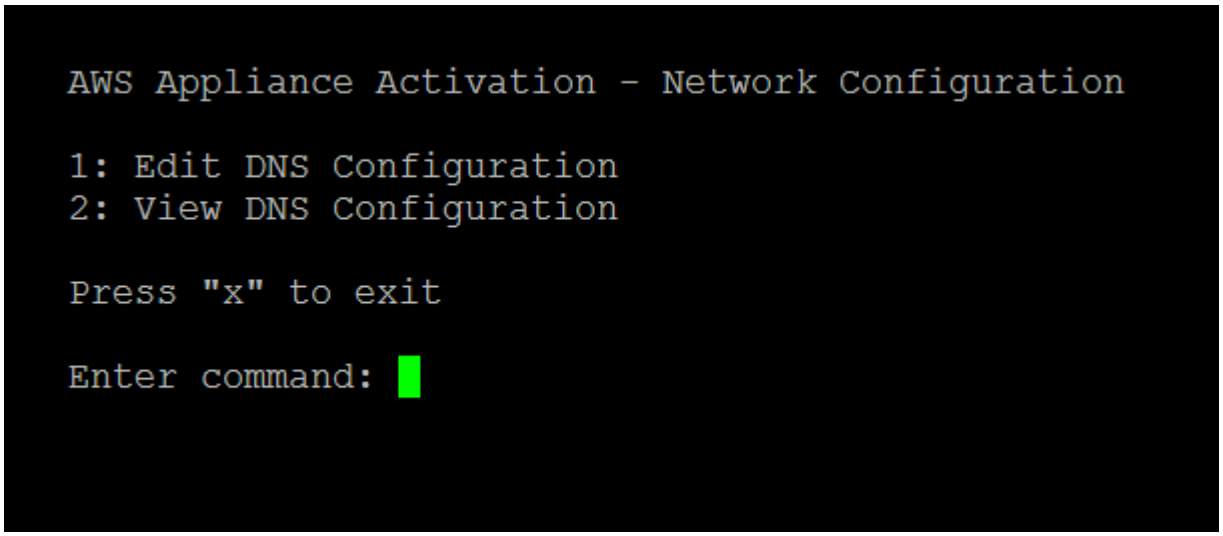
Puoi visualizzare e configurare le impostazioni del Domain Name Server (DNS) attraverso la console locale.

Per configurare il gateway affinché utilizzi indirizzi IP statici

1. Accedere alla console locale del gateway. Per istruzioni, consultare Accesso alla console locale del gateway Amazon EC2.
2. SulAWSAttivazione appliance - Configurazionemenu principale, entra**2**per iniziare a configurare il server DNS.



3. Scegliere una delle seguenti opzioni dal menu Network Configuration (Configurazione di rete).



Per	eseguire questa operazione
Modificare la configurazione DNS del gateway	Specificare (sì **1**.

Per	eseguire questa operazione
	Vengono visualizzate le schede disponibili dei server DNS primario e secondario. Viene richiesto di fornire il nuovo indirizzo IP.
Visualizzare la configurazione DNS del gateway	Specificare (sì **2**. Vengono visualizzate le schede disponibili dei server DNS primario e secondario.

Test della connettività di rete del gateway

Avvalendoti della console locale del gateway, puoi testare la connettività di rete. e conseguentemente risolvere eventuali problemi di rete del gateway.

Per testare la connettività del gateway

1. Accedere alla console locale del gateway. Per istruzioni, consultare Accesso alla console locale del gateway Amazon EC2.
2. DalAWSAttivazione appliance - Configurazionemenu principale, inserisci il numero corrispondente da selezionareConnettività 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 eRegione AWScome descritto nei seguenti passaggi.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se è stato selezionato il tipo di endpoint pubblico, immettere il numero corrispondente per selezionareRegione AWSche vuoi testare. Per supportatoRegioni AWSe elenco diAWSendpoint di servizio che è possibile utilizzare con Storage Gateway, vedereAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

Man mano che il test progredisce, ogni endpoint viene visualizzato[PASSATO]o[FAILED]indicante lo stato della connessione nel modo seguente:

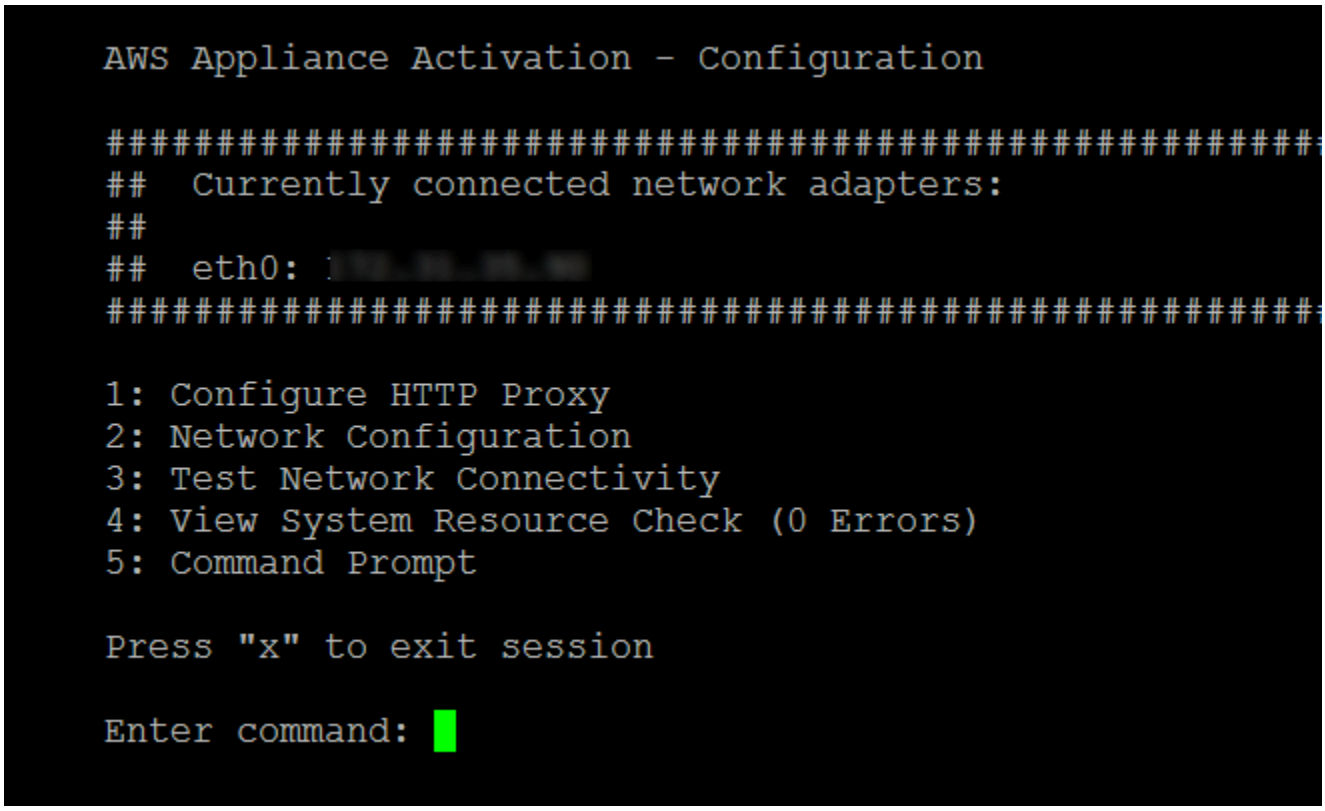
Messaggio	Descrizione
[PASSED]	Storage Gateway ha connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato delle risorse del sistema 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 istruzioni, consultare Accesso alla console locale del gateway Amazon EC2.
2. NellaConfigurazione Storage Gatewaymenu principale, entra**4**per visualizzare i risultati di un controllo delle risorse di sistema.



La console visualizza un messaggio [OK], [WARNING] ([ATTENZIONE]) o [FAIL] ([ESITO NEGATIVO]) per ogni risorsa, come descritto nella tabella seguente.

Messaggio	Descrizione
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti raccomand ati, ma il gateway continuerà 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 correttam ente. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.

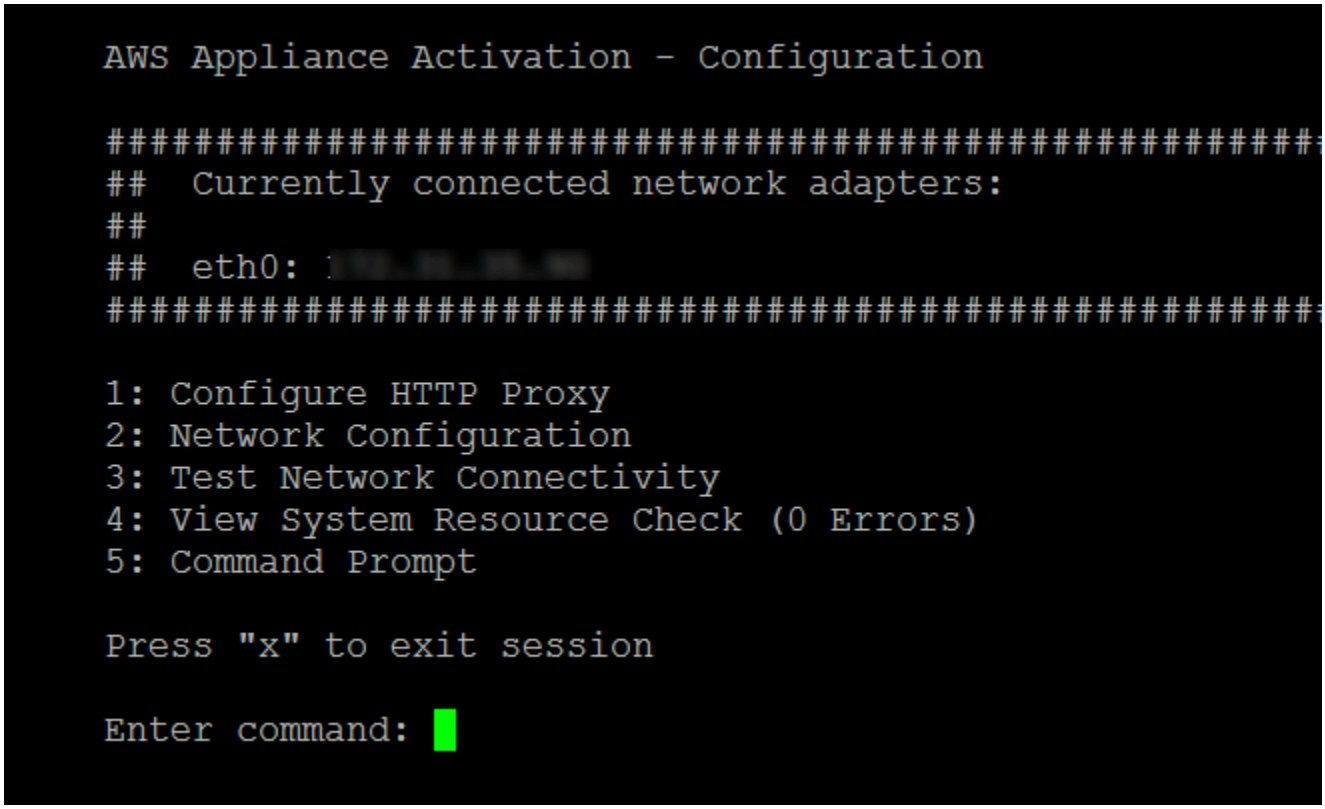
La console visualizza inoltre il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

Esecuzione di comandi Storage Gateway sulla console locale

La console di AWS Storage Gateway offre un ambiente sicuro per la configurazione e la diagnostica dei problemi del gateway. Utilizzando i comandi della console, è possibile eseguire operazioni di manutenzione come ad esempio il salvataggio delle tabelle di routing o la connessione al Support Amazon Web Services.

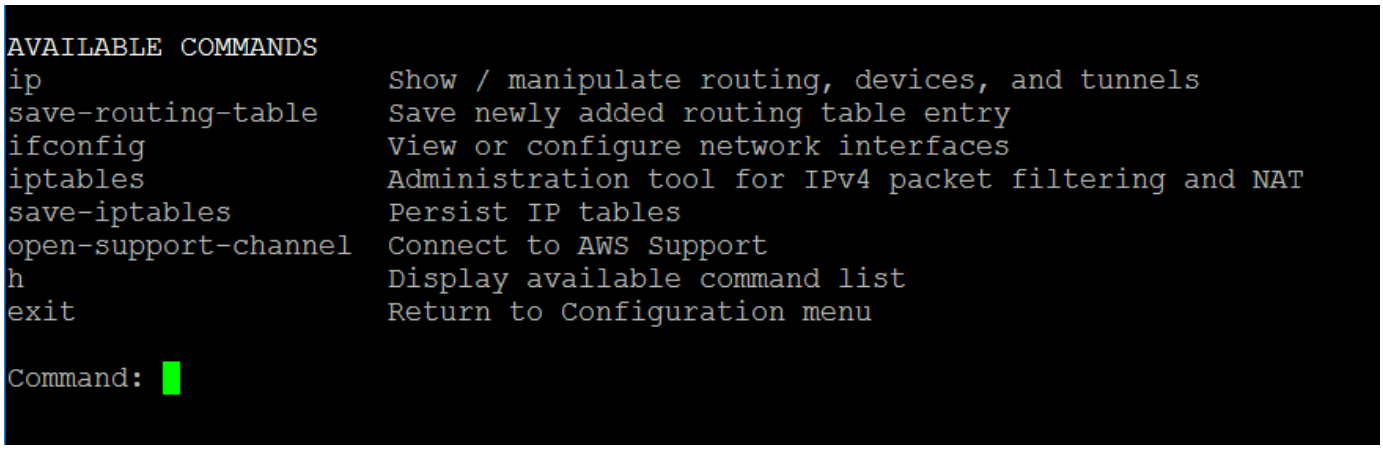
Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway. Per istruzioni, consultare Accesso alla console locale del gateway Amazon EC2.
2. NellaAWSConfigurazione per l'attivazionemenu principale, entra**5**perConsole del gateway.



3. Digitare **h** al prompt dei comandi, quindi premere il tasto Enter (Invio).

   La console mostra il menu AVAILABLE COMMANDS (COMANDI DISPONIBILI) con i comandi disponibili. Dopo il menu, viene visualizzato un prompt Gateway Console (Console del gateway), come mostrato nello screenshot seguente.



4. Al prompt dei comandi, inserire il comando che desideri utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitare il nome del comando nel prompt di comando.

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 sono disponibili informazioni su come accedere alla console locale della macchina virtuale tramite KVM (Linux Kernel-based Virtual Machine), VMware ESXi e Microsoft Hyper-V Manager.

Argomenti

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. Utilizzare il comando seguente per elencare le macchine virtuali attualmente disponibili in KVM.

   ```
   # virsh list
   ```

   È possibile scegliere le macchine virtuali disponibili per `Id`.

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

   ```
   # virsh console VM_Id
   ```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

3. Per ottenere le credenziali predefinite per accedere alla console locale, consulta Accesso alla console locale del gateway del file.
4. Dopo aver effettuato l'accesso, è possibile attivare e configurare il gateway.

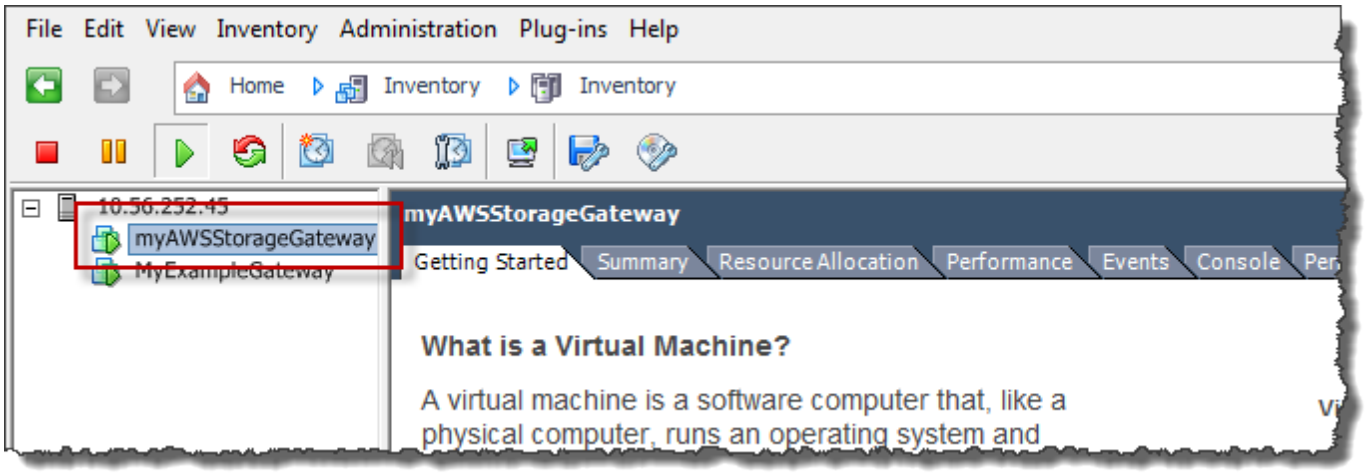
```
AWS Appliance Activation - Configuration

##################################################################
##  Currently connected network adapters:
##
##  eth0: 10.0.3.32
##################################################################

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

Accesso alla console locale del gateway con VMware ESXi

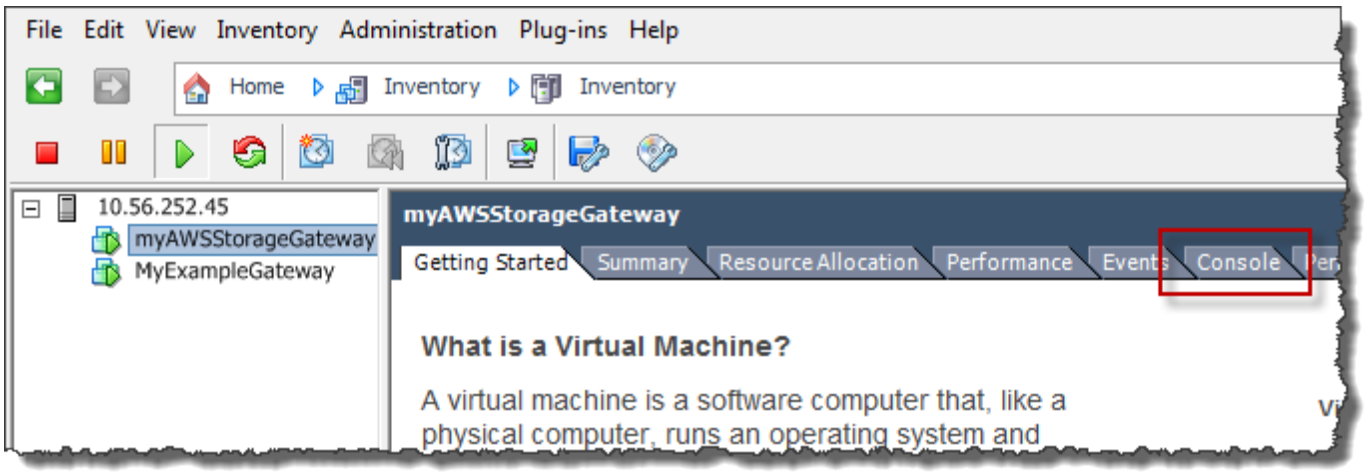
Per accedere alla console locale del gateway con VMware ESXi

1. Nel client VMware vSphere, seleziona la VM del gateway.
2. Verifica che il gateway sia attivo.

> **Note**
>
> Se la VM del gateway è attiva, viene visualizzata un'icona con una freccia verde con l'icona della VM, come illustrato nello screenshot seguente. Se la macchina virtuale del gateway non è attiva, è possibile attivarla scegliendo l'icona verde Power On (Accendi) nel menu Toolbar (Barra degli strumenti).



3. Scegli la scheda Console.



Dopo alcuni istanti, la macchina virtuale è pronta per l'accesso.

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

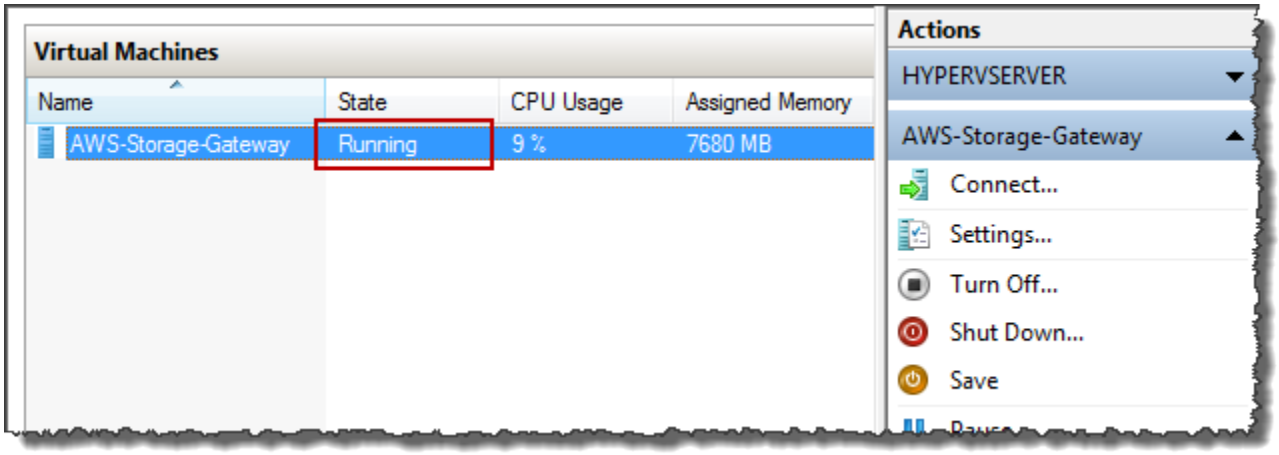
4. Per accedere tramite le credenziali predefinite, continua con la procedura Accesso alla console locale del gateway del file.

Accesso alla console locale del gateway con Microsoft Hyper-V

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

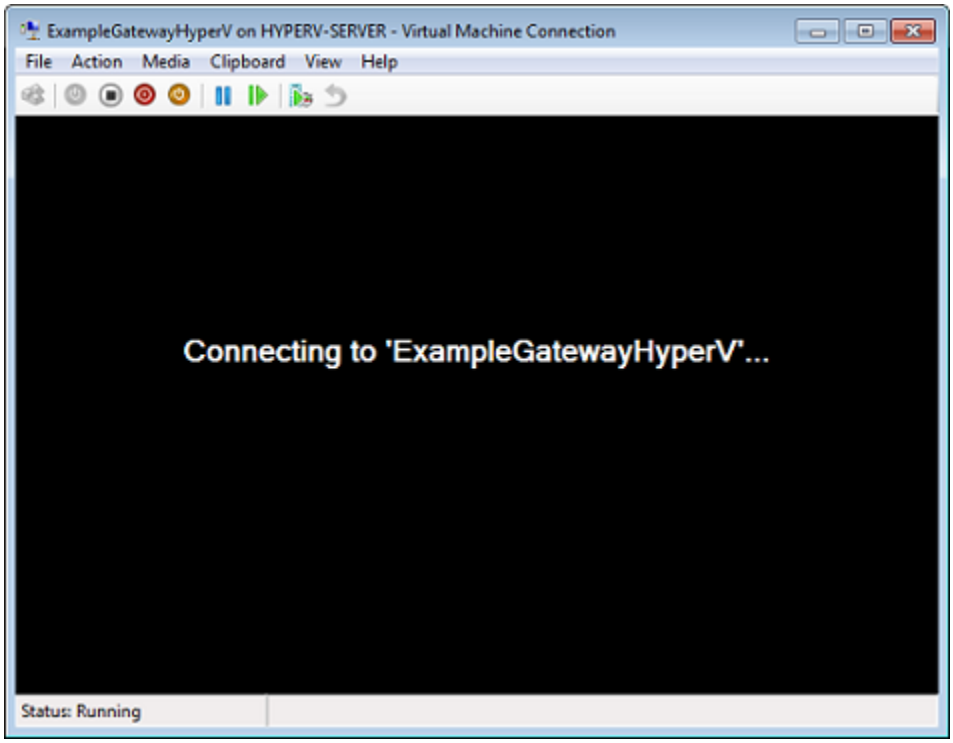
1. Nell'elenco Virtual Machines (Macchine virtuali) di Microsoft Hyper-V Manager, selezionare la macchina virtuale del gateway.
2. Verifica che il gateway sia attivo.

> **Note**
>
> Se la macchina virtuale del gateway è attivata, viene visualizzata l'indicazione `Running` nella colonna State (Stato) per la macchina virtuale, come illustrato nello screenshot seguente. Se la macchina virtuale del gateway non è attivata, è possibile attivarla scegliendo Start (Avvia) nel riquadro Actions (Operazioni).



3. Nel riquadro Actions (Operazioni) scegliere Connect (Connetti).

   Verrà visualizzata la finestra Virtual Machine Connection (Connessione macchina virtuale). Se viene visualizzata una finestra di autenticazione, digitare il nome utente e la password forniti dall'amministratore dell'hypervisor.



Dopo alcuni istanti, la macchina virtuale è pronta per l'accesso.

4. Per accedere tramite le credenziali predefinite, continua con la procedura Accesso alla console locale del gateway del file.

Configurazione delle schede di rete per il gateway

In questa sezione è possibile trovare informazioni su come configurare più schede di rete per il gateway.

Argomenti

- Configurazione del gateway per più NIC in un host VMware ESXi
- Configurazione del gateway per più NIC nell'host Microsoft Hyper-V

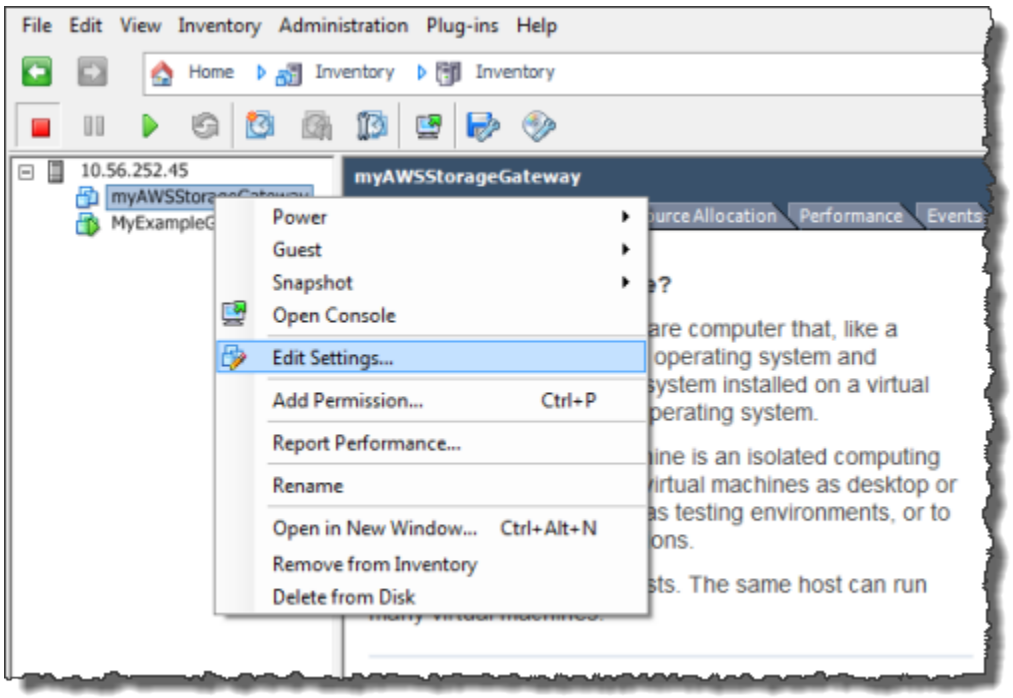
Configurazione del gateway per più NIC in un host VMware ESXi

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. La procedura seguente mostra come aggiungere una scheda per VMware ESXi.

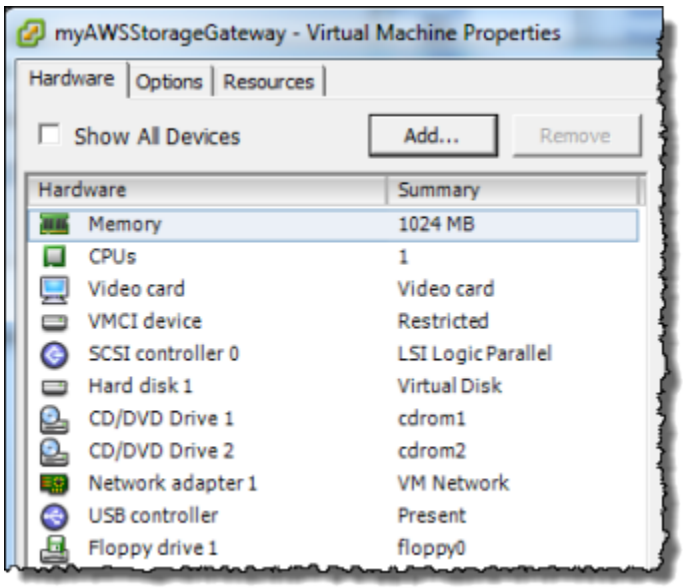
Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host VMware ESXi

1. Arresta il gateway.
2. Nel client VMware vSphere, seleziona la VM del 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).

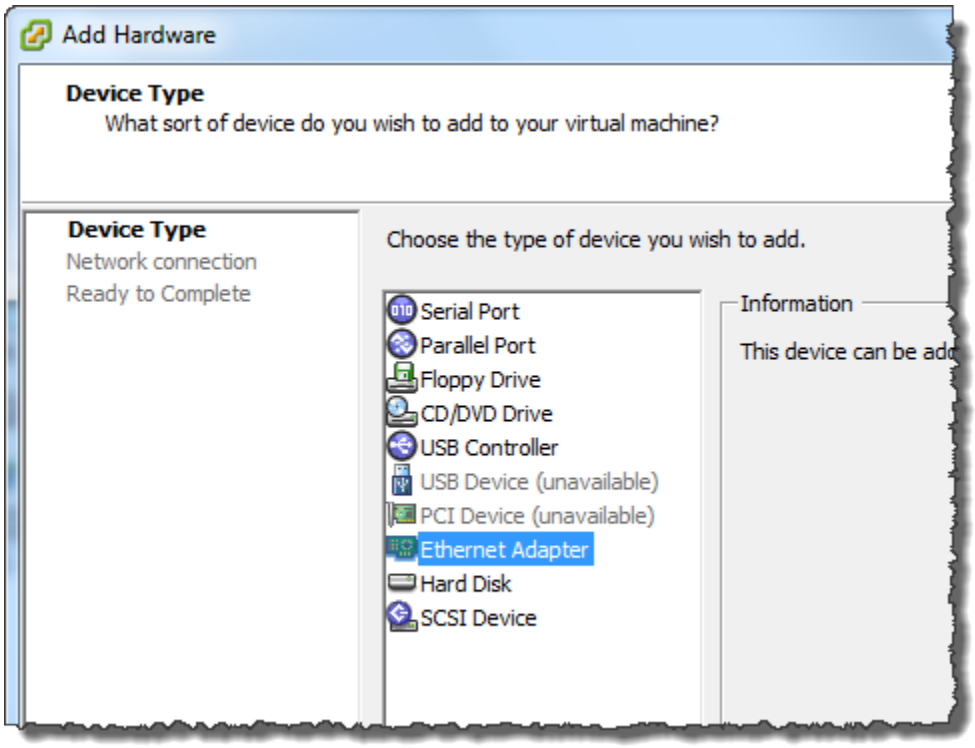


4. Nella scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), scegli Add (Aggiungi) per aggiungere un dispositivo.



5. Segui la procedura guidata Add Hardware (Aggiungi hardware) per aggiungere una scheda di rete.

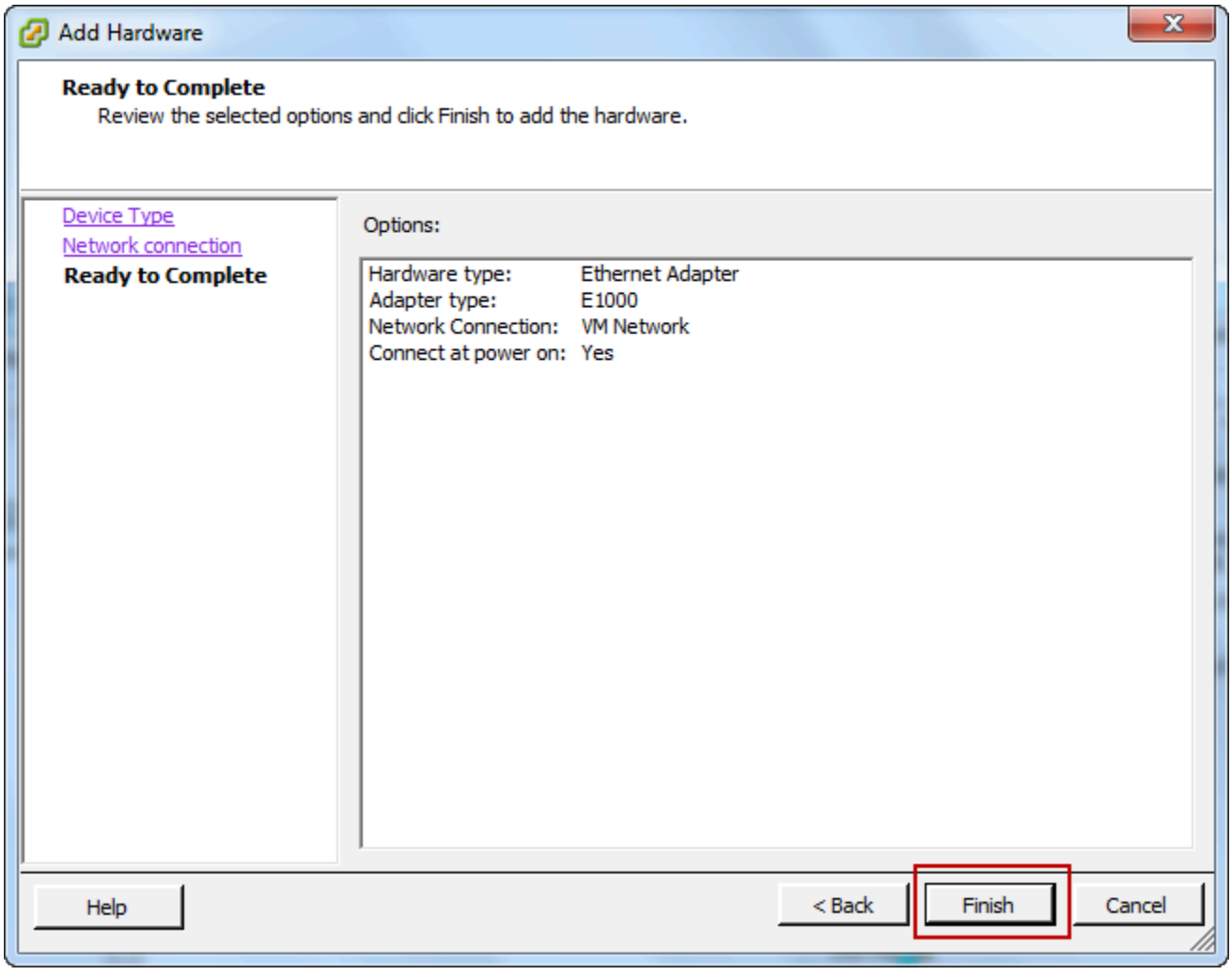
   a. Nel riquadro Device Type (Tipo di dispositivo), scegli Ethernet Adapter (Scheda Ethernet) per aggiungere una scheda, quindi scegli Next (Avanti).



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).

   Con Storage Gateway, è consigliabile utilizzare la scheda di rete E1000. Per ulteriori informazioni sui tipi di schede che potrebbero essere visualizzati nell'elenco delle schede, consulta la sezione relativa ai tipi di schede di rete nella documentazione di ESXi e vCenter Server.

c. Nel riquadro Ready to Complete (Pronto al completamento), rivedi le informazioni, quindi scegli Finish (Fine).

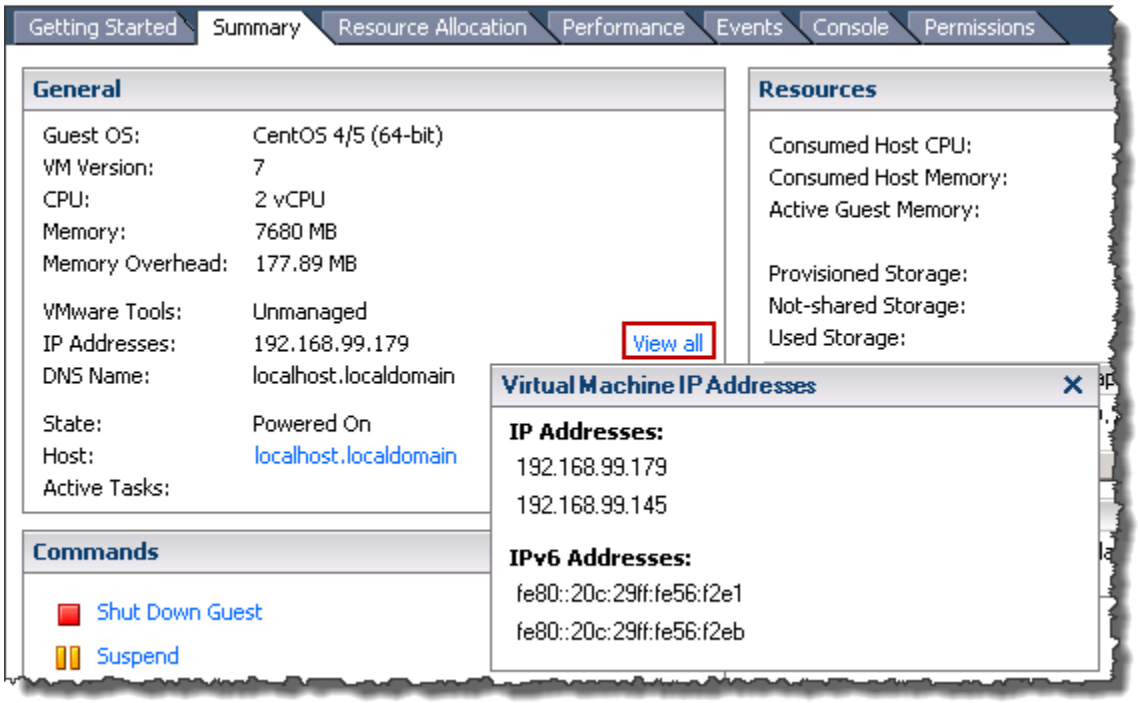


6. Scegli la scheda Summary (Riepilogo) della VM, quindi scegli View All (Visualizza tutto) accanto alla casella IP Address (Indirizzo IP). Nella finestra Virtual Machine IP Addresses (Indirizzi IP

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.

La seguente immagine è solo a scopo illustrativo. In pratica, uno degli indirizzi IP sarà l'indirizzo attraverso il quale il gateway comunica con AWS e l'altro sarà un indirizzo in un'altra sottorete.



7. Nella console Storage Gateway, attiva il gateway.
8. NellaNavigazionepannello della console Storage Gateway, scegliereGatewaye scegliere il gateway a cui aggiungere la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

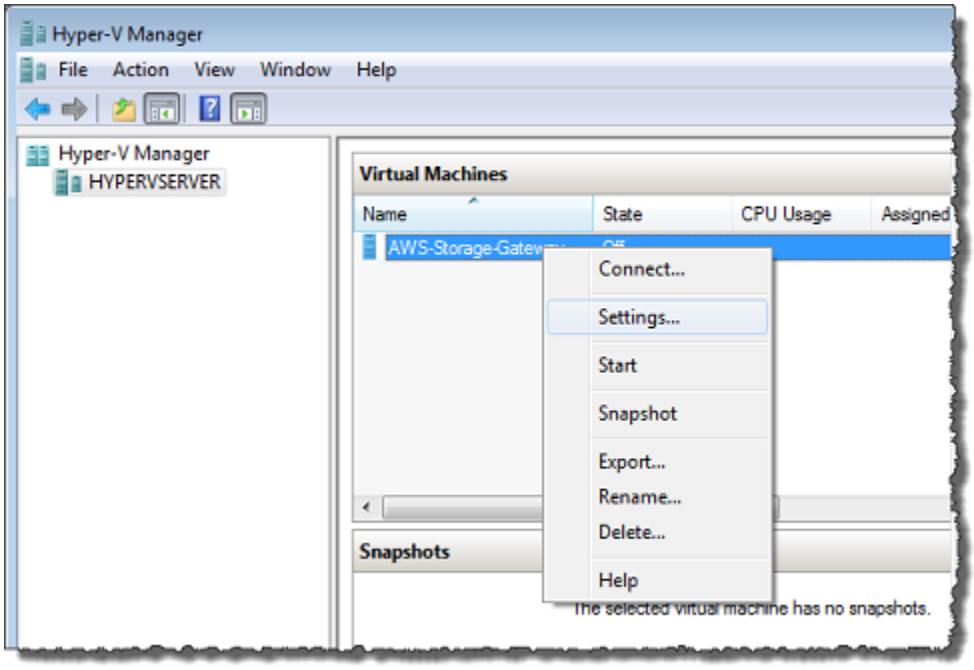
Per informazioni sulle attività locali della console comuni a VMware e agli Hyper-V e KVM, consulta [Esecuzione di attività nella console locale della VM (gateway del file)]

Configurazione del gateway per più NIC nell'host Microsoft Hyper-V

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.

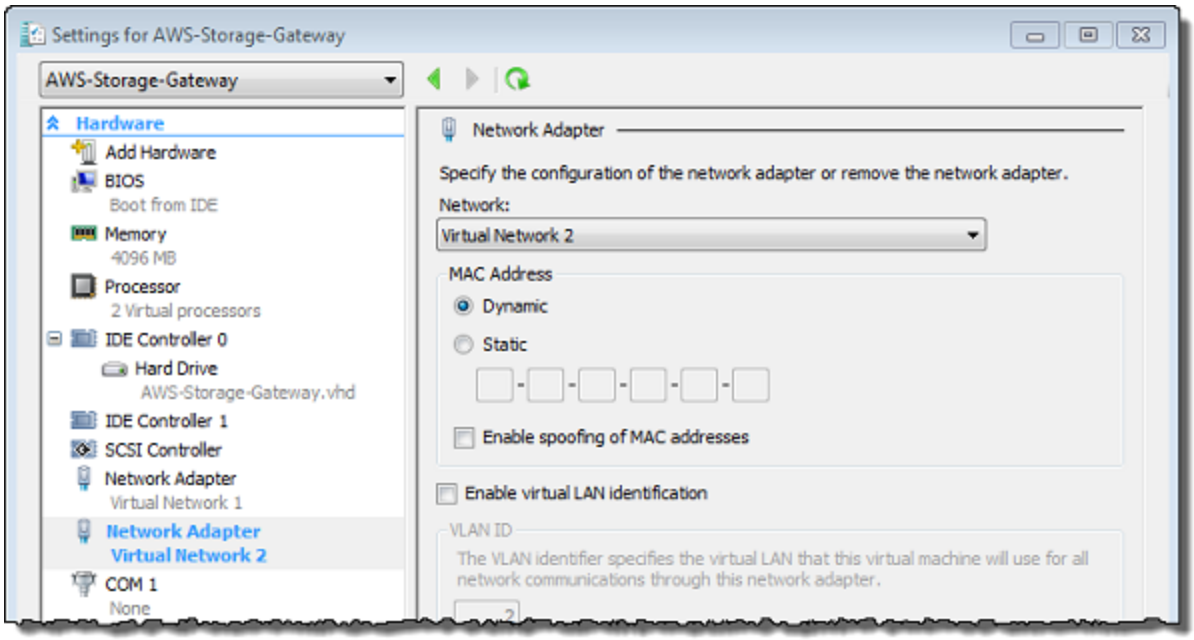
Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host Microsoft Hyper-V

1. Nella console Storage Gateway disattivare il gateway.
2. In Microsoft Hyper-V Manager selezionare la macchina virtuale del gateway.
3. Se la macchina virtuale non è ancora disattivata, aprire il menu contestuale (clic con il pulsante destro del mouse) per il gateway e scegliere Turn Off (Disattiva).
4. Nel client aprire il menu contestuale per la macchina virtuale del gateway e scegliere Settings (Impostazioni).



5. Nella finestra di dialogo Settings (Impostazioni) per la macchina virtuale, per Hardware scegliere Add Hardware (Aggiungi hardware).
6. Nel riquadro Add Hardware (Aggiungi hardware) scegliere Network Adapter (Scheda di rete) e quindi Add (Aggiungi) per aggiungere un dispositivo.
7. Configurare la scheda di rete e quindi scegliere Apply (Applica) per applicare le impostazioni.

Nell'esempio seguente è selezionata l'opzione Virtual Network 2 (Rete virtuale 2) per la nuova scheda.



8. Nella finestra di dialogo Settings (Impostazioni), per Hardware verificare che la seconda scheda sia stata aggiunta e quindi scegliere OK.
9. Nella console Storage Gateway, attiva il gateway.
10. Nel riquadro Navigation (Navigazione) scegliere Gateways (Gateway), quindi selezionare il gateway a cui è stata aggiunta la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

Per informazioni sulle attività locali della console comuni a VMware e agli Hyper-V e KVM, consulta Esecuzione di attività nella console locale della VM (gateway del file)

Eliminazione del gateway tramite la console AWS Storage 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.

L'eliminazione comporta l'esclusione del gateway dalla console di gestione AWS Storage Gateway e la chiusura della sua connessione iSCSI all'iniziatore. 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, consultaAWS Storage GatewayDocumentazione di riferimento API.

Argomenti

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 KVM (Linux Kernel-based Virtual Machine) per connettersi all'host e rimuovere la VM. Non è possibile riutilizzare la VM di un gateway eliminato per attivare un nuovo gateway.

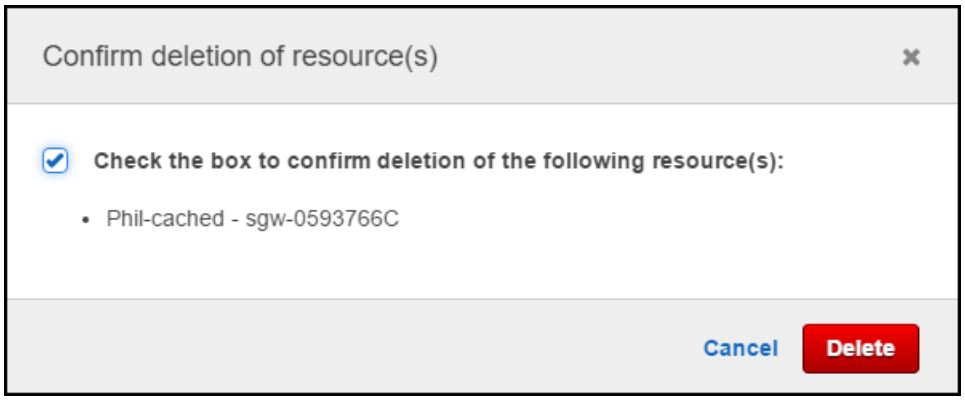
Come eliminare un gateway

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.

2. Nel riquadro di navigazione, scegliere Gateways (Gateway) e selezionare il gateway da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack).
4.

> **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.
> Inoltre, un gateway eliminato non può più essere recuperato.

Nella finestra di dialogo visualizzata, selezionare la casella di controllo appropriata per confermare l'eliminazione. Verificare che l'ID gateway riportato indichi il gateway da eliminare, quindi selezionare Delete (Elimina).



> **Important**
>
> A seguito dell'eliminazione del gateway, non si corre più in alcun costo di software; tuttavia, risorse quali nastri virtuali, snapshot Amazon EBS) di Amazon Elastic Block Store (Amazon EBS) e istanze Amazon EC2 restano disponibili e continuano a essere addebitate. Puoi rimuovere le istanze Amazon EC2 e gli snapshot Amazon EBS annullando l'abbonamento ad Amazon EC2. Se si desidera mantenere l'abbonamento ad Amazon EC2, gli snapshot Amazon EBS possono essere eliminati adoperando la console Amazon EC2.

Rimozione di risorse da un gateway distribuito in locale

Per rimuovere risorse da un gateway distribuito in locale, attieniti alle istruzioni riportate di seguito.

Rimozione di risorse da un gateway di volumi distribuito su una VM

Se il gateway da eliminare è distribuito su una macchina virtuale (VM), è consigliabile effettuare la pulizia delle risorse compiendo le seguenti azioni:

- Eliminare il gateway.

Rimozione di risorse da un gateway distribuito su un'istanza Amazon EC2

Se si desidera eliminare un gateway distribuito su un'istanza Amazon EC2, consigliamo di rimuovere l'AWSrisorse che sono state utilizzate con il gateway, così facendo aiuta a evitare costi di utilizzo indesiderati.

Rimozione di risorse da volumi nella cache distribuiti su Amazon EC2

Per eliminare un gateway con volumi nella cache distribuito su EC2 e rimuoverne le risorse:

1. Nella console Storage Gateway, eliminare il gateway come illustrato inEliminazione del gateway tramite la console Storage Gateway.
2. Nella console Amazon EC2, sospendere l'istanza EC2, se si intende riutilizzarla. In alternativa, terminare l'istanza. In vista dell'eliminazione di volumi, annotare, prima di terminare l'istanza, i dispositivi a blocchi collegati alla stessa e gli identificatori dei dispositivi, dati che risulteranno necessari per individuare i volumi da eliminare.
3. Nella console Amazon EC2, rimuovere tutti i volumi Amazon EBS collegati all'istanza, se non si intende utilizzarli nuovamente. Per ulteriori informazioni, consultaPulizia di un'istanza e di un volumenellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

Sostituzione del file gateway esistente con una nuova istanza

È possibile sostituire un File Gateway esistente con una nuova istanza man mano che le esigenze di dati e prestazioni aumentano o se si riceve unAWSNotifica per migrare il gateway. Potrebbe essere necessario farlo se si desidera spostare il gateway su una piattaforma host migliore o su istanze Amazon EC2 più recenti o aggiornare l'hardware del server sottostante.

Esistono due metodi per sostituire un File Gateway esistente. La tabella seguente descrive i vantaggi e gli svantaggi di ciascun metodo. Utilizzando queste informazioni, selezionare il metodo più adatto all'ambiente gateway, quindi fare riferimento alla procedura descritta nella sezione corrispondente di seguito.

	Metodo 1: Migrazione del disco cache e dell'ID gateway all'istanza sostituti	Metodo 2: Istanza sostituti va con disco cache vuoto e nuovo ID gateway
Memorizzare i dati disco	I dati sul disco cache vengono conservati. Questo metodo è utile se il gateway dispone di un disco cache di grandi dimensioni o se le applicazi oni sono sensibili al ritardo causato dalle operazioni di lettura fuori cache.	I dati nella cache vengono scaricati dalAWSnuvola. Questo metodo è ottimale per carichi di lavoro pesanti in scrittura, se le applicazioni sono in grado di tollerare il ritardo causato dalle letture fuori cache.
Tempo di inattività	Il gateway sarà offline per 1-2 ore durante il processo di migrazione.	Nessun tempo di inattivit à. Il gateway esistente può essere utilizzato contempor aneamente al gateway sostitutivo fino a quando non si sceglie di eliminarlo. Gli scrittori multipli non sono supportati mentre entrambi i gateway sono in uso.

	Metodo 1: Migrazione del disco cache e dell'ID gateway all'istanza sostituti	Metodo 2: Istanza sostituti va con disco cache vuoto e nuovo ID gateway
ID gateway	Il nuovo gateway eredita l'ID gateway dal gateway che sostituisce.	Il gateway e il gateway sostitutivo esistenti dispongon o di ID gateway separati e univoci.

> **Note**
>
> I dati possono essere spostati solo tra gateway dello stesso tipo.

Metodo 1: Migrazione del disco cache e dell'ID gateway all'istanza sostituti

Per migrare il disco cache e l'ID gateway di File Gateway in un'istanza sostitutiva:

1. Interrompere tutte le applicazioni che stanno scrivendo sul gateway file esistente.
2. Verificare che l'`CachePercentDirty`Parametri di nellaMonitoraggioscheda per il gateway di file esistente è`0`.
3. Spegnere il gateway di file esistente spegnendo la macchina virtuale host (VM) utilizzando i controlli dell'hypervisor.

   Per ulteriori informazioni sulla chiusura di un'istanza Amazon EC2, consultaArrestare e avviare un'istanzanellaGuida per l'utente di Amazon EC2.

   Per ulteriori informazioni sulla chiusura di una VM KVM, VMware o Hyper-V, consulta la documentazione dell'hypervisor.
4. Scollega tutti i dischi, inclusi il disco principale, i dischi cache e carica i dischi buffer dalla vecchia VM gateway.

> **Note**
>
> Prendi nota dell'ID del volume del disco principale e dell'ID gateway associato a quel disco root. Sarà necessario scollegare il disco dal nuovo hypervisor del gateway di storage in un passaggio successivo.

Se utilizzi un'istanza Amazon EC2 come VM per il gateway di file, consultaDistaccare un volume Amazon EBS da un'istanza WindowsoDistaccare un volume Amazon EBS da un'istanza LinuxnellaGuida per l'utente di Amazon EC2.

Per ulteriori informazioni su come staccare dischi da una VM KVM, VMware o Hyper-V, consultare la documentazione dell'hypervisor.

5. Creazione di un nuovoAWSIstanza VM hypervisor Storage Gateway, ma non attivarla come gateway. In una fase successiva, questa nuova VM assumerà l'identità del vecchio gateway.

   Per ulteriori informazioni sulla creazione di una nuova VM hypervisor Storage Gateway, consultareSelezione di una piattaforma host e download della VM.

   > **Note**
   >
   > Non aggiungere dischi cache per la nuova VM. Questa VM utilizzerà gli stessi dischi cache utilizzati dalla vecchia VM.

6. Configurare la nuova VM Storage Gateway per utilizzare le stesse impostazioni di rete della vecchia VM.

   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.

   Se è necessario configurare manualmente un indirizzo IP statico per la VM del gateway, consultareConfigurazione di rete del gateway.

   Se la VM del gateway deve utilizzare un proxy Socket Secure versione 5 (SOCKS5) per connettersi a Internet, consultareInstradamento del gateway in locale tramite un proxy.

7. Avviare la nuova VM Storage Gateway.

8. Collegare i dischi staccati dalla vecchia VM gateway alla nuova VM gateway. Non scollegare il disco radice esistente dalla nuova VM gateway.

   > **Note**
   >
   > Per eseguire correttamente la migrazione, tutti i dischi devono rimanere invariati. La modifica delle dimensioni del disco o di altri valori provoca incongruenze nei metadati che impediscono la corretta migrazione.

9. Avviare il processo di migrazione del gateway collegandosi alla nuova VM con un URL che utilizza il seguente formato:

   `http://`*`your-VM-IP-address`*`/migrate?gatewayId=`*`your-gateway-ID`

   È possibile utilizzare lo stesso indirizzo IP per la nuova VM gateway utilizzata per la vecchia VM gateway. L'URL dovrebbe essere simile all'esempio seguente:

   `http://`*`198.51.100.123`*`/migrate?gatewayId=`*`sgw-12345678`

   Utilizzare questo URL da un browser o dalla riga di comando usando cURL.

   Quando la migrazione del gateway viene avviata correttamente, viene visualizzato il seguente messaggio:

   ```
   Successfully imported Storage Gateway information. Please refer to Storage Gateway
    documentation to perform the next steps to complete the migration.
   ```

10. Attendere che lo stato del gateway diventiCorrerenellaAWSConsole Storage Gateway. A seconda della larghezza di banda disponibile, può richiedere fino a 10 minuti.
11. Arrestare la nuova VM Storage Gateway.
12. Scollega il disco radice del vecchio gateway, di cui hai notato in precedenza l'ID del volume, dal nuovo gateway.
13. Avviare la nuova VM Storage Gateway.
14. Se il gateway è stato aggiunto a un dominio Active Directory, aggiungere nuovamente il dominio. Per istruzioni, consultaConfigurazione dell'accesso a Microsoft Active Directory.

> **Note**
>
> È necessario completare questo passaggio anche se lo stato del gateway di file appare comeJoined (Collegato).

15. Verificare che le condivisioni siano disponibili all'indirizzo IP del nuovo gateway VM, quindi eliminare la vecchia VM gateway.

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

Per ulteriori informazioni sull'eliminazione di un'istanza Amazon EC2, consultaInterruzione di un'istanzanellaGuida per l'utente di Amazon EC2. Per ulteriori informazioni sull'eliminazione di una VM KVM, VMware o Hyper-V, consulta la documentazione dell'hypervisor.

Metodo 2: Istanza sostitutiva con disco cache vuoto e nuovo ID gateway

Per impostare un'istanza di File Gateway sostitutiva con disco cache vuoto e nuovo ID gateway:

1. Interrompere tutte le applicazioni che stanno scrivendo sul gateway file esistente. Verificare che l'`CachePercentDirty`Parametri di nellaMonitoraggioLa scheda è`0`prima di configurare le condivisioni di file sul nuovo gateway.
2. Utilizzo dell'AWS Command Line Interface(AWS CLI) per raccogliere e salvare le informazioni di configurazione relative al gateway di file e alle condivisioni di file esistenti effettuando le seguenti operazioni:

   a. Salva le informazioni di configurazione del gateway per il gateway di file.

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

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

b. Salvare le impostazioni SMB (Server Message Block) del gateway file.

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

Questo comando emette un blocco JSON che contiene metadati relativi alla condivisione di file SMB, ad esempio il nome di dominio, lo stato di Microsoft Active Directory, l'impostazione della password guest e il tipo di strategia di sicurezza.

c. Salva le informazioni sulla condivisione di file per ogni condivisione di file SMB e Network File System (NFS) del gateway di file:

- Utilizzare il seguente comando per le condivisioni di file SMB.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

Questo comando emette un blocco JSON contenente metadati relativi alla condivisione di file NFS, ad esempio nome, classe di storage, stato, ruolo IAM (Amazon Resource Name), un elenco di client a cui è consentito accedere al gateway di file e il percorso utilizzato dal client SMB per identificare il mount point.

- Utilizzare il seguente comando per le condivisioni file NFS.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Questo comando emette un blocco JSON contenente metadati relativi alla condivisione di file NFS, ad esempio nome, classe di archiviazione, stato, ruolo IAM ARN, un elenco di client a cui è consentito accedere al gateway di file e il percorso utilizzato dal client NFS per identificare il punto di montaggio.

3. Arrestare il gateway di file esistente effettuando le seguenti operazioni:

a. Interrompere tutte le applicazioni che stanno scrivendo sul gateway file esistente. Verificare che l'`CachePercentDirty`Parametri di nellaMonitoraggioLa scheda è`0`prima di configurare le condivisioni di file sul nuovo gateway.

b. Arrestare il gateway di file esistente spegnendo la macchina virtuale (VM) che ospita il gateway.

4. Creare un nuovo File Gateway.
5. Montare le condivisioni di file configurate sul vecchio gateway.
6. Verificare che il nuovo gateway funzioni correttamente, quindi eliminare il vecchio gateway dalla console Storage Gateway.

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

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

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

Prestazioni

In questa sezione è possibile trovare informazioni sulle prestazioni di Storage Gateway.

Argomenti

Guida alle prestazioni dei gateway di file

In questa sezione è possibile trovare linee guida di configurazione per il provisioning dell'hardware per la macchina virtuale del gateway di file. Le dimensioni delle istanze e i tipi elencati nella tabella sono esempi e vengono forniti a scopo di 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.

Nelle tabelle seguenti,hit della cacheLe operazioni di lettura vengono lette dalle condivisioni di file servite dalla cache. Manca cacheLe operazioni di lettura vengono lette dalle condivisioni di file servite da Amazon S3.

> **Note**
>
> Non è consigliabile utilizzare lo storage temporaneo. Per informazioni sull'utilizzo dello storage temporaneo, consulta Utilizzo di storage effimero con gateway EC2.

Di seguito sono riportati esempi di configurazioni del gateway file.

Prestazioni di S3 File Gateway sui client Linux

Configurazioni di esempio	Protocollo	Throughput di scrittura (dimensioni file 1 GB)	Throughput di lettura riscontro della cache	Throughput di lettura mancante della cache
Disco root: 80 GB io1, 4.000 IOPS Disco cache: 512 GiB cache, io1, 1.500 provisioned IOPS Prestazioni di rete minime: 10 Gb/s CPU: 16 vCPU | RAM: 32 GB Protocollo NFS consigliato per Linux	NFSv3 - 1 filo	110 MiB/sec (0,92 Gbps)	590 MiB/s (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 thread	160 MiB/s (1,3 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv4 - 1 filo	130 MiB/sec (1,1 Gbps)	590 MiB/s (4,9 Gbps)	295 MiB/s (2,5 Gbps)
	NFSv4 - 8 thread	160 MiB/s (1,3 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	SMBV3 - 1 filo	115 MiB/s (1,0 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 thread	190 MiB/sec (1,6 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
Storage Gateway Hardware Appliance Prestazioni di rete minime: 10 Gb/s	NFSv3 - 1 filo	265 MiB/s (2,2 Gbps)	590 MiB/s (4,9 Gbps)	310 MiB/sec (2,6 Gbps)
	NFSv3 - 8 thread	385 MiB/sec (3,1 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv4 - 1 filo	310 MiB/sec (2,6 Gbps)	590 MiB/s (4,9 Gbps)	295 MiB/s (2,5 Gbps)
	NFSv4 - 8 thread	385 MiB/sec (3,1 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)

Configurazioni di esempio	Protocollo	Throughput di scrittura (dimensioni file 1 GB)	Throughput di lettura riscontro della cache	Throughput di lettura mancante della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: 4 dischi cache NVME da 2 TB Prestazioni di rete minime: 10 Gb/s CPU: 32 vCPU | RAM: 244 GB Protocollo NFS consigliato per Linux	SMBV3 - 1 filo	275 MiB/sec (2,4 Gbps)	325 MiB/sec (2,7 Gbps)	255 MiB/sec (2,1 Gbps)
	SMBV3 - 8 thread	455 MiB/s (3,8 Gbps)	590 MiB/s (4,9 Gbps)	335 MiB/s (2,8 Gbps)
	NFSv3 - 1 filo	300 MiB/s (2,5 Gbps)	590 MiB/s (4,9 Gbps)	325 MiB/sec (2,7 Gbps)
	NFSv3 - 8 thread	585 MiB/s (4,9 Gbps)	590 MiB/s (4,9 Gbps)	580 MiB/s (4,8 Gbps)
	NFSv4 - 1 filo	355 MiB/s (3,0 Gbps)	590 MiB/s (4,9 Gbps)	340 MiB/s (2,9 Gbps)
	NFSv4 - 8 thread	575 MiB/s (4,8 Gbps)	590 MiB/s (4,9 Gbps)	575 MiB/s (4,8 Gbps)
	SMBV3 - 1 filo	230 MiB/s (1,9 Gbps)	325 MiB/sec (2,7 Gbps)	245 MiB/s (2,0 Gbps)
	SMBV3 - 8 thread	585 MiB/s (4,9 Gbps)	590 MiB/s (4,9 Gbps)	580 MiB/s (4,8 Gbps)

Prestazioni del gateway di file sui client Windows

Configurazioni di esempio	Protocollo	Throughput di scrittura (dimensioni file 1 GB)	Throughput di lettura riscontro della cache	Throughput di lettura mancante della cache
Disco root: 80 GB io1, 4.000 IOPS Disco cache: 512 GiB cache, io1, 1.500 provisioned IOPS Prestazioni di rete minime: 10 Gb/s CPU: 16 vCPU | RAM: 32 GB Protocollo SMB consigliato per Windows	SMBV3 - 1 filo	150 MiB/s (1,3 Gbps)	1,5 MiB/s (1,5 Gbps)	20 MiB/s (0,2 Gbps)
	SMBV3 - 8 thread	190 MiB/sec (1,6 Gbps)	335 MiB/s (2,8 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 filo	95 MiB/s (0,8 Gbps)	130 MiB/sec (1,1 Gbps)	20 MiB/s (0,2 Gbps)
	NFSv3 - 8 thread	190 MiB/sec (1,6 Gbps)	330 MiB/s (2,8 Gbps)	190 MiB/sec (1,6 Gbps)
Storage Gateway Hardware Appliance Prestazioni di rete minime: 10 Gb/s	SMBV3 - 1 filo	230 MiB/s (1,9 Gbps)	255 MiB/sec (2,1 Gbps)	20 MiB/s (0,2 Gbps)
	SMBV3 - 8 thread	835 MiB/s (7,0 Gbps)	475 MiB/s (4,0 Gbps)	195 MiB/sec (1,6 Gbps)
	NFSv3 - 1 filo	135 MiB/sec (1,1 Gbps)	185 MiB/sec (1,6 Gbps)	20 MiB/s (0,2 Gbps)
	NFSv3 - 8 thread	545 MiB/sec (4,6 Gbps)	470 MiB/s (4,0 Gbps)	190 MiB/sec (1,6 Gbps)

Configurazioni di esempio	Protocollo	Throughput di scrittura (dimensioni file 1 GB)	Throughput di lettura riscontro della cache	Throughput di lettura mancante della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: 4 dischi cache NVME da 2 TB Prestazioni di rete minime: 10 Gb/s CPU: 32 vCPU | RAM: 244 GB Protocollo SMB consigliato per Windows	SMBV3 - 1 filo	230 MiB/s (1,9 Gbps)	265 MiB/s (2,2 Gbps)	30 MiB/s (0,3 Gbps)
	SMBV3 - 8 thread	835 MiB/s (7,0 Gbps)	780 MiB/s (6,5 Gbps)	250 MiB/sec (2,1 Gbps)
	NFSv3 - 1 filo	135 MiB/sec (1,1. (Gbps)	220 MiB/s (1,8 Gbps)	30 MiB/s (0,3 Gbps)
	NFSv3 - 8 thread	545 MiB/sec (4,6 Gbps)	570 MiB/s (4,8 Gbps)	240 MiB/s (2,0 Gbps)

> **Note**
>
> Le prestazioni potrebbero variare in base alla configurazione della piattaforma host e alla larghezza di banda della rete.

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, ad esempio unità a stato solido (SSD) 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. Migliori prestazioni del disco in genere consentono un throughput migliore e un maggior numero di operazioni input/output al secondo (IOPS). Per informazioni sull'aggiunta di dischi, consultaAggiunta di storage della cache.

Per misurare il throughput, utilizzare il`ReadBytes`e`WriteBytes`le metriche con`Samples`Statistiche di 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**
>
> I parametri CloudWatch non sono disponibili per tutti i gateway. Per informazioni sui parametri del gateway, consulta Monitoraggio del gateway file.

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, confermare che non si sta sfruttando eccessivamente la CPU del server host.

Quando si aggiungono ulteriori CPU al server host del gateway, si aumenta la capacità di elaborazione del gateway. In questo modo, il gateway può gestire in parallelo l'archiviazione dei dati dall'applicazione allo storage locale e il caricamento di questi dati su Amazon S3. CPU aggiuntive garantiscono che il gateway riceva risorse CPU sufficienti quando l'host è condiviso con altre macchine virtuali. Fornire un numero sufficiente di risorse CPU ha l'effetto di migliorare il throughput generale.

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

- 24 CPU.

- 16 GiB di RAM riservata per 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 cache da 16 TiB a 32 TiB
  - 48 GiB di RAM riservata per gateway con 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 utilizzano un controller NVMe.
- Disco 2 collegato a un controller 1 paravirtuale per essere usato come buffer di caricamento gateway come segue:
  - SSD che utilizzano un controller NVMe.
- Disco 3 collegato a un controller 2 paravirtuale per essere usato come buffer di caricamento gateway come segue:
  - SSD che utilizzano un controller NVMe.
- Adattatore di rete 1 configurato sulla rete macchina virtuale 1:
  - Utilizzare la rete della macchina virtuale 1 e aggiungere VMXnet3 (10 Gbps) da utilizzare per l'acquisizione.
- Adattatore di rete 2 configurato sulla rete macchina virtuale 2:
  - Utilizzare la rete della macchina virtuale 2 e aggiungere VMXnet3 (10 Gbps) da utilizzare per la connessione ad AWS.

Supportare dischi virtuali gateway con dischi fisici separati

Quando viene effettuato il provisioning dei dischi gateway, è consigliabile non effettuare il provisioning di dischi locali per lo storage locale che utilizzano lo stesso disco fisico di storage. Ad esempio, per VMware ESXi, le risorse di storage fisiche sottostanti sono rappresentate come un data store. 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. Puoi utilizzare il pluginReadByteseWriteBytesmetriche del gateway per misurare il throughput 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 è in grado di utilizzare altre risorse CPU, l'aggiunta di più CPU può aiutarla a dimensionare il carico di I/O.

Utilizzo di VMware vSphere High Availability con Storage Gateway

Storage Gateway fornisce disponibilità elevata su VMware attraverso un set di controlli di stato a livello di applicazione integrato con VMware vSphere High Availability (VMware HA). 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 ambiente VMware locale o in un VMware Cloud on AWS verrà automaticamente ripristinato dalla maggior parte delle interruzioni di servizio. Generalmente il processo dura meno di 60 secondi senza perdita di dati.

Per utilizzare VMware HA con Storage Gateway, attieniti alla procedura indicata di seguito.

Argomenti

- Attivazione del gateway
- Test della configurazione VMware High Availability

Configurazione del cluster vSphere VMware HA

Innanzitutto crea un cluster VMware, se non è già stato fatto. Per informazioni su come creare un cluster VMware, consulta l'argomento relativo alla creazione di un cluster vSphere HA nella documentazione di VMware.

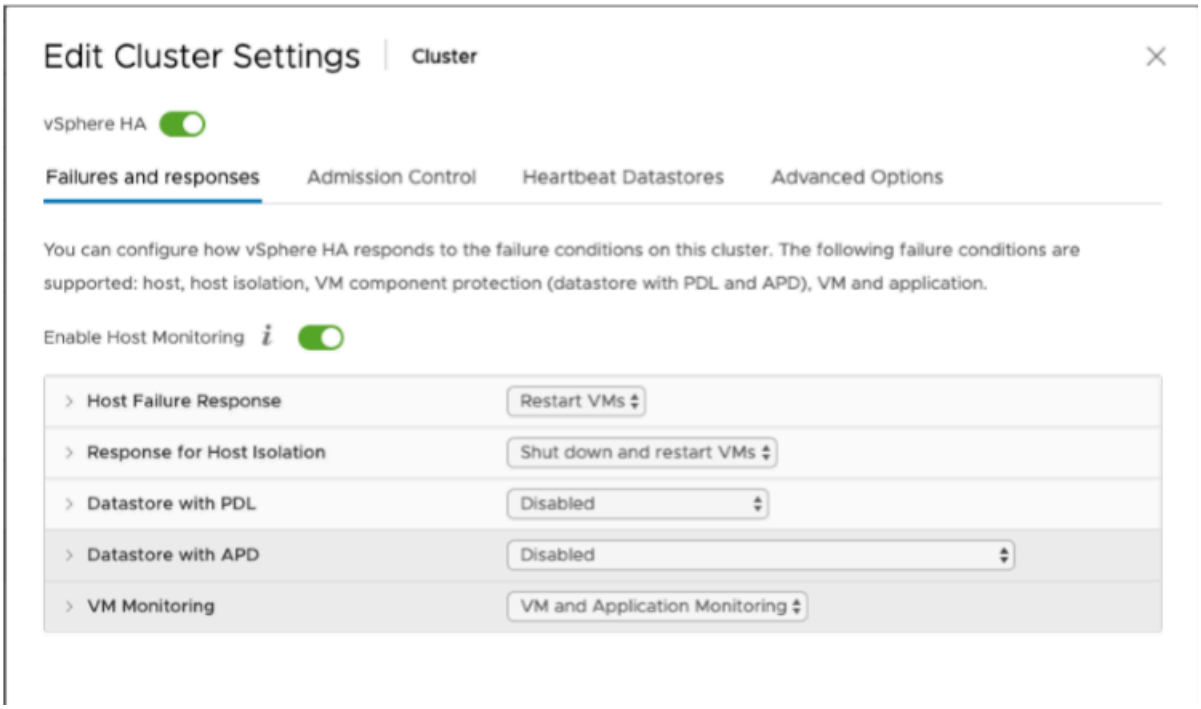
Successivamente, configura il cluster VMware per funzionare con Storage Gateway.

Per configurare il cluster VMware

1. Nella pagina Edit Cluster Settings (Modifica impostazioni cluster) in VMware vSphere verificare che il monitoraggio VM sia configurato per il monitoraggio delle macchine virtuali e delle applicazioni. A tale scopo, impostare le seguenti opzioni come indicato:

   - Risposta errore host: Riavvia VM
   - Risposta per l'isolamento host: Shut down and restart VMs
   - Datastore con PDL: Disabilitato
   - Datastore con APD: Disabilitato
   - Monitoraggio VM: Monitoraggio VM e applicazioni

   Per un esempio, vedere le immagini seguenti.



2. Ottimizzare la sensibilità del cluster regolando i seguenti valori:

   - Intervallo errore— Dopo questo intervallo, la macchina virtuale viene riavviata se non viene ricevuto un heartbeat VM.
   - Tempo di attività minimo— Il cluster attende molto tempo dopo che una macchina virtuale inizia a monitorare gli heartbeat degli strumenti VM.
   - Massimo reset per VM— Il cluster riavvia la macchina virtuale per un numero massimo di volte all'interno della finestra temporale massima di ripristino.
   - Massimo intervallo temporale di reimpostazioni massimo— 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 nel cluster sono in esecuzione altre macchine virtuali, puoi impostare questi valori in modo specifico per la 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) Aggiunta di opzioni di sostituzione per altre macchine virtuali nel cluster.

Download dell'immagine .ova per il tipo di gateway

Utilizza la procedura seguente per scaricare l'immagine .ova.

Per scaricare l'immagine .ova per il tipo di gateway

- Scarica l'immagine .ova per il tipo di gateway di una delle seguenti opzioni:
  - Gateway file —

Distribuzione del gateway

Nel cluster configurato distribuisci l'immagine .ova in uno degli host del cluster.

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.

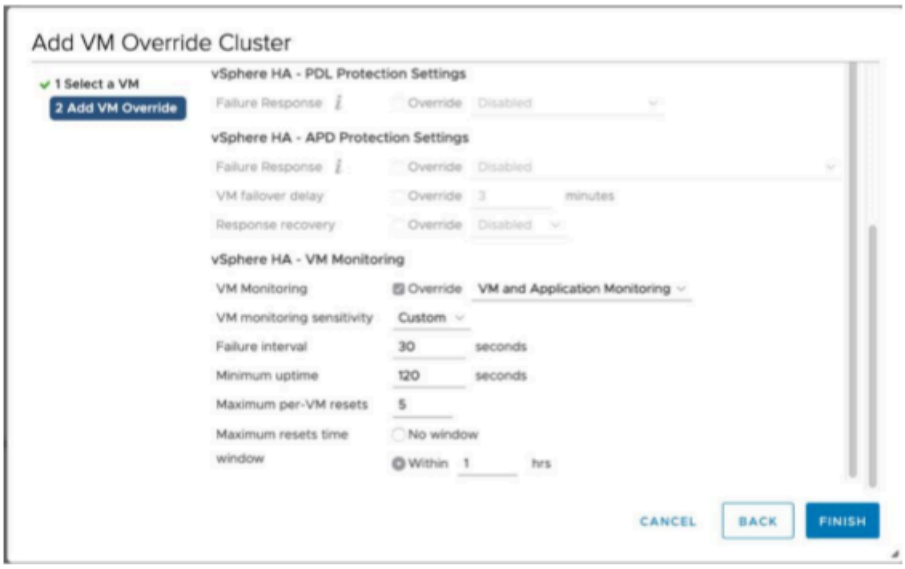
(Facoltativo) Aggiunta di opzioni di sostituzione per altre macchine virtuali nel cluster

Se nel cluster sono in esecuzione altre macchine virtuali, puoi impostare i valori del cluster in modo specifico per ogni macchina virtuale.

Per aggiungere opzioni di sostituzione per altre macchine virtuali nel cluster

1. Nella pagina Summary (Riepilogo) di VMware vSphere scegliere il cluster per aprire la pagina del cluster e quindi scegliere Configure (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.

   Per le opzioni di sostituzione, vedere lo screenshot seguente.



Attivazione del gateway

Dopo aver distribuito il file .ova per il gateway, attiva il gateway. Le istruzioni su come sono diverse per ogni tipo di gateway.

Per attivare il gateway

- Scegli le istruzioni di attivazione in base al tipo di gateway in uso:
  - Gateway file —

Test della configurazione VMware High Availability

Dopo aver attivato il gateway, esegui il test della configurazione.

Per testare la configurazione VMware HA

1. Aprire la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere Gateways (Gateway) e quindi selezionare il gateway che si desidera testare per VMware HA.
3. Per Actions (Operazioni), scegliere Verify VMware HA (Verifica VMware HA).

4. Nella casella Verify VMware High Availability Configuration (Verifica della configurazione VMware High Availability) visualizzata scegliere OK.

   > **Note**
   >
   > Il test della configurazione di VMware HA riavvia la VM 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).

È possibile trovare informazioni sugli eventi VMware HA nei gruppi di log di Amazon CloudWatch. Per ulteriori informazioni, consultare Ottenere i log dello stato del gateway di file con i gruppi di log CloudWatch.

Sicurezza inAWSStorage Gateway

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

- La sicurezza del cloud:AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel AWS Cloud. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano aAWSStorage Gateway, consultaAWSServizi nell'ambito del programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Storage Gateway. I seguenti argomenti illustrano come configurare Storage Gateway per soddisfare gli obiettivi di sicurezza e conformità. Viene anche spiegato come usare altreAWSServizi che consentono di monitorare e proteggere le risorse Storage Gateway.

Argomenti

Protezione dei dati inAWSStorage Gateway

LaAWS modello di responsabilità condivisasi applica alla protezione dei dati inAWSStorage Gateway. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include la configurazione della protezione e le attività di gestione per i servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consultare Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza negli AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli account utente con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con risorse AWS. È consigliabile TLS 1.2 o versioni successive.
- Configura la registrazione delle API e delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consultare il Federal Information Processing Standard (FIPS) 140-2.

Ti suggeriamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero, ad esempio un campo Name (Nome). Ciò include il lavoro con Storage Gateway o altroAWSservizi che utilizzano console, API,AWS CLI, oppureAWSSDK. I dati inseriti nei tag o nei campi in formato libero utilizzati per i nomi possono essere utilizzati per i registri di fatturazione o di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dati utilizzandoAWS KMS

Storage Gateway utilizza SSL/TLS (Secure Socket Layer/Transport Layer Security) per crittografare i dati trasferiti tra un'appliance gateway eAWSarchiviazione. Per impostazione predefinita, Storage Gateway utilizza chiavi di crittografia gestite da Amazon S3 (SSE-S3) per crittografare lato server tutti i dati archiviati in Amazon S3. Puoi usare l'API Storage Gateway per configurare il gateway per crittografare i dati archiviati nel cloud utilizzando la crittografia lato server conAWS Key Management ServiceChiavi master del cliente (SSE-KMS) (SSE-KMS).

> **Important**
>
> Quando si utilizza un appositoAWS KMSCMK per la crittografia lato server, è necessario scegliere una chiave CMK simmetrica. Storage Gateway non supporta le chiavi CMK asimmetriche. Per ulteriori informazioni, consulta Utilizzo di chiavi simmetriche e asimmetriche nella Guida per gli sviluppatori di AWS Key Management Service.

Crittografia di una condivisione file

Per una condivisione di file, puoi configurare il gateway per crittografare gli oggetti conAWS KMS—chiavi gestite utilizzando SSE-KMS. Per informazioni sull'uso dell'API Storage Gateway per crittografare dati scritti in una condivisione di file, consultaCreateNFSFileSharenellaAWS Storage GatewayDocumentazione di riferimento API.

Crittografia di un file system

Per informazioni, consulta.Crittografia dei dati in Amazon FSxnellaGuida per l'utente di Amazon FSx for Windows File Server.

Quando utilizzi AWS KMS per crittografare i dati, ricorda quanto segue:

- I dati vengono crittografati nel cloud mentre sono inattivi. Ciò significa che i dati vengono crittografati in Amazon S3.
- Gli utenti di IAM devono disporre delle autorizzazioni necessarie per chiamare ilAWS KMSOperazioni API. Per ulteriori informazioni, consultaUtilizzo delle policy IAM conAWS KMSnellaAWS Key Management ServiceGuida per gli sviluppatori.
- Se elimini o disabiliti la CMK o revochi il token di concessione, non potrai accedere ai dati sul volume o sul nastro. Per ulteriori informazioni, consultaEliminazione delle chiavi master del clientenellaAWS Key Management ServiceGuida per gli sviluppatori.

- Se crei una snapshot da un volume con crittografia KMS, la snapshot sarà crittografata. La snapshot eredita la chiave KMS del volume.
- Se crei un nuovo volume da una snapshot con crittografia KMS, il volume sarà crittografato. Puoi specificare una chiave KMS differente per il nuovo volume.

> **Note**
>
> Storage Gateway non supporta la creazione di un volume non crittografato da un punto di ripristino di un volume con crittografia KMS o una snapshot con crittografia KMS.

Per ulteriori informazioni su AWS KMS, consulta Che cos'è AWS Key Management Service.

Autenticazione e controllo dell'accesso per Storage Gateway

L'accesso a AWS Storage Gateway richiede credenziali che AWS può utilizzare per autenticare le richieste. Tali credenziali devono disporre delle autorizzazioni per l'accesso.AWSrisorse, ad esempio un gateway, una condivisione file, un volume o un nastro. Le sezioni seguenti forniscono informazioni su come utilizzareAWS Identity and Access Management(IAM)Storage Gateway per proteggere le risorse attraverso il controllo degli accessi:

- Autenticazione
- Controllo degli accessi

Autenticazione

È possibile accedere ad AWS utilizzando uno dei seguenti tipi di identità:

- Utente root Account AWS: quando crei per la prima volta un Account AWS, si inizia con una singola identità di accesso con accesso completo a tutti i servizi e alle risorse AWS nell'account. Tale identità è detta utente root Account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Rispetta piuttosto la best practice di utilizzare l'utente root soltanto per creare il tuo primo utente IAM. Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio.

- Utente IAM— UnUtente IAMè un'identità all'interno del tuoAccount AWSche dispone di autorizzazioni personalizzate specifiche (ad esempio le autorizzazioni necessarie per creare un gateway in Storage Gateway). Puoi utilizzare nome utente e password IAM per accedere a pagine Web AWS sicure come AWS Management Console, forum di discussione AWS o Center AWS Support.

  Oltre a un nome utente e una password, puoi anche generare chiavi di accesso per ciascun utente, che puoi utilizzare per accedere ai servizi AWS in modo programmatico, tramite uno dei vari SDK o l'AWS Command Line Interface (CLI). L'SDK e gli strumenti della CLI utilizzano le chiavi di accesso per firmare crittograficamente la tua richiesta. Se non utilizzi gli strumenti di AWS, devi firmare la richiesta personalmente. Supporta Storage GatewaySignature Version 4, un protocollo per l'autenticazione di richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste API, consulta Processo di firma con Signature Version 4 in Riferimenti generali AWS.

- IAM role (Ruolo IAM): un ruolo IAM) è un'identità IAM che è possibile creare nell'account e che dispone di autorizzazioni specifiche. Un ruolo IAM è simile a un utente IAM, in quanto è un'identità AWS con policy di autorizzazioni che determinano ciò che l'identità può e non può fare in AWS. Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Inoltre, un ruolo non ha credenziali a lungo termine standard associate (password o chiavi di accesso). Tuttavia, quando assumi un ruolo, vengono fornite le credenziali di sicurezza provvisorie per la sessione del ruolo. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

  - Accesso di utenti federati: anziché creare un utente IAM, puoi utilizzare le identità utente preesistenti da AWS Directory Service, la directory utente aziendale o un provider di identità Web. Sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta la sezione relativa a utenti federati e ruoli nella Guida per l'utente di IAM.

  - Accesso al servizioAWS: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella Guida per l'utente di IAM.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste API AWS CLI o AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Controllo degli accessi

Per autenticare le richieste puoi disporre di credenziali valide, ma a meno che tu non disponga delle autorizzazioni non puoi creare o accedere a risorse Storage Gateway. Ad esempio, per creare un gateway in Storage Gateway, devi avere le autorizzazioni appropriate.

Le seguenti sezioni descrivono come gestire le autorizzazioni per Storage Gateway. Consigliamo di leggere prima la panoramica.

- Panoramica sulla gestione delle autorizzazioni di accesso a Storage Gateway
- Policy basate su identità (policy IAM)

Panoramica sulla gestione delle autorizzazioni di accesso a Storage Gateway

OgniAWSLa risorsa è di proprietà di un account Amazon Web Services e le autorizzazioni necessarie per creare o accedere a una risorsa sono regolate dalle policy di autorizzazione. Un amministratore account può collegare le policy di autorizzazione a identità IAM (utenti, gruppi e ruoli) e alcuni servizi (ad esempio AWS Lambda) supportano anche il collegamento delle policy di autorizzazione alle risorse.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consulta Best practice IAM nella Guida per l'utente di IAM.

Quando si concedono le autorizzazioni, è necessario specificare gli utenti che le riceveranno e le risorse per cui si concedono, nonché le operazioni specifiche da consentire su tali risorse.

Argomenti

- Risorse e operazioni Storage Gateway
- Informazioni sulla proprietà delle risorse
- Gestione dell'accesso alle risorse
- Specificazione degli elementi delle policy: Operazioni, effetti, risorse e entità principal
- Specifica delle condizioni in una policy

Risorse e operazioni Storage Gateway

In Storage Gateway, la risorsa principale è unGateway. Storage Gateway supporta anche questi tipi di risorsa aggiuntivi: condivisione file, volume, nastro virtuale, destinazione iSCSI e dispositivo VTL (Virtual Tape Library). In questo caso, si parla di risorse secondarie, che non esistono a meno che non siano state associate a un gateway.

A risorse e risorse secondarie sono associati Amazon Resource Name (ARN) univoci, come illustrato nella tabella seguente.

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`*

> **Note**
>
> Gli ID della risorsa Storage Gateway sono maiuscoli. Quando usi 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. Gli ARN per i gateway attivati prima del 2 settembre 2015 contengono il nome del gateway invece dell'ID gateway. Per ottenere l'ARN per il gateway, usa l'operazione API `DescribeGatewayInformation`.

Per concedere autorizzazioni per determinate operazioni API, come la creazione di un nastro, Storage Gateway fornisce un set di operazioni API che ti permettono di creare e gestire queste risorse e risorse secondarie. Per un elenco di operazioni API di, consultaOperazioninellaAWS Storage GatewayDocumentazione di riferimento API.

Per concedere autorizzazioni per determinate operazioni API, come la creazione di un nastro, Storage Gateway definisce un set di operazioni che possono essere specificate in una policy di autorizzazioni per concedere le autorizzazioni per operazioni API specifiche. Un'operazione API può richiedere le autorizzazioni per più di un'operazione. Per una tabella che mostra tutte le operazioni API Storage Gateway e le risorse cui si applicano, consultaAutorizzazioni API Storage Gateway: Riferimento a operazioni, risorse e condizioni.

Informazioni sulla proprietà delle risorse

UNproprietario delle risorseè l'account Amazon Web Services che ha creato la risorsa. Cioè, il proprietario della risorsa è l'account Amazon Web Services dellaentità principale(l'account root, un utente IAM o un ruolo IAM) che autentica la richiesta che crea la risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se usi credenziali dell'account root del tuo account Amazon Web Services per attivare un gateway, l'account Amazon Web Services è il proprietario della risorsa (in Storage Gateway la risorsa è il gateway).
- Se crei un utente IAM nell'account Amazon Web Services e concedi a`ActivateGateway`Per l'utente, l'utente potrà attivare un gateway. Tenere presente tuttavia che l'account Amazon Web Services a cui appartiene l'utente è il proprietario della risorsa gateway.
- Se crei un ruolo IAM nel tuo account Amazon Web Services con autorizzazioni per l'attivazione di un gateway, chiunque possa assumere il ruolo può attivare un gateway. L'account Amazon Web Services a cui appartiene il ruolo è il proprietario della risorsa gateway.

Gestione dell'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

> **Note**
>
> In questa sezione viene discusso l'uso di IAM nel contesto di Storage Gateway. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione IAM completa, consultaChe cos'è IAMnellaIAM User Guide.Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Riferimento alle policy IAM di AWS nella Guida per l'utente di IAM.

Le policy collegate a un'identità IAM vengono definite policy basate su identità (policy IAM), mentre quelle collegate a una risorsa vengono definite policy basate su risorse. Storage Gateway supporta solo le policy basate su identità (policy IAM).

Argomenti

- Policy basate su identità (policy IAM)

- Policy basate su risorse

Policy basate su identità (policy IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Collegare una policy di autorizzazioni a un utente o un gruppo dell'account— Un amministratore dell'account può utilizzare una policy di autorizzazioni associata a un utente specifico per concedere le autorizzazioni necessarie perché l'utente possa creare una risorsa Storage Gateway, ad esempio un gateway, un volume o un nastro.
- Collega una policy di autorizzazione a un ruolo (assegnazione di autorizzazioni tra account): per concedere autorizzazioni multi-account, è possibile collegare una policy di autorizzazione basata su identità a un ruolo IAM. Ad esempio, l'amministratore dell'account A può creare un ruolo per concedere autorizzazioni multiaccount a un altro account Amazon Web Services (ad esempio l'account B) oppure a unAWSservizio come segue:
  1. L'amministratore dell'account A crea un ruolo IAM e attribuisce una policy di autorizzazione al ruolo che concede le autorizzazioni sulle risorse per l'account A.
  2. L'amministratore dell'account A attribuisce una policy di attendibilità al ruolo, identificando l'account B come il principale per tale ruolo.
  3. L'amministratore dell'account B può quindi delegare le autorizzazioni per assumere tale ruolo a qualsiasi utente dell'account B. In questo modo, gli utenti nell'account B possono creare o accedere alle risorse nell'account A. Se si desidera concedere a un servizio AWS le autorizzazioni per assumere il ruolo, l'entità nella policy di attendibilità può essere anche un'entità servizio AWS.

  Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consulta Access Management nella IAM User Guide (Guida per l'utente di IAM).

Di seguito viene mostrata una policy di esempio che concede autorizzazioni per tutte le operazioni `List*` su tutte le risorse. Questa operazione è di sola lettura. Di conseguenza, la policy non permette all'utente di modificare lo stato delle risorse.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
```

```
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni sull'uso di policy basate su identità con Storage Gateway, consultaUtilizzo di policy basate su identità (policy IAM) per Storage Gateway. Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Policy basate su risorse

Anche altri servizi, come Amazon S3, supportano policy di autorizzazioni basate su risorse. Ad esempio, è possibile associare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. Storage Gateway non supporta policy basate su risorse.

Specificazione degli elementi delle policy: Operazioni, effetti, risorse e entità principal

Per ogni risorsa Storage Gateway (vedereAutorizzazioni API Storage Gateway: Riferimento a operazioni, risorse e condizioni), il servizio definisce un set di operazioni API (consultaOperazioni). Per concedere le autorizzazioni per queste operazioni API, Storage Gateway definisce un insieme di operazioni che possono essere specificate in una policy. Ad esempio, per la risorsa gateway Storage Gateway, vengono definite queste operazioni:`ActivateGateway`,`DeleteGateway`, e`DescribeGatewayInformation`. Si noti che l'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'azione.

Di seguito sono elencati gli elementi di base di una policy:

- Risorsa - in una policy si utilizza un nome Amazon Resource Name (ARN) per identificare la risorsa a cui si applica la policy stessa. Per le risorse Storage Gateway, si utilizza sempre il carattere jolly`(*)`nelle policy IAM. Per ulteriori informazioni, consultare Risorse e operazioni Storage Gateway.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, a seconda del specificato`Effect`, il`storagegateway:ActivateGateway`consente o rifiuta all'utente le autorizzazioni per eseguire Storage Gateway`ActivateGateway`operazione.

- Effetto: l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- Principale - Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). Storage Gateway non supporta policy basate su risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta AWSRiferimento alle policy IAM nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le operazioni API Storage Gateway, consultaAutorizzazioni API Storage Gateway: Riferimento a operazioni, risorse e condizioni.

Specifica delle condizioni in una policy

Quando concedi le autorizzazioni, puoi usare il linguaggio delle policy IAM per specificare le condizioni in base alle quali applicare una policy. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta Condizione nella Guida per l'utente di IAM.

Per esprimere le condizioni, devi usare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per Storage Gateway. Tuttavia, ci sono disponibili chiavi di condizione AWS che puoi utilizzare secondo necessità. Per un elenco completo delle chiavi AWS, consulta Chiavi disponibili nella Guida per l'utente IAM.

Utilizzo di policy basate su identità (policy IAM) per Storage Gateway

In questo argomento vengono forniti esempi di policy basate su identità in cui un amministratore account può collegare policy di autorizzazione a identità IAM, ovvero utenti, gruppi e ruoli.

> **Important**
>
> Innanzitutto, è consigliabile esaminare gli argomenti introduttivi in cui vengono spiegati i concetti di base e le opzioni disponibili per gestire l'accesso alle risorse Storage Gateway. Per ulteriori informazioni, consultare Panoramica sulla gestione delle autorizzazioni di accesso a Storage Gateway.

In questa sezione vengono trattati gli argomenti seguenti:

- Autorizzazioni necessarie per l'uso della console Storage Gateway
- AWSpolicy gestite per Storage Gateway
- Esempi di policy gestite dal cliente

Di seguito viene illustrato un esempio di policy di autorizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

La policy include due istruzioni. Nota gli elementi `Action` e `Resource` in entrambe le istruzioni:

- La prima istruzione concede le autorizzazioni per due operazioni Storage Gateway (`storagegateway:ActivateGatewaystoragegateway:ListGateways`) su una risorsa gateway.

  Il carattere jolly (*) significa che questa istruzione può corrispondere a qualsiasi risorsa. In questo caso, la dichiarazione consente la`storagegateway:ActivateGatewaystoragegateway:ListGatewaysazioni` su qualsiasi

gateway. Qui viene utilizzato il carattere jolly perché non si conosce l'ID risorsa finché non crei il gateway. Per informazioni su come usare un carattere jolly (*) in una policy, consulta Esempio 2: Consentire l'accesso in sola lettura a un gateway.

> **Note**
>
> Gli ARN identificano in modo univocoAWSrisorse AWS. Per ulteriori informazioni, consulta Amazon Resource Name (ARN) e Spazi dei nomi del servizio AWS nei AWS Riferimenti generali.

Per limitare le autorizzazioni per una determinata operazione su un solo gateway specifico, crea un'istruzione separata per l'operazione nella policy e indica l'ID gateway nell'istruzione.

- La seconda istruzione concede le autorizzazioni per le operazioni `ec2:DescribeSnapshots` e `ec2:DeleteSnapshot`. Queste operazioni Amazon Elastic Compute Cloud (Amazon EC2) richiedono autorizzazioni perché gli snapshot generati da Storage Gateway vengono archiviati in Amazon Elastic Block Store (Amazon EBS) e gestiti come risorse Amazon EC2 e di conseguenza richiedono operazioni EC2 corrispondenti. Per ulteriori informazioni, consultaOperazioninellaInformazioni di riferimento delle API di Amazon EC2. Poiché queste operazioni Amazon EC2 non supportano le autorizzazioni a livello di risorsa, la policy specifica il carattere jolly (*) come`Resource`valore invece di specificare un gateway ARN.

Per una tabella che mostra tutte le operazioni API di Storage Gateway e le risorse a cui si applicano, consultaAutorizzazioni API Storage Gateway: Riferimento a operazioni, risorse e condizioni.

Autorizzazioni necessarie per l'uso della console Storage Gateway

Per utilizzare la console Storage Gateway, devi concedere autorizzazioni di sola lettura. Se prevedi di descrivere snapshot, devi anche concedere autorizzazioni per operazioni aggiuntive, come mostrato nella policy di autorizzazioni seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Questa autorizzazione aggiuntiva è necessaria perché gli snapshot Amazon EBS generati da Storage Gateway vengono gestiti come risorse Amazon EC2.

Per configurare le autorizzazioni minime necessarie per passare alla console Storage Gateway, consultaEsempio 2: Consentire l'accesso in sola lettura a un gateway.

AWSpolicy gestite per Storage Gateway

Amazon Web Services gestisce molti casi di utilizzo comune con policy IAM autonome create e amministrate daAWS. Le policy gestite concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non dover cercare quali sono le autorizzazioni richieste. Per ulteriori informazioni suAWSpolicy gestite, consultaAWSPolicy gestitenellaIAM User Guide.

I seguentiAWSLe policy gestite da, che puoi collegare agli utenti nel tuo account, sono specifiche di Storage Gateway:

- AWSStorageGatewayReadOnlyAccess: concede accesso in sola lettura a risorse AWS Storage Gateway.
- AWSStorageGatewayFullAccess: concede accesso completo a risorse AWS Storage Gateway.

> **Note**
>
> Per esaminare queste policy di autorizzazione, accedi alla console IAM ed esegui la ricerca delle policy specifiche.

Puoi anche creare policy IAM personalizzate per concedere autorizzazioni per operazioni API AWS Storage Gateway. Puoi collegare queste policy personalizzate agli utenti o ai gruppi IAM che richiedono le autorizzazioni.

Esempi di policy gestite dal cliente

In questa sezione vengono mostrate policy utente di esempio che concedono autorizzazioni per diverse operazioni Storage Gateway. Queste policy funzionano quando usiAWSSDK eAWS CLI. Se utilizzi la console, sarà necessario concedere autorizzazioni aggiuntive specifiche per quest'ultima, come illustrato in Autorizzazioni necessarie per l'uso della console Storage Gateway.

> **Note**
>
> Tutti gli esempi utilizzano la regione Stati Uniti occidentali (Oregon) (`us-west-2`) e contengono ID account fittizi.

Argomenti

Esempio 1: Consenti qualsiasi azione Storage Gateway su tutti i gateway

La policy seguente permette a un utente di eseguire tutte le operazioni Storage Gateway. La policy permette inoltre all'utente di eseguire operazioni Amazon EC2 (DescribeSnapshotseDeleteSnapshot) sugli snapshot Amazon EBS generati da Storage Gateway.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Esempio 2: Consentire l'accesso in sola lettura a un gateway

La policy seguente permette tutte le operazioni `List*` e `Describe*` su tutte le risorse. Tieni presente che queste operazioni sono di sola lettura. Di conseguenza, la policy non permette all'utente di modificare lo stato di alcuna risorsa, ovvero non permette all'utente di eseguire operazioni come `DeleteGateway`, `ActivateGateway` e `ShutdownGateway`.

La policy permette anche l'operazione Amazon EC2 `DescribeSnapshots`. Per ulteriori informazioni, consultaDescribeSnapshotsnellaInformazioni di riferimento delle API di Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

Invece di usare un carattere jolly (*) nella policy precedente, puoi definire l'ambito delle risorse gestite dalla policy in base a un gateway specifico, come mostrato nell'esempio seguente. La policy permette quindi le operazioni solo sul gateway specifico.

```
"Resource": [
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

All'interno di un gateway puoi limitare ulteriormente l'ambito delle risorse ai soli volumi del gateway, come mostrato nell'esempio seguente:

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

Esempio 3: Consentire l'accesso a un gateway specifico

La policy seguente permette tutte le operazioni su un gateway specifico. All'utente non è consentito accedere ad altri gateway che potresti aver distribuito.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

La policy precedente funziona se l'utente cui è collegata usa l'API o unAWSSDK per accedere al gateway. Tuttavia, se l'utente userà la console Storage Gateway, devi concedere anche le autorizzazioni necessarie per permettere la`ListGateways`action, come mostrato nell'esempio seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        }
    ]
}
```

Esempio 4: Consentire a un utente di accedere a un volume specifico

La policy seguente permette a un utente di eseguire tutte le operazioni su un volume specifico in un gateway. Poiché un utente non ottiene alcuna autorizzazione per impostazione predefinita, la policy permette all'utente di accedere a un solo volume specifico.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

La policy precedente funziona se l'utente cui è collegata usa l'API o unAWSSDK per accedere al volume. Tuttavia, se questo utente utilizzerà ilAWS Storage Gatewayconsole, devi concedere anche le autorizzazioni per consentire`ListGateways`action, come mostrato nell'esempio seguente.

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

```
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Esempio 5: Consenti tutte le azioni sui gateway con un prefisso specifico

La policy seguente permette a un utente di eseguire tutte le operazioni Storage Gateway su gateway con nomi che iniziano per`DeptX`. La policy permette anche la`DescribeSnapshots`Azione Amazon EC2, necessaria se prevedi di descrivere snapshot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        }
    ]
}
```

La policy precedente funziona se l'utente cui è collegata usa l'API o unAWSSDK per accedere al gateway. Tuttavia, se questo utente ha intenzione di utilizzare ilAWS Storage Gatewayconsole, devi concedere autorizzazioni aggiuntive come descritto inEsempio 3: Consentire l'accesso a un gateway specifico.

Utilizzo dei tag per controllare l'accesso al gateway e alle risorse

Per controllare l'accesso alle operazioni e risorse di gateway, è possibile utilizzare le 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`.

```
{
  "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:region:account-id:*/*"
        }
    ]
}
```

Controllo dell'accesso in base ai tag di una richiesta IAM

Per controllare cosa un utente IAM può fare su una risorsa di gateway, è possibile utilizzare le condizioni in una policy IAM basata su tag. Ad esempio, è possibile scrivere una policy che consente o nega a un utente IAM 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.

```
{
   "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"
            }
         }
      }
   ]
}
```

Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB

Amazon S3 File Gateway supporta due metodi diversi per il controllo dell'accesso a file e directory che vengono archiviati tramite una condivisione di file SMB: Autorizzazioni POSIX o ACL Windows.

In questa sezione, è possibile trovare informazioni su come utilizzare le liste di controllo degli accessi (ACL) di Microsoft Windows su condivisioni di file SMB abilitate con Microsoft Active Directory (AD). Utilizzando le ACL di Windows, è possibile impostare autorizzazioni granulari su file e cartelle nella propria condivisione di file SMB.

Di seguito sono elencate alcune importanti caratteristiche delle Windows ACL su condivisioni di file SMB:

- Gli ACL di Windows vengono selezionati per impostazione predefinita per le condivisioni di file SMB quando il File Gateway viene unito a un dominio Active Directory.
- Quando le ACL sono abilitate, le informazioni sulle ACL vengono conservate nei metadati degli oggetti Amazon S3.
- Il gateway conserva fino a 10 ACL per ogni file o cartella.
- Quando si utilizza una condivisione di file SMB con ACL abilitati ad accedere a oggetti S3 creati all'esterno del gateway, gli oggetti ereditano le informazioni delle ACL dalla cartella principale.
- La lista di controllo degli accessi root predefinita per un file di condivisione SMB offre accesso completo a tutti, ma è possibile modificare le autorizzazioni della ACL root. È possibile utilizzare le liste di controllo accessi (ACL) per controllare l'accesso alla condivisione di file. È possibile impostare chi può montare la condivisione di file (mappare l'unità) e quali autorizzazioni ottiene l'utente per i file e le cartelle in modo ricorsivo nella condivisione di file. Tuttavia, consigliamo di impostare questa autorizzazione nella cartella di livello superiore nel bucket S3 in modo che la lista di controllo degli accessi venga mantenuta.

È possibile abilitare le liste di controllo degli accessi di Windows al momento della creazione di un nuovo file di condivisione SMB utilizzando l'operazione API CreateSMBFileShare. In alternativa, è possibile abilitare le ACL di Windows in un file di condivisione SMB esistente tramite l'operazione API UpdateSMBFileShare.

Abilitazione di ACL di Windows in una nuova condivisione di file SMB

Segui la procedura seguente per abilitare le ACL di Windows in una nuova condivisione di file SMB.

Come abilitare le ACL di Windows al momento della creazione di una nuova condivisione di file SMB

1. Creare un file gateway se non si dispone già di uno. Per ulteriori informazioni, consultare .
2. Se il gateway non è stato aggiunto a un dominio, aggiungerlo a un dominio. Per ulteriori informazioni, consultare .
3. Creare una condivisione di file SMB.
4. Abilitare le ACL di Windows sulla condivisione file dalla console Storage Gateway.

   Per utilizzare la console Storage Gateway, eseguire queste operazioni:

   a. Scegliere la condivisione file e scegliere Edit file share (Modifica condivisione file).
   b. Per l'opzione File/directory access controlled by (Accesso a file/directory controllato da) scegliere Windows Access Control List (Lista di controllo accessi di Windows).

5. (Facoltativo) Aggiungere un utente amministratore a AdminUsersList, se si desidera che l'utente amministratore disponga di privilegi per aggiornare le ACL su tutti i file e tutte le cartelle nella condivisione di file.
6. Aggiornare le liste di controllo degli accessi per le cartelle padre nella cartella root. Per eseguire questa operazione, utilizzare Windows File Explorer per configurare le ACL nelle cartelle nella condivisione di file SMB.

   > **Note**
   >
   > Se configuri le liste di controllo degli accessi nella root invece della cartella padre in root, le autorizzazioni ACL non vengono mantenute in Amazon S3.

   Consigliamo di impostare le ACL nella cartella principale nel root della condivisione di file, invece di impostare le ACL direttamente nel root della condivisione di file. Questo approccio mantiene le informazioni come metadati degli oggetti in Amazon S3.
7. Abilitare l'ereditarietà in base alle esigenze.

   > **Note**
   >
   > È possibile abilitare l'ereditarietà per condivisioni di file create dopo l'8 maggio 2019.

Se abiliti l'ereditarietà e aggiorni le autorizzazioni in modo ricorsivo, Storage Gateway aggiorna tutti gli oggetti nel bucket S3. A seconda del numero di oggetti nel bucket, l'aggiornamento può richiedere alcuni minuti per il completamento.

Abilitazione di ACL di Windows in una condivisione file SMB esistente

Segui la procedura seguente per abilitare le ACL di Windows in una condivisione di file SMB esistente con autorizzazioni POSIX.

Per abilitare le ACL di Windows su una condivisione file SMB esistente tramite la console Storage Gateway

1. Scegliere la condivisione file e scegliere Edit file share (Modifica condivisione file).
2. Per l'opzione File/directory access controlled by (Accesso a file/directory controllato da) scegliere Windows Access Control List (Lista di controllo accessi di Windows).

3. Abilitare l'ereditarietà in base alle esigenze.

> **Note**
>
> Non è consigliabile impostare le ACL al livello root, poiché se si effettua questa operazione e si elimina il gateway, è necessario ripristinare nuovamente le ACL.

Se abiliti l'ereditarietà e aggiorni le autorizzazioni in modo ricorsivo, Storage Gateway aggiorna tutti gli oggetti nel bucket S3. A seconda del numero di oggetti nel bucket, l'aggiornamento può richiedere alcuni minuti per il completamento.

Restrizioni nell'utilizzo di ACL di Windows

Mantieni i seguenti limiti quando utilizzi ACL di Windows per controllare l'accesso a condivisioni di file SMB:

- Le ACL di Windows sono supportate solo su condivisioni di file abilitate per Active Directory quando utilizzi client SMB Windows per accedere alle condivisioni di file.
- I gateway di file supportano un massimo di 10 voci ACL per ogni file e directory.
- I gateway file non supportano`AuditeAlarm`voci, ovvero voci SACL (elenco di controllo degli accessi al sistema). I file gateway supportano voci `Allow` e `Deny`, ovvero voci DACL (elenco di controllo degli accessi discrezionale).
- Le impostazioni ACL root di condivisione dei file SMB sono presenti solo sul gateway e le impostazioni vengono mantenute in aggiornamenti e riavvii del gateway.

> **Note**
>
> Se configuri le ACL nella root invece della cartella padre nel root, le autorizzazioni ACL non vengono mantenute in Amazon S3.

In tali condizioni, assicurati di eseguire quanto segue:

- Se configuri più gateway per accedere allo stesso bucket Amazon S3, configura l'ACL root su ciascuno dei gateway per mantenere le autorizzazioni coerenti.
- Se elimini una condivisione di file e la ricrei sullo stesso bucket Amazon S3, assicurati di utilizzare lo stesso set di ACL root.

Autorizzazioni API Storage Gateway: Riferimento a operazioni, risorse e condizioni

Quando configuri il controllo dell'accesso e scrivi policy di autorizzazione da collegare a un'identità IAM (policy basate sull'identità), è possibile utilizzare la seguente tabella come riferimento. Nella tabella sono elencate le operazioni API di Storage Gateway, le operazioni corrispondenti per le quali puoi concedere le autorizzazioni necessarie per eseguire l'operazione eAWSrisorsa per la quale è possibile concedere le autorizzazioni. Puoi specificare le operazioni nel campo `Action` della policy e il valore della risorsa nel campo `Resource`.

È possibile utilizzareAWS-chiavi di condizione a livello di nelle policy Storage Gateway per esprimere le condizioni. Per un elenco completo delle chiavi AWS, consulta Chiavi disponibili nella Guida per l'utente IAM.

> **Note**
>
> Per specificare un'operazione, utilizza il prefisso `storagegateway:` seguito dal nome dell'operazione API (ad esempio, `storagegateway:ActivateGateway`). Per ogni operazione Storage Gateway, puoi specificare un carattere jolly (*) come risorsa.

Per un elenco delle risorse Storage Gateway con i formati ARN, consultaRisorse e operazioni Storage Gateway.

L'API Storage Gateway e le autorizzazioni necessarie per le operazioni sono le seguenti.

ActivateGateway

Operazioni: `storagegateway:ActivateGateway`

Risorsa: *

AddCache

Operazioni: `storagegateway:AddCache`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

AddTagsToResource

Operazioni: `storagegateway:AddTagsToResource`

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

oppure

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

oppure

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

Operazioni: storagegateway:AddUploadBuffer

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

Operazioni: storagegateway:AddWorkingStorage

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

Operazioni: storagegateway:CancelArchival

Risorsa: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

Operazioni: storagegateway:CancelRetrieval

Risorsa: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

Operazioni: storagegateway:CreateCachediSCSIVolume

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

Operazioni: storagegateway:CreateSnapshot

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

Operazioni: `storagegateway:CreateSnapshotFromVolumeRecoveryPoint`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

CreateStorediSCSIVolume

Operazioni: `storagegateway:CreateStorediSCSIVolume`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

CreateTapes

Operazioni: `storagegateway:CreateTapes`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteBandwidthRateLimit

Operazioni: `storagegateway:DeleteBandwidthRateLimit`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteChapCredentials

Operazioni: `storagegateway:DeleteChapCredentials`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

DeleteGateway

Operazioni: `storagegateway:DeleteGateway`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteSnapshotSchedule

Operazioni: `storagegateway:DeleteSnapshotSchedule`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DeleteTape

Operazioni: `storagegateway:DeleteTape`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteTapeArchive

Operazioni: `storagegateway:DeleteTapeArchive`

Risorsa: *

DeleteVolume

Operazioni: `storagegateway:DeleteVolume`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeBandwidthRateLimit

Operazioni: `storagegateway:DescribeBandwidthRateLimit`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeCache

Operazioni: `storagegateway:DescribeCache`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeCachediSCSIVolumes

Operazioni: `storagegateway:DescribeCachediSCSIVolumes`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeChapCredentials

Operazioni: `storagegateway:DescribeChapCredentials`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

DescribeGatewayInformation

Operazioni: `storagegateway:DescribeGatewayInformation`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeMaintenanceStartTime

Operazioni: `storagegateway:DescribeMaintenanceStartTime`

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

Operazioni: storagegateway:DescribeSnapshotSchedule

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

Operazioni: storagegateway:DescribeStorediSCSIVolumes

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeTapeArchives

Operazioni: storagegateway:DescribeTapeArchives

Risorsa: *

DescribeTapeRecoveryPoints

Operazioni: storagegateway:DescribeTapeRecoveryPoints

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

Operazioni: storagegateway:DescribeTapes

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeUploadBuffer

Operazioni: storagegateway:DescribeUploadBuffer

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeVTLDevices

Operazioni: storagegateway:DescribeVTLDevices

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeWorkingStorage

Operazioni: storagegateway:DescribeWorkingStorage

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DisableGateway

Operazioni: storagegateway:DisableGateway

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListGateways

Operazioni: storagegateway:ListGateways

Risorsa: *

ListLocalDisks

Operazioni: storagegateway:ListLocalDisks

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListTagsForResource

Operazioni: storagegateway:ListTagsForResource

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

oppure

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

oppure

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

Operazioni: storagegateway:ListTapes

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

Operazioni: storagegateway:ListVolumeInitiators

Risorsa: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

Operazioni: `storagegateway:ListVolumeRecoveryPoints`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListVolumes

Operazioni: `storagegateway:ListVolumes`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RemoveTagsFromResource

Operazioni: `storagegateway:RemoveTagsFromResource`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

oppure

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

oppure

arn:aws:storagegateway:*`region`*:*`account-id`*:tape/*`tapebarcode`*

ResetCache

Operazioni: `storagegateway:ResetCache`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RetrieveTapeArchive

Operazioni: `storagegateway:RetrieveTapeArchive`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

RetrieveTapeRecoveryPoint

Operazioni: `storagegateway:RetrieveTapeRecoveryPoint`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ShutdownGateway

Operazioni: `storagegateway:ShutdownGateway`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

StartGateway

Operazioni: `storagegateway:StartGateway`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateBandwidthRateLimit

Operazioni: `storagegateway:UpdateBandwidthRateLimit`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateChapCredentials

Operazioni: `storagegateway:UpdateChapCredentials`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

UpdateGatewayInformation

Operazioni: `storagegateway:UpdateGatewayInformation`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateGatewaySoftwareNow

Operazioni: `storagegateway:UpdateGatewaySoftwareNow`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateMaintenanceStartTime

Operazioni: `storagegateway:UpdateMaintenanceStartTime`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateSnapshotSchedule

Operazioni: `storagegateway:UpdateSnapshotSchedule`

Risorsa: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

UpdateVTLDeviceType

Operazioni: `storagegateway:UpdateVTLDeviceType`

Risorsa: `arn:aws:storagegateway:region:account-id:gateway/gateway-id/device/vtldevice`

Argomenti correlati

- Controllo degli accessi
- Esempi di policy gestite dal cliente

Utilizzo di ruoli collegati ai servizi per Storage Gateway

Utilizzo Storage GatewayAWS Identity and Access Management(IAM)ruoli collegati ai servizi. Un ruolo collegato ai servizi è un tipo univoco di ruolo IAM collegato direttamente a Storage Gateway. I ruoli collegati ai servizi sono definiti automaticamente da Storage Gateway e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri.AWSservizi per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Storage Gateway perché permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Storage Gateway definisce le autorizzazioni dei relativi ruoli collegati ai servizi e, salvo diversamente definito, solo Storage Gateway potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegliere un link Yes (Sì) per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Storage Gateway

Storage Gateway utilizza il ruolo collegato ai servizi denominatoRuolo del servizio AWS per Storage Gateway— Ruolo del servizio AWS per Storage Gateway.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForStorageGateway considera attendibili i seguenti servizi:

- `storagegateway.amazonaws.com`

La policy delle autorizzazioni del ruolo consente a Storage Gateway di eseguire le seguenti operazioni sulle risorse specificate:

- Operazione: `fsx:ListTagsForResource` su `arn:aws:fsx:*:*:backup/*`

Devi configurare le autorizzazioni per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di creare e modificare un ruolo collegato ai servizi. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Storage Gateway

Non devi creare manualmente un ruolo collegato ai servizi. Quando si crea uno Storage Gateway`AssociateFileSystem`Chiamata API nellaAWS Management Console, ilAWS CLI, o ilAWSAPI, Storage Gateway crea automaticamente il ruolo collegato ai servizi.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Inoltre, se si utilizzava il servizio Storage Gateway prima del 31 marzo 2021, quando ha iniziato a supportare i ruoli collegati ai servizi, Storage Gateway ha creato il ruolo AWSServiceRoleForStorageGateway nell'account. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se si elimina questo ruolo collegato ai servizi e quindi deve essere creato di nuovo, è possibile utilizzare lo stesso processo per ricreare il ruolo nell'account. Quando si crea uno Storage Gateway`AssociateFileSystem`Chiamata API, Storage Gateway crea nuovamente il ruolo collegato ai servizi per conto tuo.

È inoltre possibile utilizzare la console IAM per creare un ruolo collegato ai servizi con ilRuolo del servizio AWS per Storage Gatewaycaso d'uso. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `storagegateway.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per Storage Gateway

Storage Gateway non consente di modificare il ruolo collegato ai servizi AWSServiceRoleForStorageGateway. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne

la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Storage Gateway

Storage Gateway non elimina automaticamente il ruolo AWSServiceRoleForStorageGateway. Per eliminare il ruolo AWSServiceRoloforStorageGateway, è necessario richiamare il ruolo`iam:DeleteSLR`API. Se non ci sono risorse gateway di storage che dipendono dal ruolo collegato al servizio, l'eliminazione avrà esito positivo, altrimenti l'eliminazione avrà esito negativo. Se si desidera eliminare il ruolo collegato al servizio, è necessario utilizzare le API IAM`iam:DeleteRole`o`iam:DeleteServiceLinkedRole`. In questo caso, è necessario utilizzare le API Storage Gateway per eliminare innanzitutto eventuali gateway o associazioni di file system nell'account, quindi eliminare il ruolo collegato al servizio utilizzando`iam:DeleteRole`o`iam:DeleteServiceLinkedRole`API. Quando si elimina il ruolo collegato al servizio utilizzando IAM, è necessario utilizzare Storage Gateway`DisassociateFileSystemAssociation`API innanzitutto per eliminare tutte le associazioni di file system nell'account. In caso contrario, l'operazione di eliminazione avrà esito negativo.

> **Note**
>
> Se il servizio Storage Gateway utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Storage Gateway utilizzate da AWSServiceRoleForStorageGateway

1. Utilizza la nostra console di servizio, CLI o API per effettuare una chiamata che pulisce le risorse ed elimina il ruolo o utilizza la console IAM, la CLI o l'API per eseguire l'eliminazione. In questo caso, è necessario utilizzare le API Storage Gateway per eliminare innanzitutto i gateway e le associazioni di file system nell'account.
2. Se si usa la console IAM, CLI o l'API, elimina il ruolo collegato ai servizi tramite IAM`DeleteRole`o`DeleteServiceLinkedRole`API.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizzare la console IAM,AWS CLI, o ilAWSAPI per eliminare il ruolo collegato al servizio AWSServiceRoleForStorageGateway collegato al ruolo collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Storage Gateway

Storage Gateway supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint del servizio AWS.

Storage Gateway non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. È possibile utilizzare il ruolo AWSServiceRoleForStorageGateway nelle seguenti regioni.

Nome regione	Identità della regione	Support in Storage Gateway
US East (N. Virginia)	us-east-1	Sì
US East (Ohio)	us-east-2	Sì
Stati Uniti occidentali (California settentrionale)	us-west-1	Sì
US West (Oregon)	us-west-2	Sì
Asia Pacifico (Mumbai)	ap-south-1	Sì
Asia Pacifico (Osaka)	ap-northeast-3	Sì
Asia Pacifico (Seoul)	ap-northeast-2	Sì
Asia Pacific (Singapore)	ap-southeast-1	Sì
Asia Pacific (Sydney)	ap-southeast-2	Sì
Asia Pacific (Tokyo)	ap-northeast-1	Sì
Canada (Centrale)	ca-central-1	Sì
Europa (Francoforte)	eu-central-1	Sì

Nome regione	Identità della regione	Support in Storage Gateway
Europe (Ireland)	eu-west-1	Sì
Europa (Londra)	eu-west-2	Sì
Europa (Parigi)	eu-west-3	Sì
South America (São Paulo)	sa-east-1	Sì
AWS GovCloud (US)	us-gov-west-2	Sì

Registrazione e monitoraggio in AWS Storage Gateway

Storage Gateway è integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Storage Gateway. CloudTrail acquisisce tutte le chiamate API per Storage Gateway come eventi. Le chiamate acquisite includono le chiamate dalla console Storage Gateway e le chiamate di codice alle operazioni dell'API Storage Gateway. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Storage Gateway. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata a Storage Gateway, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni su Storage Gateway in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Storage Gateway, questa viene registrata in un evento CloudTrail insieme ad altri.AWSeventi di servizio inCronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continuativa di attività ed eventi nella tuaAWSaccount, inclusi gli eventi per Storage Gateway, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket

Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di registro nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei registri CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le operazioni Storage Gateway sono registrate e documentate nellaOperazioniargomento. Ad esempio, le chiamate alle operazioni `ActivateGateway`, `ListGateways` e `ShutdownGateway` generano voci nei file di log di CloudTrail.

Ogni evento o voce del registro contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail.

Informazioni sulle voci dei file di log di Storage Gateway

Un trail è una configurazione che consente l'implementazione di eventi come i file di log in un bucket Amazon S3 che specifichi. I file di registro di CloudTrail possono contenere una o più voci di registro. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione .

```
{ "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 log di CloudTrail che illustra l'operazione ListGateways.

```
{
 "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"
              }]
}
```

Convalida della conformità perAWSStorage Gateway

Revisori di terze parti valutano la sicurezza e la conformità diAWSStorage Gateway come parte di piùAWSprogrammi di conformità. Questi includono SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Per un elenco dei servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consulta Servizi AWS che rientrano nell'ambito del programma di conformità . Per informazioni generali, consulta Programmi per la conformità di AWS.

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La tua responsabilità di conformità durante l'utilizzo di Storage Gateway è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e normative applicabili.AWSfornisce le seguenti risorse per facilitare la conformità:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance) (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- Risorse per la conformitàAWS - Una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config - Il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza inAWSStorage Gateway

L'infrastruttura globale di AWS è basata su regioni e zone di disponibilità AWS. AWS Le Regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle regioni AWS e sulle zone di disponibilit, consulta Infrastruttura globale di AWS.

Oltre allaAWSinfrastruttura globale, Storage Gateway offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

- Utilizzare VMware vSphere High Availability (VMware HA) per proteggere i carichi di lavoro di archiviazione da errori hardware, hypervisor o di rete. Per ulteriori informazioni, consultaUtilizzo di VMware vSphere High Availability con Storage Gateway.

- Usa AWS Backup per il backup dei volumi. Per ulteriori informazioni, consultaUtilizzo diAWS Backupper il backup dei volumi.
- Clona il volume da un punto di ripristino. Per ulteriori informazioni, consultaClonazione di un volume.
- Archivia i nastri virtuali in Amazon S3 Glacier. Per ulteriori informazioni, consultaArchiviazione di nastri virtuali.

Sicurezza dell'infrastruttura inAWSStorage Gateway

Come servizio gestito,AWSStorage Gateway è protetto daAWSprocedure di sicurezza di rete globali descritte nellaAmazon Web Services: Panoramica sui processi di sicurezzawhite epaper.

Si usaAWSchiamate all'API pubblicate per accedere a Storage Gateway tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura 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 le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Best practice relative alla sicurezza per Storage Gateway

AWSStorage Gateway fornisce una serie di caratteristiche di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Dato che queste best practice potrebbero non essere appropriate o sufficienti nel proprio ambiente, si considerino come riflessioni utili più che istruzioni. Per ulteriori informazioni, consultaAWSBest practice di sicurezza.

Risoluzione dei problemi del gateway

Le informazioni riportate di seguito ti consentono di risolvere i problemi relativi a gateway, condivisioni di file, volumi, nastri virtuali e snapshot in cui potresti imbatterti. Le soluzioni ai problemi di gateway in locale valgono sia per i gateway distribuiti su client VMware ESXi che per quelli su Microsoft Hyper-V. Le informazioni sulla risoluzione dei problemi relativi alla condivisione file riguardano il tipo Amazon S3 File Gateway (File Gateway) di Amazon S3. Le informazioni sulla risoluzione dei problemi relativi ai volumi riguardano il tipo di gateway di volumi. Le informazioni sulla risoluzione dei problemi relativi ai nastri riguardano il tipo di gateway di nastri. Le informazioni sulla risoluzione dei problemi relativi al gateway riguardano l'utilizzo delle metriche di CloudWatch. Le informazioni sulla risoluzione dei problemi relativi alla disponibilità elevata riguardano i gateway in esecuzione sulla piattaforma VMware vSphere High Availability (HA).

Argomenti

Come risolvere i problemi di gateway in locale

Nelle informazioni seguenti sono elencati i più comuni problemi che potrebbero verificarsi utilizzando gateway distribuiti in locale e su come abilitare.AWS SupportPer aiutare a risolvere i problemi del gateway.

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. • Per VMware ESXi, l'indirizzo IP della VM si trova nel client vSphere nella scheda Summary (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: • 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 abilitino questi endpoint di servizio alle comunicazioni in uscita aAWS. Per ulteriori informazioni sui requisiti di rete e del firewall, consulta Requisiti di rete e firewall.
Facendo clic sul pulsante, l'attivazione del gateway non si attivaContinua con l'attivazionepulsante nella Storage Gateway Management Console.	• 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 Test 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 su come verificare e sincronizzare

Problema	Operazione da eseguire
	l'orario di host degli hypervisor e VM, consulta Configurazione di un server NTP (Network Time Protocol) per il gateway. • Dopo queste fasi preliminari, è possibile tornare a dedicarsi alla distribuzione del gateway con la console Storage Gateway (Storage Gateway) eConfigurazione e attivazione del gatewaymago. • Verificare che la VM disponga di almeno 7,5 GB di RAM; in caso contrario, l'allocazione del gateway avrà esito negativo. Per ulteriori informazioni, consultare Configurazione del gateway di file.
È necessario rimuovere un disco allocato come spazio del buffer di caricamen to. Ad esempio, si intende ridurre lo spazio del buffer di caricamento di un gateway o bisogna sostituir e un disco utilizzato come buffer di caricamento in cui si sono verificati errori.	

Problema	Operazione da eseguire
Occorre aumentare la larghezza di banda tra il gateway eAWS.	Per aumentare la larghezza di banda tra il gateway e AWS è sufficiente impostare la connessione Internet con AWS su una scheda di rete (NIC) diversa da quella che connette le applicazioni e la VM del gateway. Così facendo, si può disporre di una connessio ne ad ampia larghezza di banda ad AWS senza incorrere nelle contese di banda, rischio concreto soprattutto durante un ripristin o di snapshot. Per esigenze di carichi di lavoro ad alto throughpu t, è possibile utilizzareAWS Direct Connectstabilire una connessio ne di rete dedicata tra il gateway locale eAWS. Per misurare la larghezza di banda della connessione tra il gateway e AWSutiliz zare i parametri del gateway `CloudBytesDownloaded` e `CloudBytesUploaded` . Per ulteriori informazioni su questo argomento, consulta Prestazioni. 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.	• Sulportalenella scheda Storage Gateway (Storage Gateway), verificare che gli indirizzi IP della VM del gateway corrispondano a quelli visualizzati con il software del client dell'hypervisor (il client VMware vSphere o Microsoft Hyper-V Manager). In caso di mancata corrispondenza, riavviare il gateway dalla console Storage Gateway, come illustrato inSpegnimento della macchina virtuale del gateway. Dopo il riavvio, gli indirizzi nellIndirizzi IPelenco nella console di Storage Gatewayportaledovrebbe corrispondere agli indirizzi IP del gateway, determinati dal client dell'hypervisor.
	  • Per VMware ESXi, l'indirizzo IP della VM si trova nel client vSphere nella scheda Summary (Riepilogo).
	  • Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale.
	• Verificare la connettività del gateway ad AWS come descritto in Test della connettività di rete del gateway.
	• Controllare la configurazione della scheda di rete del gateway per assicurarsi che tutte le interfacce necessarie siano effettivamente abilitate. Per farlo, attenersi alle istruzioni riportate in Configurazione delle schede di rete per il gateway e selezionare l'opzione inerente alla visualizzazione della configurazione di rete del gateway.
	
	Il throughput da e verso il gateway può essere visualizzato dalla console Amazon CloudWatch. Per ulteriori informazioni sulla misurazione del throughput da e verso il gateway con AWS, consulta Prestazioni.

Si sono verificati problemi durante l'importazione (distribuzione) di Storage Gateway su Microsoft Hyper-V.	Consultare Come risolvere i problemi relativi alla 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
Riceverai un messaggio che dice: «I dati scritti sul volume del gateway non sono archiviati in modo sicuro inAWS«.	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, rivolgersiAWS Support.

Abilitazione diAWS Supportper aiutare a risolvere i problemi del gateway ospitato in locale

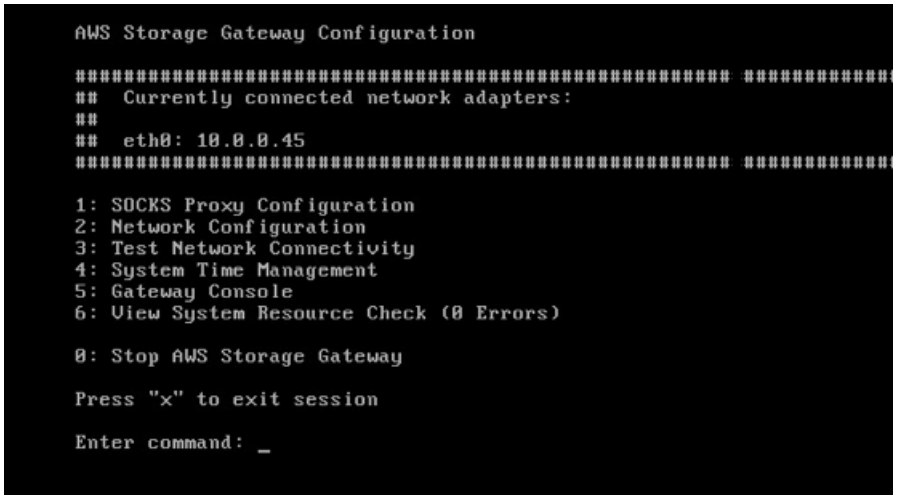
Storage Gateway fornisce una console locale che è possibile utilizzare per eseguire diverse attività di manutenzione, tra cui l'abilitazioneAWS SupportPer accedere al gateway per aiutarti a risolvere i problemi relativi al gateway. Per impostazione predefinita,AWS SupportL'accesso al gateway è disattivato. È possibile abilitare l'accesso tramite la console locale dell'host. Per concedereAWS SupportPer accedere al gateway, occorre prima effettuare l'accesso alla console locale dell'host, poi passare alla console di Storage Gateway e infine connettersi al server di supporto.

Per abilitareAWS Supportaccesso al gateway

1. Accedere alla console locale dell'host.

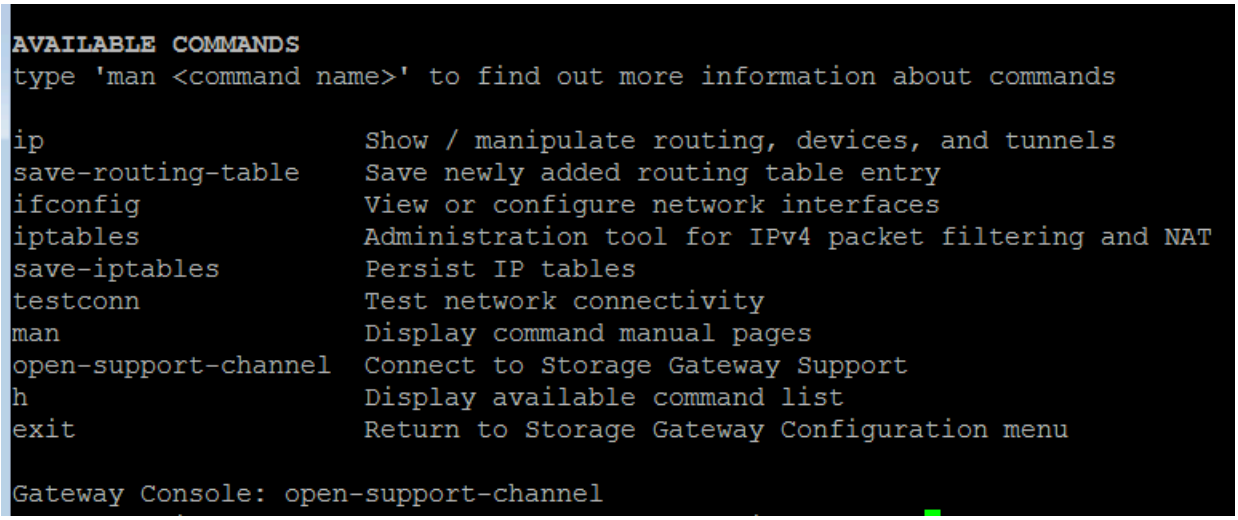
   - VMware ESXi: per ulteriori informazioni, consultaAccesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consultaAccesso alla console locale del gateway con Microsoft Hyper-V.

   La console locale appare come qui di seguito.



2. Al prompt di, inserisci**5**per aprireAWS SupportConsole Channel
3. Immettere **h** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Completa una delle seguenti operazioni:

   - Se il gateway utilizza un endpoint pubblico, nellaCOMANDI DISPONIBILIfinestra, inserisci**`open-support-channel`**per connettersi all'assistenza clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto aAWS. 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, nelCOMANDI DISPONIBILIfinestra, 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 aAWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

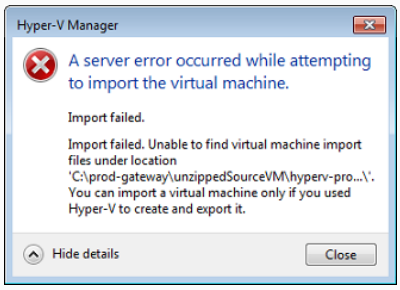
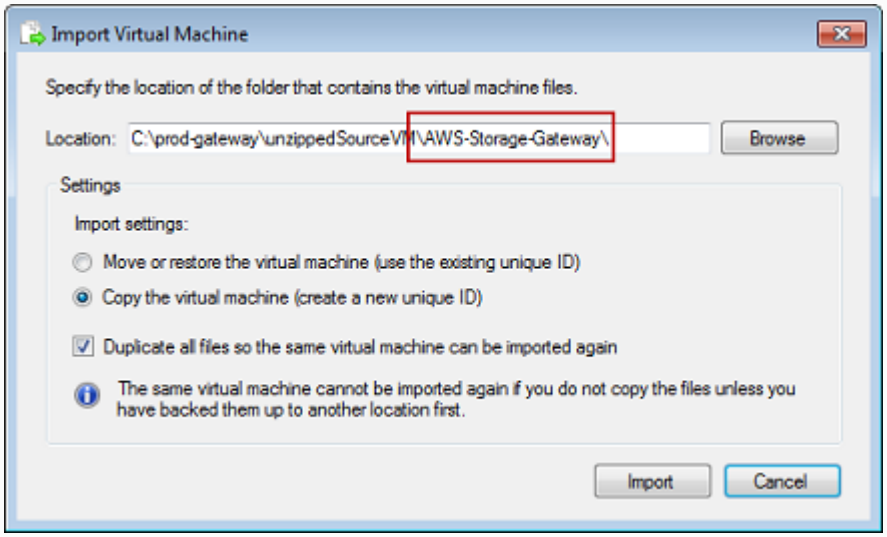


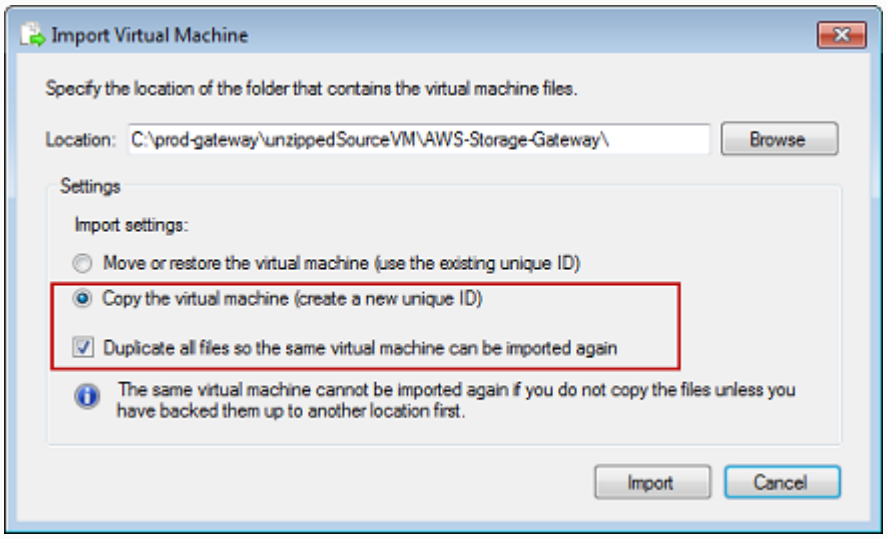
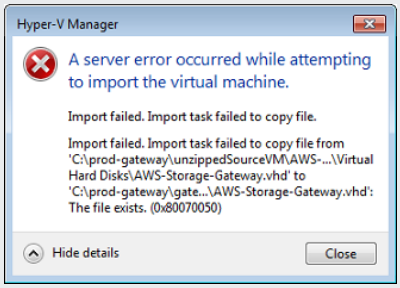
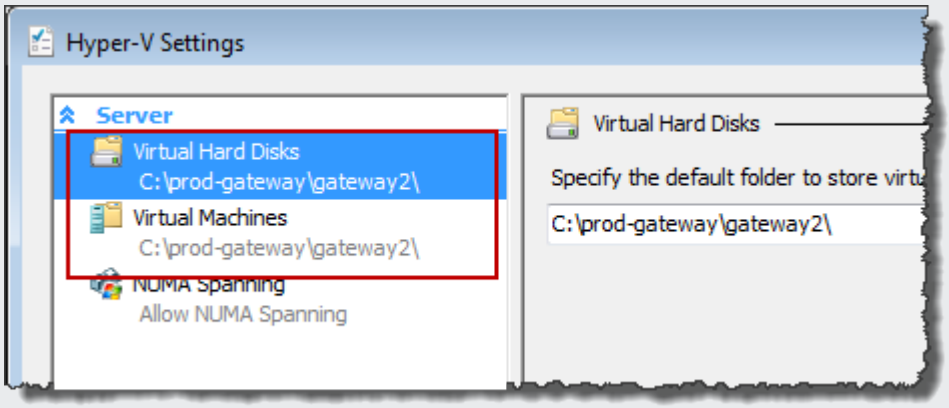
> **Note**
>
> Il numero del canale non è un numero di porta Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server Storage Gateway e su questa mette a disposizione il canale di assistenza.

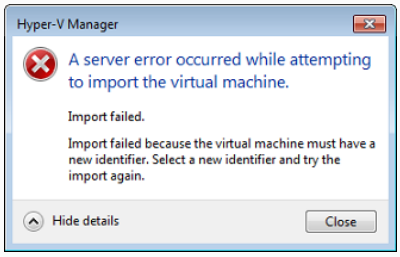
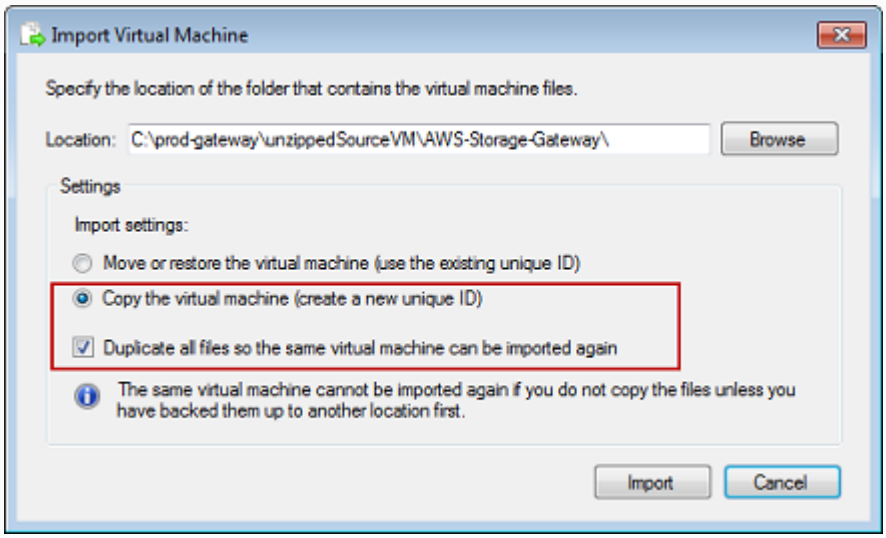
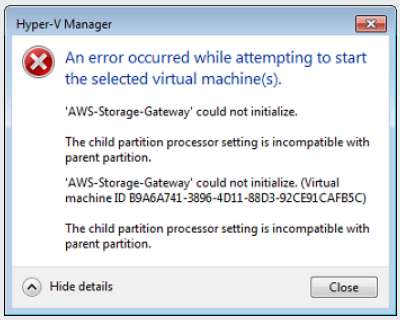
5. Dopo aver stabilito il canale di supporto, comunicare il numero di supporto aAWS SupportcosìAWS Supportpuò fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **q** per terminare. Non chiudere la sessione fino a quando il Support Amazon Web Services non ti avvisa che la sessione di supporto è stata completata.
7. Invio**`exit`**per disconnettersi dalla console Storage Gateway.
8. Seguire le istruzioni per uscire dalla console locale.

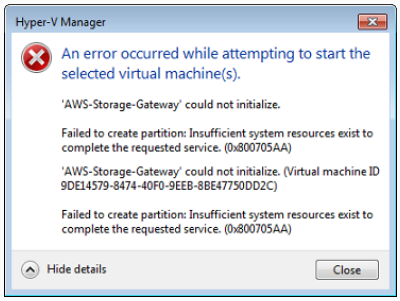
Come risolvere i problemi relativi alla configurazione di Microsoft Hyper-V

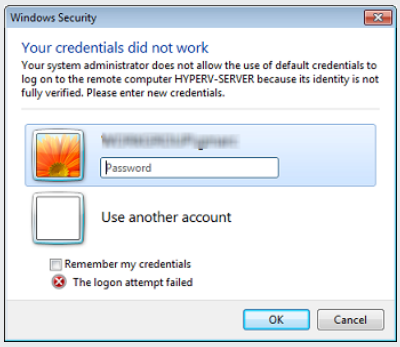
Nella tabella seguente sono elencati i più comuni problemi che potrebbero verificarsi quando si distribuisce Storage Gateway sulla piattaforma Microsoft Hyper-V.

Problema	Operazione da eseguire
Nel tentativo di importare un gateway si riceve il messaggio di errore: «Importazione fallita. Impossibile trovare il file di importazione della macchina virtuale nella sede...". 	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 sede specificata nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale) deve essere `AWS-Storage-Gateway` , come nell'esempio seguente:  • 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 decompressi in una nuova sede, da utilizzare come origine d'importazione. L'esempio seguente mostra le opzioni da selezionare per creare più gateway da un'unica sede di file sorgente decompressi.

Problema	Operazione da eseguire
	
Nel tentativo di importare un gateway si riceve il messaggio di errore: «Importazione fallita. Impossibile copiare file". 	Questo errore si verifica quando, con un gateway già distribuito, 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, bisogna specificare nuove sedi nella finestra di dialogo Hyper-V Settings (Impostazioni di Hyper-V). 

Problema	Operazione da eseguire
Nel tentativo di importare un gateway si riceve un messaggio di errore: «Importazione fallita. Per importare, assegna alla macchina virtuale un nuovo identificatore. Seleziona il nuovo identificatore e riprova." 	Quando si importa il gateway, assicurarsi di 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) per creare un nuovo ID univoco per la VM. L'esempio seguente mostra le opzioni da utilizzare nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale). 
Nel tentativo di avviare una VM del gateway viene visualizzato il messaggio di errore "La configura zione dell'elaboratore di partizione secondario non è compatibile con la partizione principale". 	Questo errore potrebbe essere causato da una discrepanza tra le CPU necessarie per il gateway e quelle disponibili sull'host. Accertarsi che il conteggio di CPU della VM sia supportato dall'hype rvisor sottostante. Per ulteriori informazioni sui requisiti per Storage Gateway, consultaConfigurazione del gateway di file.

Problema	Operazione da eseguire
Tentando di avviare una VM del gateway viene visualizzato il messaggio di errore «Impossibile creare la partizione: Non esistono risorse sufficienti per completare il servizio richiesto.» 	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, consultaConfigurazione del gateway di file.
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, consultare Configurazione di un server NTP (Network Time Protocol) per il gateway.
È necessario inserire i file decompressi di Storage Gateway 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.

Problema	Operazione da eseguire
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.

Risoluzione dei 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 locale e uno distribuito in Amazon EC2, consultaDistribuzione di un gateway di file su un host Amazon EC2.

Per informazioni sull'utilizzo dello storage temporaneo, consulta Utilizzo di storage effimero con gateway EC2.

Argomenti

- L'attivazione del gateway non si è verificata dopo pochi istanti
- Non è possibile trovare l'istanza del gateway EC2 nell'elenco delle istanze
- VuoiAWS Supportper aiutare a risolvere i problemi del gateway EC2

L'attivazione del gateway non si è verificata dopo pochi istanti

Controlla quanto segue nella console Amazon EC2:

- La porta 80 è abilitata nel gruppo di sicurezza associato all'istanza. Per ulteriori informazioni sull'aggiunta di una regola del gruppo di sicurezza, consultaAggiunta di una regola del gruppo di sicurezzanellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

- L'istanza del gateway è contrassegnata come in esecuzione. Nella console Amazon EC2StatoIl valore dell'istanza dovrebbe essere RUNNING.
- Il tipo di istanza Amazon EC2 soddisfa i requisiti minimi, come descritto inRequisiti di storage.

Dopo aver risolto il problema, provare di nuovo ad attivare il gateway. Per fare ciò, aprire la console Storage Gateway, scegliereDistribuzione di un nuovo gateway su Amazon EC2e immettere nuovamente l'indirizzo IP dell'istanza.

Non è possibile trovare l'istanza del gateway EC2 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. Un'istanza basata sull'AMI di Storage Gateway di 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.

VuoiAWS Supportper aiutare a risolvere i problemi del gateway EC2

Storage Gateway fornisce una console locale che è possibile utilizzare per eseguire diverse attività di manutenzione, tra cui l'abilitazioneAWS SupportPer accedere al gateway per aiutarti a risolvere i problemi relativi al gateway. Per impostazione predefinita,AWS SupportL'accesso al gateway è disattivato. È possibile abilitare l'accesso tramite la console locale 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 a un gruppo di sicurezza, consultaGruppi di sicurezza Amazon EC2nellaGuida per l'utente di Amazon EC2.

Per lasciareAWS SupportPer connettersi al gateway, occorre prima effettuare l'accesso alla console locale dell'istanza Amazon EC2, poi navigare fino alla console di Storage Gateway e infine fornire l'accesso.

Per abilitareAWS Supportaccesso a un gateway distribuito su un'istanza Amazon EC2

1. Accedere alla console locale dell'istanza Amazon EC2. Per istruzioni, vai suConnessione all'istanzanellaGuida 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**
   >
   > La*CHIAVE PRIVATA*è il`.pem`file contenente il certificato privato della key pair EC2 utilizzata per avviare l'istanza Amazon EC2. Per ulteriori informazioni, consultaRecupero della chiave pubblica per la coppia di chiavinellaGuida per l'utente di Amazon EC2. La*NOME-PUBLIC-DNS-NAME*è il nome pubblico del Domain Name System (DNS) dell'istanza Amazon EC2 su cui è in esecuzione il gateway. È possibile ottenere questo nome DNS pubblico selezionando l'istanza Amazon EC2 nella console EC2 e facendo clic suDescription (Descrizione)scheda.

2. Al prompt di, inserisci**`6 - Command Prompt`**per aprireAWS SupportConsole Channel
3. Immettere **h** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Completa una delle seguenti operazioni:

   - Se il gateway utilizza un endpoint pubblico, nellaCOMANDI DISPONIBILIfinestra, inserisci**`open-support-channel`**per connettersi all'assistenza clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto aAWS. 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, nelCOMANDI DISPONIBILIfinestra, 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 aAWS. 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 Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server Storage Gateway e su questa mette a disposizione il canale di assistenza.

5. Dopo aver stabilito il canale di supporto, comunicare il numero di supporto aAWS SupportcosìAWS Supportpuò fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **q** per terminare. Non chiudere la sessione fino a quando il Support Amazon Web Services non ti avvisa che la sessione di supporto è stata completata.
7. Invio**exit**per uscire dalla console Storage Gateway.
8. Seguire i menu della console per uscire dall'istanza Storage Gateway.

Come risolvere i problemi di hardware

I seguenti argomenti illustrano i problemi che possono verificarsi con Storage Gateway Hardware Appliance e i suggerimenti per risolverli.

Non è possibile 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 reimpostare l'appliance ai valori di fabbrica, contattare il team di Storage Gateway Hardware Appliance per Support, come descritto nella sezione seguente.

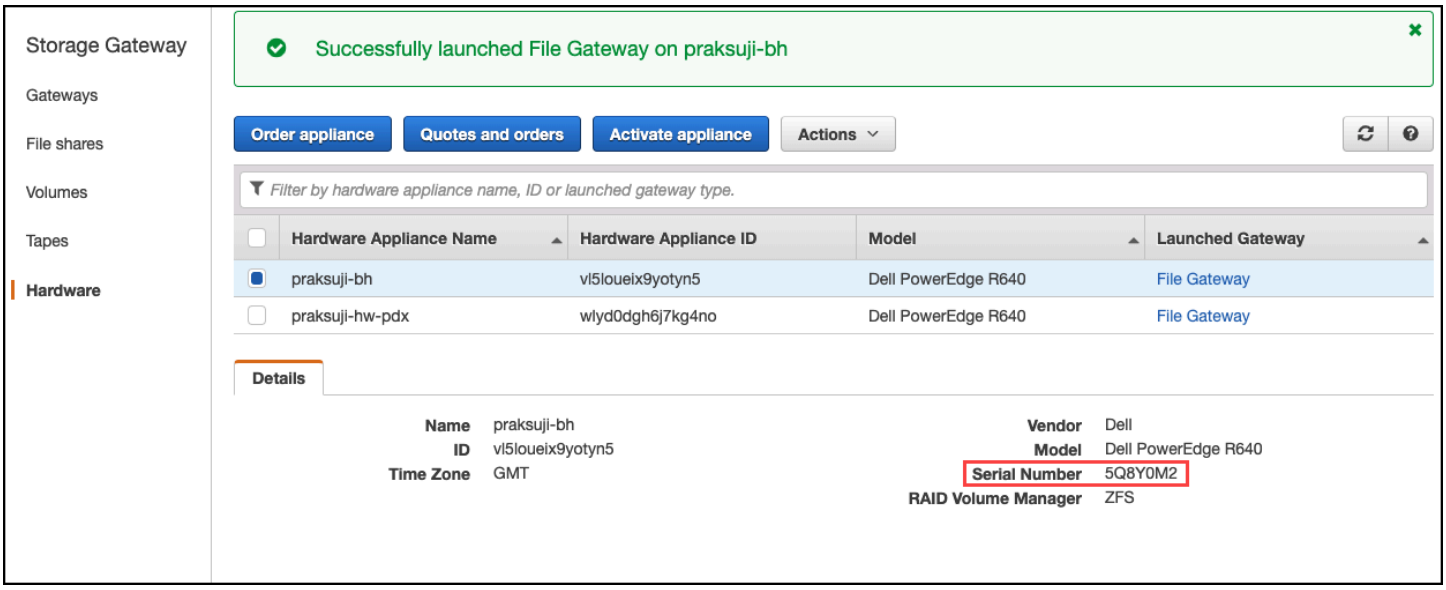
Dove si ottiene il supporto Dell iDRAC?

Il server Dell PowerEdge R640 viene fornito con l'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, consultaDell PowerEdge: qual è il nome utente e la password predefiniti per iDRAC?.
- Assicurarsi che il firmware sia aggiornato per evitare intrusioni.
- Spostare l'interfaccia di rete iDRAC su una porta normale (`em`) può causare problemi di prestazioni o prevenire il normale funzionamento dell'appliance.

Non è possibile trovare il numero di serie dell'appliance hardware

Per trovare il numero di serie dell'appliance hardware, andare allaHardwarenella console Storage Gateway, come illustrato di seguito.



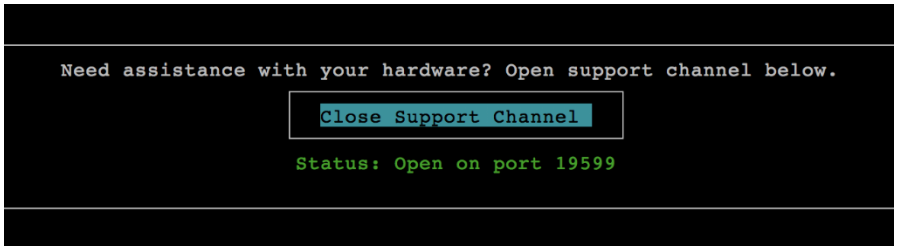
Dove ottenere il supporto per dispositivi hardware

Per contattare il supporto di Storage Gateway Hardware Appliance, vedereAWS Support.

LaAWS SupportIl team potrebbe richiedere di attivare il canale di supporto per risolvere i problemi del gateway in 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 perAWS

1. Aprire la console hardware.
2. Scegliere Open Support Channel (Apri canale di supporto) come mostrato di seguito.



   Il numero di porta assegnato dovrebbe essere visualizzato entro 30 secondi, se non ci sono problemi di connettività di rete o di firewall.
3. Annotare il numero di porta e fornireAWS Support.

Come risolvere i problemi del gateway di file

Puoi configurare il gateway file con un gruppo di log Amazon CloudWatch quando esegui VMware vSphere High Availability (HA). In tal caso, vengono visualizzate le notifiche sullo stato di integrità del gateway file e sugli errori rilevati dal gateway file. Le informazioni su queste notifiche di errore e di integrità sono disponibili 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

- Risoluzione dei problemi con le metriche di CloudWatch

Errore: InaccessibleStorageClass

È possibile ottenere un`InaccessibleStorageClass`Errore durante il trasferimento di un oggetto dalla classe di storage Amazon S3 Standard.

Di solito il gateway di file rileva l'errore quando tenta di caricare l'oggetto specificato nel bucket S3 o di leggere l'oggetto dal bucket S3. Con questo errore, generalmente l'oggetto si è trasferito in Amazon S3 Glacier ed è nella classe di storage S3 Glacier e S3 Glacier Deep Archive.

Per risolvere un errore InaccessibleStorageClass

- Spostare l'oggetto dalla classe di storage S3 Glacier o S3 Glacier Deep Archive in S3.

  Se sposti l'oggetto nel bucket S3 per correggere un errore di caricamento, il file viene caricato. Se sposti l'oggetto nel bucket S3 per correggere un errore di lettura, il client SMB o NFS del gateway di file può leggere il file.

Errore: Accesso S3 negato

È possibile ottenere un`S3AccessDenied`errore per l'accesso al bucket Amazon S3 di una condivisione di fileAWS Identity and Access Management(IAM) ruolo. In questo caso, il bucket S3 accede al ruolo IAM specificato da`roleArn`nell'errore non consente l'operazione in questione. L'operazione non è consentita a causa delle autorizzazioni per gli oggetti nella directory specificata dal prefisso Amazon S3.

Per risolvere un errore S3AccessDenied

- Modifica della policy di accesso ad Amazon S3 a`roleArn`nel log dello stato del gateway di file per consentire le autorizzazioni per l'operazione Amazon S3. Assicurati che la policy di accesso consenta l'autorizzazione per l'operazione che ha causato l'errore. Inoltre, consenti l'autorizzazione per la directory specificata nel registro per `prefix`. Per informazioni sulle autorizzazioni di Amazon S3, consultaSpecificare le autorizzazioni in una policynelGuida per l'utente Amazon Simple Storage Service.

  Queste operazioni possono causare un errore `S3AccessDenied`.

  - `S3HeadObject`

- `S3GetObject`
- `S3ListObjects`
- `S3DeleteObject`
- `S3PutObject`

Errore: InvalidObjectState invalidi

È possibile ottenere un`InvalidObjectState`errore quando un writer diverso dal gateway file specificato modifica il file specificato nel bucket S3 indicato. Di conseguenza, lo stato del file per il gateway file non corrisponde al suo stato in Amazon S3. I caricamenti successivi del file in Amazon S3 o i recuperi del file da Amazon S3 non vanno a buon fine.

Per risolvere un errore InvalidObjectState

Se l'operazione che modifica il file è`S3Upload`o`S3GetObject`, eseguire le seguenti operazioni:

1. Salvare la copia più recente del file nel file system locale del client SMB o NFS (è necessaria questa copia file nella fase 4). Se la versione del file in Amazon S3 è la più recente, scaricare tale versione. A tale scopo, è possibile utilizzare la AWS Management Console o l'AWS CLI.
2. Eliminare il file in Amazon S3 utilizzando ilAWS Management ConsoleoAWS CLI.
3. Eliminare il file dal gateway di file utilizzando il client SMB o NFS.
4. Copia la versione più recente del file salvato nella fase 1 in Amazon S3 utilizzando il client SMB o NFS. Eseguire questa operazione tramite il gateway di file.

Errore: ObjectMissing

È possibile ottenere un`ObjectMissing`errore quando un writer diverso dal gateway file specificato elimina il file specificato dal bucket S3. Eventuali caricamenti successivi in Amazon S3 o recuperi da Amazon S3 per l'oggetto non vanno a buon fine.

Per risolvere un errore ObjectMissing

Se l'operazione che modifica il file è`S3Upload`o`S3GetObject`, eseguire le seguenti operazioni:

1. Salvare la copia più recente del file nel file system locale del client SMB o NFS (è necessaria questa copia file nella fase 3).

2. Eliminare il file dal gateway di file utilizzando il client SMB o NFS.
3. Copiare la versione più recente del file salvato nella fase 1 utilizzando il client SMB o NFS. Eseguire questa operazione tramite il gateway di file.

: Notification Riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console VM Hypervisor Management (Gestione hypervisor VM) o la console Storage Gateway (Storage 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.

: Notification 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 gateway VMware, un ripristino da parte di vSphere High Availability Application Monitoring può attivare questo evento.

Quando il gateway viene eseguito in questo ambiente, verifica la presenza della notifica `HealthCheckFailure` e consulta il log degli eventi VMware per la macchina virtuale.

: Notification HealthCheckFailure

Per un gateway su VMware vSphere HA, puoi ricevere una notifica `HealthCheckFailure` quando un controllo dello stato non riesce e viene richiesto un 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 solo per i gateway VMware.

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, contattaAWS Support.

: Notification AvailabilityMonitorTest

Si ottiene un`AvailabilityMonitorTest`notifica quando tueseguire un testdelControllo della disponibilità e delle applicazionisistema su gateway in esecuzione su una piattaforma VMware vSphere HA.

Errore: RoleTrustRelationshipInvalid

Questo errore viene visualizzato quando il ruolo IAM per una condivisione di file ha una relazione di trust IAM configurata in modo errato (ovvero, il ruolo IAM non considera attendibile l'principal Storage Gateway denominato con il nome di Storage Gateway denominato`storagegateway.amazonaws.com`). Di conseguenza, il gateway file non sarebbe in grado di ottenere le credenziali per eseguire le operazione sul bucket S3 che supporta la condivisione file.

Per risolvere un errore RoleTrustRelationshipInvalid

- Utilizzare la console IAM o l'API IAM per include`storagegateway.amazonaws.com`come principal attendibile da IAMRole della condivisione file. Per ulteriori informazioni sul ruolo IAM, consultaEsercitazione: delega l'accesso attraversoAWSaccount che utilizzano i ruoli IAM.

Risoluzione dei problemi con le metriche di CloudWatch

Di seguito è spiegato cosa fare per risolvere i problemi nell'utilizzo dei parametri Amazon CloudWatch con Storage Gateway.

Argomenti

- Il gateway reagisce lentamente durante la navigazione delle directory
- Il tuo gateway non risponde
- Il gateway è lento durante il trasferimento dei dati ad Amazon S3
- Il gateway sta eseguendo più operazioni Amazon S3 del previsto
- Non vengono visualizzati i file nel bucket Amazon S3
- Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway

Il gateway reagisce lentamente durante la navigazione delle directory

Se il gateway di file reagisce lentamente quando esegui il filelscomando o sfoglia directory, controlla il`IndexFetch`e`IndexEviction`Parametri di CloudWatch

- Se il file`IndexFetch`la metrica è maggiore di 0 quando si esegue un`ls`comando o esplori le directory, il gateway è stato avviato senza informazioni sul contenuto della directory interessata e ha dovuto accedere ad Amazon S3. Gli sforzi successivi per elencare i contenuti di tale directory dovrebbero avvenire più velocemente.
- Se il file`IndexEviction`il parametro è maggiore di 0, significa che il gateway di file ha raggiunto il limite di ciò che può gestire nella cache in quel momento. In questo caso, il gateway di file deve liberare spazio di storage dalla directory a cui ha avuto accesso meno di recente per elencare una nuova directory. Se ciò si verifica frequentemente e si riscontra un impatto sulle prestazioni, contattareAWS Support.

  Discutere conAWS Supportil contenuto del bucket S3 correlato e le raccomandazioni per migliorare le prestazioni in base al caso d'uso.

Il tuo gateway non risponde

Se il gateway di file non risponde, procedi come segue:

- Se di recente è stato eseguito un riavvio o aggiornamento software, controlla il parametro `IOWaitPercent`. Questo parametro mostra la percentuale di tempo in cui la CPU è inattiva quando è presente una richiesta di I/O su disco in sospeso. 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, il gateway file potrebbe essere rallentato da un disco root lento mentre ricostruisce la cache dell'indice nella RAM. Puoi risolvere questo problema utilizzando un disco fisico più veloce per il disco root.
- Se il file`MemUsedBytes`metrica è uguale o quasi uguale alla`MemTotalBytes`parametro, quindi il gateway di file sta esaurendo la RAM disponibile. Verificare che il gateway di file disponga almeno della RAM minima richiesta. In tal caso, considera l'aggiunta di più RAM al gateway file 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 sono presenti molti client connessi, potrebbe essere necessario aggiungere più RAM al gateway file.

Il gateway è lento durante il trasferimento dei dati ad Amazon S3

Se il gateway di file è lento durante il trasferimento dei dati ad Amazon S3, procedi come segue:

- Se il file`CachePercentDirty`La metrica è pari o superiore a 80, il gateway file scrive i dati su disco più velocemente di quanti ne possa caricare in Amazon S3. Prendi in considerazione l'aumento della larghezza di banda per il caricamento dal gateway, l'aggiunta di uno o più dischi della cache o il rallentamento delle scritture client.
- Se il file`CachePercentDirty`la metrica è bassa, controlla il`IoWaitPercent`Parametri di Se`IoWaitPercent`è maggiore di 10, il gateway file potrebbe essere rallentato dalla velocità del disco della 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.
- Se`S3PutObjectRequestTime`,`S3UploadPartRequestTime`, oppure`S3GetObjectRequestTime`sono alti, potrebbe esserci un collo di bottiglia di rete. Prova ad analizzare la tua rete per verificare che il gateway abbia la larghezza di banda prevista.

Il gateway sta eseguendo più operazioni Amazon S3 del previsto

Se il gateway di file sta eseguendo più operazioni Amazon S3 del previsto, controlla il`FilesRenamed`Parametri di Le operazioni di rinominazione sono costose da eseguire in Amazon S3. Ottimizza il flusso di lavoro per ridurre al minimo il numero di operazioni di rinominazione.

Non vengono visualizzati i file nel bucket Amazon S3

Se noti che i file nel gateway non si riflettono nel bucket Amazon S3, controllarne la`FilesFailingUpload`Parametri di Se la metrica segnala che alcuni file non sono stati caricati, controlla le notifiche dello stato. Quando i file non vengono caricati, il gateway genera una notifica di integrità contenente ulteriori dettagli sul problema.

Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway

Se il processo di backup del gateway file non riesce o si verificano errori durante la scrittura nel gateway file, effettuare le operazioni seguenti:

- Se il file`CachePercentDirty`Il parametro è pari o superiore al 90%, il gateway file non può accettare nuove scritture su disco perché non è disponibile spazio sufficiente sul disco della cache.

Per verificare la velocità di caricamento del gateway di file su Amazon FSx o Amazon S3, consulta la`CloudBytesUploaded`Parametri di Confronta quella metrica con la`WriteBytes`parametro, che mostra la velocità con cui il client sta scrivendo file nel gateway di file. Se il gateway file scrive più velocemente di quanto possa caricare in Amazon FSx o Amazon S3, aggiungi più dischi della cache per coprire almeno la dimensione del processo di backup. In alternativa, aumenta la larghezza di banda di caricamento.

- Se un processo di backup fallisce ma il`CachePercentDirty`La metrica è inferiore all'80%, il gateway file potrebbe causare un timeout della sessione lato client. Per SMB, puoi aumentare questo timeout utilizzando il comando PowerShell `Set-SmbClientConfiguration -SessionTimeout 300`. L'esecuzione di questo comando imposta il timeout su 300 secondi.

  Per NFS, assicurati che il client sia montato utilizzando un hard mount anziché un soft mount.

Come risolvere i problemi relativi alla condivisione file

Di seguito è spiegato cosa fare se si verificano problemi imprevisti nella condivisione file.

Argomenti

La condivisione di file è bloccata nello stato CREATING

Non appena la configuri, alla condivisione file viene assegnato lo stato CREATING (CREAZIONE IN CORSO) che diventa AVAILABLE (DISPONIBILE) solo al termine della creazione. Se la condivisione file si blocca allo stato CREATING (CREAZIONE IN CORSO), occorre procedere come segue:

1. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Verificare che il bucket S3 su cui è mappata la condivisione file esista. In caso contrario, crearlo. Una volta creato il bucket, lo stato della condivisione file passa a AVAILABLE (DISPONIBILE). Per informazioni su come creare un bucket S3, consultaCreazione di un bucketnellaGuida dell'utente di Amazon Simple Storage.
3. Verificare che il nome del bucket rispetti le regole di denominazione di Amazon S3. Per ulteriori informazioni, consulta le Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.
4. Verificare che il ruolo IAM utilizzato per accedere al bucket S3 disponga delle autorizzazioni corrette e che il bucket S3 sia elencato tra le risorse nella policy IAM. Per ulteriori informazioni, consultare Concessione dell'accesso a un bucket Amazon S3.

Non è possibile creare una condivisione file

1. Se non riesci a creare una condivisione file perché si blocca allo stato CREATING (CREAZIONE IN CORSO), verifica innanzitutto che il bucket S3 su cui l'hai mappata esista. Per informazioni su come fare, consulta il paragrafo precedente, La condivisione di file è bloccata nello stato CREATING.
2. Se il bucket S3 esiste, verificare cheAWS Security Token Serviceè abilitato nella regione in cui vuoi creare la condivisione file. Qualora non fosse già attivo, occorrerà abilitare il token di sicurezza. Per informazioni su come abilitare un token utilizzandoAWS Security Token Service, consultaAttivazione e disattivazioneAWSSTS inAWSRegionnellaIAM User Guide.

Le condivisioni file SMB non consentono più metodi di accesso diversi

Le condivisioni di file SMB hanno le seguenti restrizioni:

1. Quando lo stesso client tenta di montare sia una condivisione file Active Directory che una condivisione SMB con accesso guest viene visualizzato il seguente messaggio di errore: `Multiple connections to a server or shared resource by the same user,`

```
using more than one user name, are not allowed. Disconnect all previous
connections to the server or shared resource and try again.
```

2. Un utente di Windows non può essere connesso a due condivisioni di file SMB con accesso guest e potrebbe essere disconnesso quando viene stabilita una nuova connessione con accesso guest.
3. Un client di Windows non è in grado di montare insieme una condivisione file Active Directory e una condivisione SMB con accesso guest esportate dallo stesso gateway.

Le condivisioni di file multiple non possono scrivere sul bucket S3 mappato

Non è consigliabile configurare il bucket S3 in modo da permettervi la scrittura da parte di più condivisioni file. Tale approccio, infatti, è in grado di determinare risultati imprevisti.

Al contrario, è bene consentire a un'unica condivisione file di scrivere su ciascun bucket S3. Per permettere al solo ruolo associato alla tua condivisione file di scrivere sul bucket, puoi creare una policy del bucket. Per ulteriori informazioni, consultare Best practice per la condivisione file.

Impossibile caricare file nel bucket S3

Se non si riesce a caricare file nel bucket S3, occorre procedere come segue:

1. Verificare di aver concesso le autorizzazioni di accesso necessarie affinché Amazon S3 File Gateway carichi file nel bucket S3. Per ulteriori informazioni, consultare Concessione dell'accesso a un bucket Amazon S3.
2. Verificare che il ruolo che ha creato il bucket sia autorizzato a scrivere nel bucket S3. Per ulteriori informazioni, consultare Best practice per la condivisione file.
3. Se il gateway di file utilizza SSE-KMS per la crittografia, assicurarsi che il ruolo IAM associato alla condivisione di file includakms:Encrypt,kms:Decrypt,KMS: ricrittografa,kms:GenerateDataKey, ekms:DescribeKeyautorizzazioni. Per ulteriori informazioni, consultaUtilizzo di policy basate su identità (Policy IAM) per Storage Gateway.

Impossibile modificare la crittografia predefinita per utilizzare SSE-KMS per crittografare gli oggetti memorizzati nel bucket S3

Se si modifica la crittografia predefinita e si crea la crittografia SSE-KMS (lato server conAWS KMS —managed keys) il valore predefinito per il bucket S3, gli oggetti memorizzati da Amazon S3 File Gateway nel bucket non sono crittografati con SSE-KMS. Per impostazione predefinita, un Gateway

file S3 utilizza la crittografia lato server gestita con Amazon S3 (SSE-S3) quando scrive dati in un bucket S3. Modificare l'impostazione predefinita non modificherà automaticamente la crittografia.

Per modificare la crittografia in modo da utilizzare SSE-KMS con la chiave AWS KMS, è necessario abilitare la crittografia SSE-KMS. A tale scopo, ti basta fornire l'Amazon Resource Name (ARN) della chiave KMS quando crei la condivisione file. Puoi anche aggiornare le impostazioni KMS per la condivisione file utilizzando l'operazione API `UpdateNFSFileShare` o `UpdateSMBFileShare`. Questo aggiornamento si applica agli oggetti archiviati nei bucket S3 dopo l'aggiornamento. Per ulteriori informazioni, consultare Crittografia dati utilizzandoAWS KMS.

Le modifiche apportate direttamente in un bucket S3 con il controllo delle versioni degli oggetti abilitato possono influire su ciò che vedi nella condivisione di file

Quando il bucket S3 include oggetti scritti da client alternativi, la sua visualizzazione potrebbe non essere aggiornata a causa della funzione Versioni multiple degli oggetti di un bucket S3. Prima di esaminare i file d'interesse, occorre aggiornare la cache.

La funzione Versioni multiple degli oggetti è una funzione facoltativa dei bucket S3 che consente di preservare i dati memorizzando più copie di un oggetto con lo stesso nome. Ad esempio, ad esempio, ogni copia ha un valore ID separato`file1.jpg`:`ID="xxx"`e`file1.jpg`: `ID="yyy"`. Il numero degli oggetti con lo stesso nome e la loro durata sono regolati dalle policy per il ciclo di vita di Amazon S3. Per ulteriori informazioni su questi concetti di Amazon S3, consultaUso della funzione Versioni multipleeGestione del ciclo di vita degli oggettinellaGuida per gli sviluppatori Amazon S3.

Un oggetto con versione eliminato acquisisce il contrassegno di eliminazione, ma viene conservato. Solo il proprietario del bucket S3 può eliminare definitivamente un oggetto con la funzione Versioni multiple attiva.

I file mostrati nel gateway S3 sono le versioni più recenti degli oggetti in un bucket S3 al momento del recupero o dell'aggiornamento della cache. Il gateway file S3 ignora le versioni obsolete o eventuali oggetti contrassegnati per l'eliminazione. Quando si legge un file, vengono visualizzati i dati della versione più recente. Quando si scrive un file nella condivisione, il gateway file S3 crea una nuova versione dell'oggetto specificato con le modifiche, che diviene la versione più recente.

Nel caso in cui al bucket S3 venisse aggiunta una nuova versione al di fuori della propria applicazione, il gateway file S3 continuerebbe a leggere dalla versione precedente, sulla quale, inoltre, proseguirebbero a basarsi gli aggiornamenti apportati. Per leggere la versione più recente

di un oggetto, utilizzare l'operazione API Aggiorna cache o eseguire l'aggiornamento dalla console come descritto in Aggiornamento di oggetti nel bucket Amazon S3.

> **Important**
>
> Non è consigliabile scrivere oggetti o file nel bucket S3 File Gateway S3 dall'esterno della condivisione file.

Quando si scrive su un bucket S3 con il controllo delle versioni degli oggetti abilitato, Amazon S3 File Gateway può creare più versioni di un oggetto S3

Con il controllo delle versioni degli oggetti abilitato, potresti avere più versioni di un oggetto create in Amazon S3 per ogni aggiornamento di un file dal tuo client NFS o SMB. Di seguito sono riportati gli scenari che possono comportare la creazione di più versioni di un oggetto nel bucket S3:

- Quando un file viene modificato in Amazon S3 File Gateway da un client NFS o SMB dopo che è stato caricato su Amazon S3, S3 File Gateway carica i dati nuovi o modificati invece di caricare l'intero file. La modifica del file comporta la creazione di una nuova versione dell'oggetto Amazon S3.
- Quando un file viene scritto su S3 File Gateway da un client NFS o SMB, il Gateway file S3 carica i dati del file su Amazon S3 seguito dai relativi metadati (proprietà, timestamp, ecc.). Il caricamento dei dati del file crea un oggetto Amazon S3 e il caricamento dei metadati per il file aggiorna i metadati per l'oggetto Amazon S3. Questo processo crea un'altra versione dell'oggetto, risultando in due versioni di un oggetto.
- Quando S3 File Gateway sta caricando file più grandi, potrebbe essere necessario caricare pezzi più piccoli del file prima che il client abbia finito di scrivere sul gateway di file. Alcuni motivi per questo includono la liberazione di spazio nella cache o un elevato tasso di scritture su un file. Ciò può risultare in più versioni di un oggetto nel bucket S3.

È necessario monitorare il bucket S3 per determinare quante versioni di un oggetto esistono prima di impostare i criteri del ciclo di vita per spostare gli oggetti in classi di storage diverse. È necessario configurare la scadenza del ciclo di vita per le versioni precedenti per ridurre al minimo il numero di versioni disponibili per un oggetto nel bucket S3. L'uso della replica della stessa regione (SRR) o della replica Cross-Region (CRR) tra i bucket S3 aumenterà lo storage utilizzato. Per ulteriori informazioni sulla replica, consultaReplica.

> **Important**
>
> Non configurare la replica tra bucket S3 finché non si capisce quanto spazio di archiviazione viene utilizzato quando è abilitato il controllo delle versioni degli oggetti.

Avvalendosi dei bucket S3 con le versioni, si aumenta molto più spazio di storage in Amazon S3, poiché per ogni modifica a un file viene creata una nuova versione dell'oggetto S3. Per impostazione predefinita, Amazon S3 continua ad archiviare tutte le versioni, a meno che non si crei una policy specifica per ignorare questo comportamento e limitare il numero di versioni conservate. Se noti un utilizzo insolitamente ampio dello spazio di storage con la funzione Versioni multiple degli oggetti attiva, verifica che le policy di storage siano impostate appropriatamente. L'utilizzo della funzione Versioni multiple degli oggetti può provocare, inoltre, l'incremento del numero di risposte `HTTP 503-slow down` alle richieste del browser.

Se si abilita il controllo delle versioni degli oggetti dopo l'installazione di un gateway file S3, tutti gli oggetti univoci vengono conservati (`ID=″NULL″`) e puoi vederli tutti nel file system. Alle nuove versioni degli oggetti viene assegnato un ID univoco (le versioni precedenti vengono comunque conservate). Nel file system NFS viene visualizzata solo l'ultima versione dell'oggetto in base al suo time stamp.

Una volta abilitata la funzione Versioni multiple degli oggetti, non è possibile riportare il bucket S3 nello stato senza versione. Tuttavia, si può sospendere la funzione. In seguito alla sospensione, a un nuovo oggetto viene assegnato un ID. In presenza di un oggetto con lo stesso nome e un valore `ID=″NULL″`, la versione meno recente viene sovrascritta. Eventuali versioni contenenti un ID diverso da `NULL`, tuttavia, restano disponibili. I time stamp identificano il nuovo oggetto come quello attuale, nonché l'unico da visualizzare nel file system NFS.

Le modifiche apportate a un bucket S3 non si riflettono in Storage Gateway

Storage Gateway aggiorna automaticamente la cache di condivisione file quando si scrivono file nella cache localmente utilizzando la condivisione file. Tuttavia, Storage Gateway non aggiorna automaticamente la cache quando carichi un file direttamente su Amazon S3. Quando lo fai, devi eseguire una`RefreshCache`operazione per vedere le modifiche apportate alla condivisione di file. Se si dispone di più di una condivisione file, è necessario eseguire la`RefreshCache`operazione su ogni condivisione di file.

È possibile aggiornare la cache utilizzando la console Storage Gateway e ilAWS Command Line Interface(AWS CLI):

- Per aggiornare la cache utilizzando la console Storage Gateway, consulta Aggiornamento degli oggetti nel bucket Amazon S3.
- Per aggiornare la cache utilizzando ilAWS CLI:
  1. Eseguire il comandoaws storagegateway list-file-shares
  2. Copia l'Amazon Resource Number (ARN) della condivisione file con la cache che desideri aggiornare.
  3. Eseguirerefresh-cachecomando con il tuo ARN come valore--file-share-arn:

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Per automatizzareRefreshCacheoperazione, vediCome posso automatizzare l'operazione RefreshCache su Storage Gateway?

Le autorizzazioni di ACL non funzionano come previsto

Se le autorizzazioni della lista di controllo accessi (ACL) non funzionano come previsto con la tua condivisione di file SMB, è possibile eseguire un test.

Per eseguire questa operazione, testa prima le autorizzazioni su un server di file di Microsoft Windows o in una condivisione locale di file Windows. Quindi confronta il comportamento con la condivisione di file del gateway.

Le prestazioni del gateway sono diminuite dopo aver eseguito un'operazione ricorsiva

In alcuni casi, è possibile eseguire un'operazione ricorsiva, ad esempio la rinomina di una directory o l'abilitazione dell'ereditarietà per una lista ACL e spingerla in fondo alla struttura. In questo caso, il Gateway file S3 applica ricorsivamente l'operazione a tutti gli oggetti nella condivisione file.

Ad esempio, supponiamo di applicare l'ereditarietà agli oggetti esistenti in un bucket S3. Il gateway file S3 applica ricorsivamente l'ereditarietà a tutti gli oggetti nel bucket. Tali operazioni possono provocare il peggioramento delle prestazioni del gateway.

Notifiche di stato della disponibilità elevata

Quando esegui il gateway sulla piattaforma VMware vSphere High Availability (HA), potresti ricevere le notifiche di stato. Per ulteriori informazioni sulle notifiche sullo stato, consulta Come risolvere i problemi relativi all'elevata disponibilità.

Come risolvere i problemi relativi all'elevata disponibilità

Di seguito sono riportate le informazioni sulle azioni da intraprendere in caso di problemi di disponibilità.

Argomenti

Notifiche di Health

Quando esegui il gateway su VMware vSphere HA, tutti i gateway producono le seguenti notifiche di stato al gruppo di log Amazon CloudWatch configurato. Queste notifiche vengono inserite in un flusso di log chiamato `AvailabilityMonitor`.

Argomenti

: Notification Riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console VM Hypervisor Management (Gestione hypervisor VM) o la console Storage Gateway (Storage 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.

: Notification 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 gateway VMware, un ripristino da parte di vSphere High Availability Application Monitoring può attivare questo evento.

Operazione da eseguire

Quando il gateway viene eseguito in questo ambiente, verifica la presenza della notifica `HealthCheckFailure` e consulta il log degli eventi VMware per la macchina virtuale.

: Notification HealthCheckFailure

Per un gateway su VMware vSphere HA, puoi ricevere una notifica `HealthCheckFailure` quando un controllo dello stato non riesce e viene richiesto un 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 solo per i gateway VMware.

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, contattaAWS Support.

: Notification AvailabilityMonitorTest

Per un gateway su VMware vSphere HA, puoi ottenere un`AvailabilityMonitorTest`notifica quando tueseguire un testdelControllo della disponibilità e delle applicazionisistema in VMware.

Parametri

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. Consulta il gruppo di log CloudWatch configurato per informazioni dettagliate sugli eventi.

Best practice per il recupero 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'AMI (Amazon Machine Image) 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.

Argomenti

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 Test della connettività di rete del gateway.

- Se il gateway non funziona correttamente e si verificano problemi con i volumi o i nastri a causa di un arresto imprevisto, è possibile ripristinare i dati. Per informazioni su come ripristinare i dati, consulta le sezioni seguenti applicabili allo scenario specifico.

Ripristino dei dati da un disco 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.
- Se il disco della cache è danneggiato o non è accessibile, arresta il gateway, reimposta il disco della cache, riconfigura il disco per lo storage della cache e riavvia il gateway.

Per informazioni dettagliate, vedere Ripristino dei dati da un disco cache malfunzionante.

Come ripristinare i 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 ripristinare i dati da un gateway di file in un data center inaccessibile

Per il gateway file, è possibile mappare a una nuova condivisione file nel bucket Amazon S3 che contiene i dati da ripristinare.

1. Creare e attivare un nuovo gateway di file su un host Amazon EC2. Per ulteriori informazioni, consultare Distribuzione di un gateway di file su un host Amazon EC2.
2. Creare una nuova condivisione file nel gateway EC2 creato. Per ulteriori informazioni, consultaCreare una condivisione file.
3. Montare la condivisione file nel client e mapparla al bucket S3 contenente i dati da ripristinare. Per ulteriori informazioni, consultaMonta e usa la condivisione di file.

Risorse Storage Gateway

In questa sezione, puoi trovare informazioni suAWSe software, strumenti e risorse di terze parti che possono essere utili per configurare o gestire il gateway e vengono illustrati i dati di Storage Gateway.

Argomenti

Impostazione dell'host

Argomenti

Configurazione di VMware for Storage Gateway

Nel configurare VMware for Storage Gateway, assicurati di sincronizzare la data e l'ora della macchina virtuale con quelle dell'host, di configurare la macchina virtuale per l'uso di controller dei dischi paravirtualizzati durante l'assegnazione dello storage e di fornire protezione dagli errori nel livello dell'infrastruttura che supporta una macchina virtuale del gateway.

Argomenti

- Utilizzo di Storage Gateway con VMware High Availability

Sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host

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).

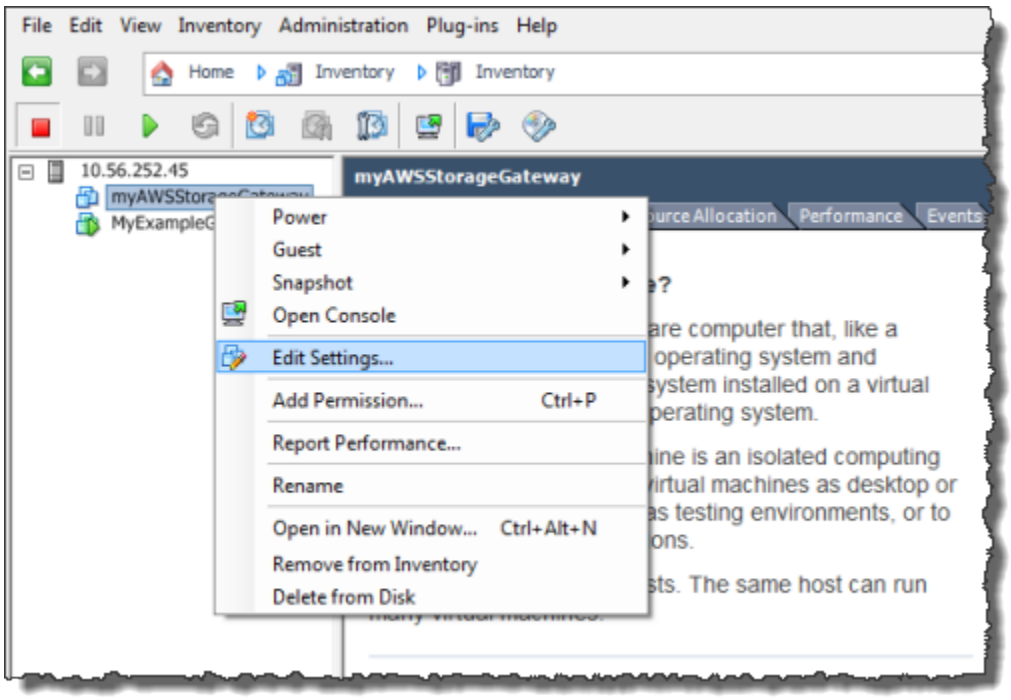
> **Important**
>
> La sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host è necessaria per una corretta attivazione del gateway.

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 aprire il menu contestuale (clic con il pulsante destro del mouse) per la macchina virtuale del gateway e scegliere Edit Settings (Modifica impostazioni).

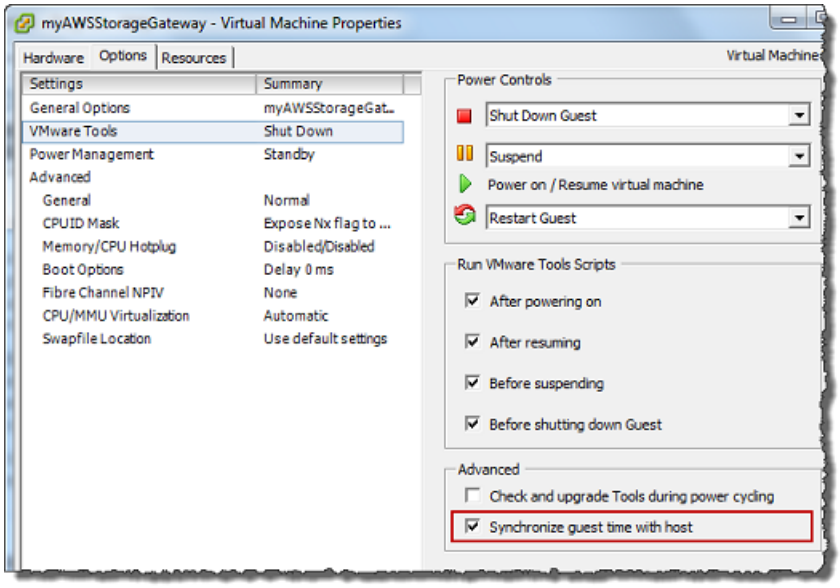
      Viene visualizzata la finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale).



b. Scegliere la scheda Options (Opzioni) e quindi VMware Tools (Strumenti VMware) nell'elenco delle opzioni.

c. Controllare l'opzione Synchronize guest time with host (Sincronizza data e ora guest con host) e quindi scegliere OK.

   La macchina virtuale sincronizza le proprie data e ora con quelle dell'host.



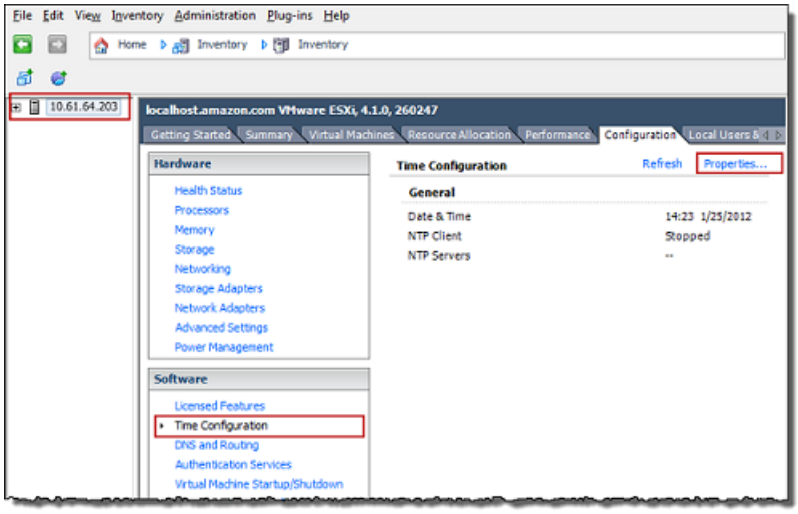
2. Configurare la data e l'ora dell'host.

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.

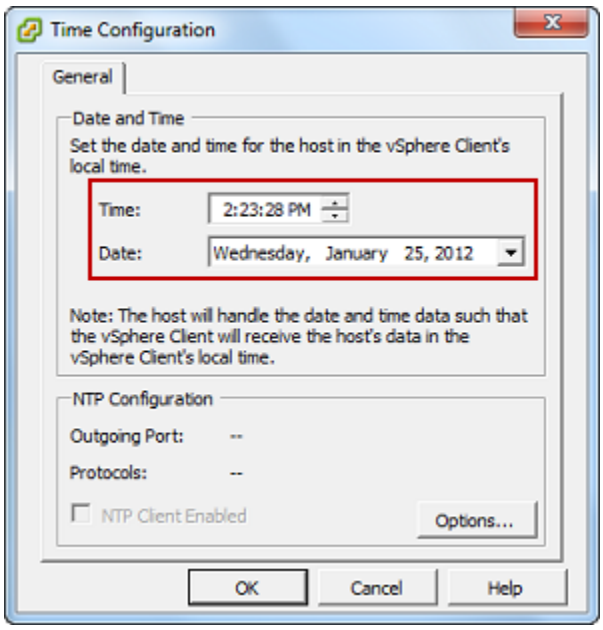
a. Nel client VMware vSphere selezionare il nodo host vSphere nel riquadro a sinistra e quindi scegliere la scheda Configuration (Configurazione).

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).

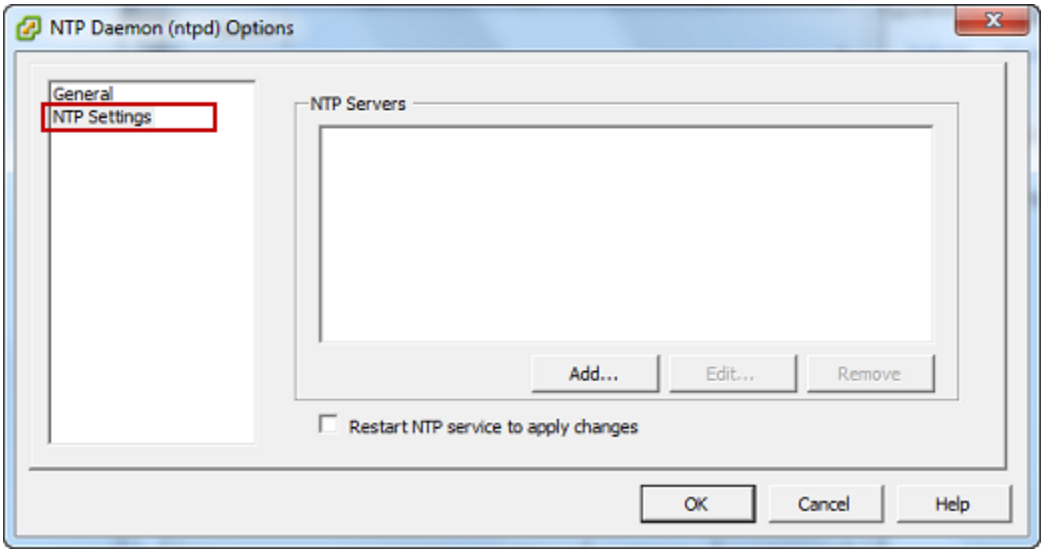


c. Nel pannello Date and Time (Data e ora) impostare la data e l'ora.



d. Configurare l'host per la sincronizzazione automatica di data e ora con un server NTP.

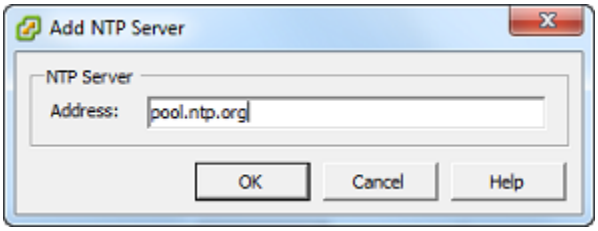
   i. Scegliere Options (Opzioni) nella finestra di dialogo Time Configuration (Configurazione data e ora) e quindi nella finestra di dialogo NTP Daemon (ntpd) (Daemon NTP - ntpd) scegliere NTP Settings (Impostazioni NTP) nel riquadro a sinistra.



   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.

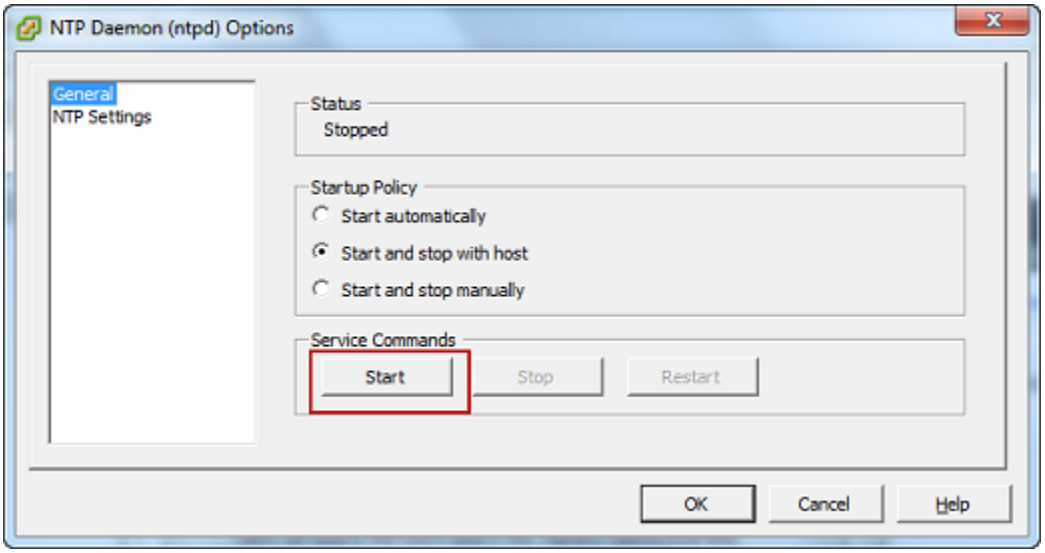
   È possibile usare `pool.ntp.org` come mostrato nell'esempio seguente.



iv. Nella finestra di dialogo NTP Daemon (ntpd) Options (Opzioni daemon NTP - ntpd) scegliere General (Generali) nel riquadro a sinistra.

v. Nel riquadro Service Commands (Comandi servizio) scegliere Start (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).

Utilizzo di Storage Gateway con VMware High Availability

VMware High Availability (HA) è un componente di vSphere che può fornire protezione dagli errori nel livello di infrastruttura che supporta una macchina virtuale gateway. Per fare ciò, VMware HA utilizza più host configurati come cluster, in modo che se un host che esegue una macchina virtuale gateway restituisce un errore, la macchina virtuale gateway può essere riavviata automaticamente su un altro

host all'interno del cluster. Per ulteriori informazioni su VMware HA, consultaVMware HA: Concetti e best practicesul sito Web di VMware.

Per usare Storage Gateway con VMware HA, ti consigliamo di svolgere queste operazioni:

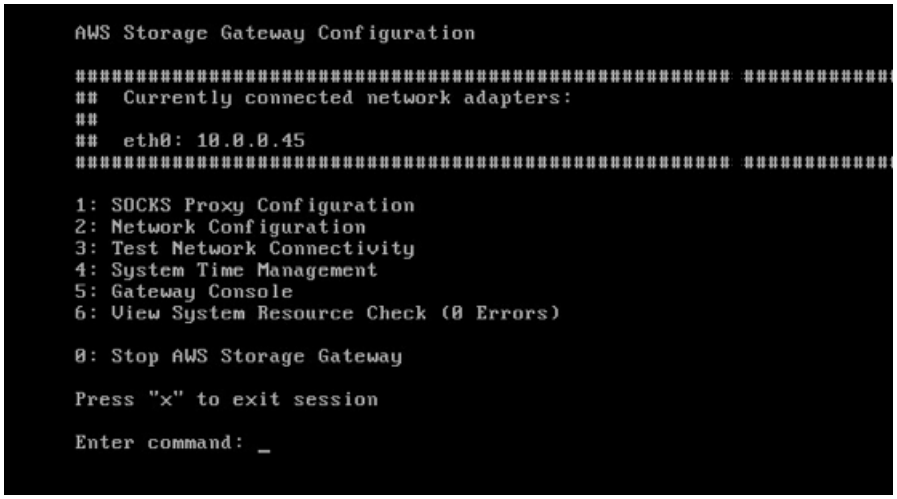
- Implementazione di VMware ESX`.ova`pacchetto scaricabile che contiene la VM Storage Gateway su un solo host in un cluster.
- Quando si distribuisce il pacchetto `.ova`, selezionare un datastore che non sia locale per un host. Al contrario, utilizzare un datastore accessibile a tutti gli host del cluster. 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` al cluster, seleziona un host nel momento in cui ti viene richiesto. In alternativa, puoi distribuire direttamente a un host in un cluster.

Sincronizzazione dell'ora della VM associata al gateway

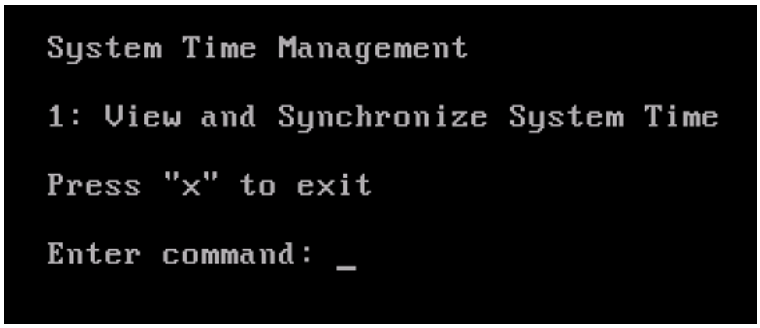
In caso di gateway distribuito su VMware ESXi, per evitare scostamenti temporali basta impostare l'ora dell'host dell'hypervisor e sincronizzazione l'ora della VM con quella dell'host. Per ulteriori informazioni, consultare Sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host. Per un gateway distribuito in Microsoft Hyper-V, è necessario controllare periodicamente l'ora della macchina virtuale usando la procedura descritta di seguito.

Per visualizzare e sincronizzare l'ora di una macchina virtuale del gateway hypervisor con un server NTP (Network Time Protocol)

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console locale di VMware ESXi, consultare 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 per la macchina virtuale basata su kernel (KVM) Linux, consulta Accesso alla console locale del gateway con Linux KVM.
2. SulConfigurazione di Storage Gatewaymenu principale, entra**4**perGestione del tempo di sistema.



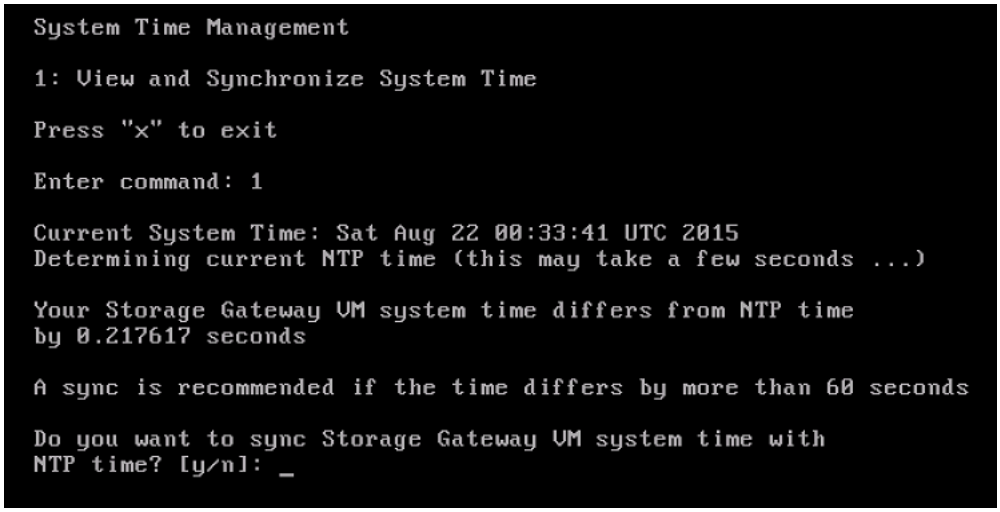
3. Nel menu System Time Management (Gestione ora di sistema), digitare **1** per View and Synchronize System Time (Visualizza e sincronizza ora di sistema).



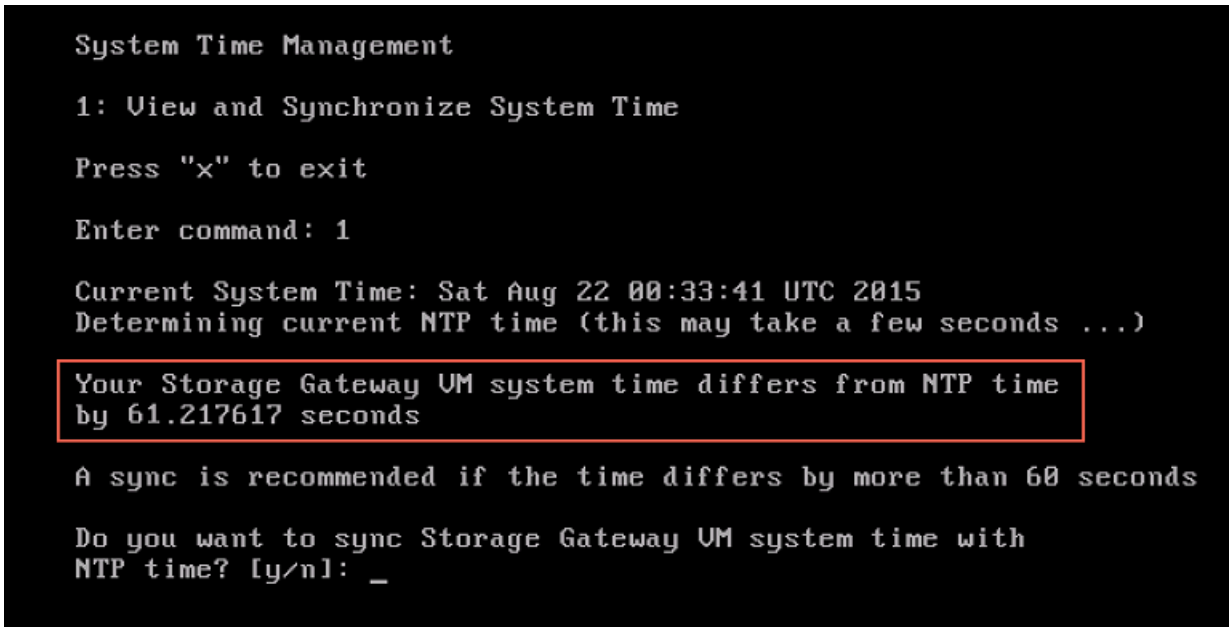
4. Se il risultato indica che è necessario sincronizzare l'ora della macchina virtuale con l'ora NTP, digitare **y**. In caso contrario, inserire **n**.

   Se si digita **y** per eseguire la sincronizzazione, l'operazione potrebbe richiedere alcuni minuti.

   Lo screenshot seguente mostra una macchina virtuale che non richiede la sincronizzazione dell'ora.



Lo screenshot seguente mostra una macchina virtuale che richiede la sincronizzazione dell'ora.



Distribuzione di un gateway di file su un host Amazon EC2

Puoi distribuire e attivare un gateway file in un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'Amazon Machine Image (AMI) del gateway di file è disponibile come AMI della community.

Per distribuire un gateway in un'istanza Amazon EC2

1. Nella pagina Select host platform (Seleziona piattaforma host) scegliere Amazon EC2.

2. Scegliere Launch Instance (Avvia istanza) per avviare un'AMI EC2 dello storage gateway. Verrai reindirizzato alla console Amazon EC2, dove puoi scegliere un tipo di istanza.
3. SulFase 2: Scegli il tipo di istanza.pagina, scegliere la configurazione hardware dell'istanza. Storage Gateway è supportato in tipi di istanza che soddisfano determinati requisiti minimi. Consigliamo di iniziare con il tipo di istanza m4.xlarge, che soddisfi i requisiti minimi per il funzionamento corretto del gateway. Per ulteriori informazioni, consultare Requisiti hardware per le macchine virtuali (VM) locali.

   È possibile ridimensionare l'istanza dopo l'avvio, se necessario. Per ulteriori informazioni, consultaRidimensionamento dell'istanzanellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux.

   > **Note**
   >
   > Determinati tipi di istanza, in particolare EC2 i3, usano dischi SSD NVMe. Questi possono causare problemi all'avvio o all'arresto del gateway file; ad esempio, è possibile perdere i dati dalla cache. Monitoraggio del`CachePercentDirty`Metrica Amazon CloudWatch e avvia/arresta il sistema solo quando il valore del parametro è`0`. Per ulteriori informazioni sui parametri di monitoraggio per il gateway, consultaParametri e dimensioni del Storage Gatewaynella documentazione di CloudWatch. Per maggiori informazioni sui requisiti in base al tipo di istanza Amazon EC2, consultathe section called “Requisiti per i tipi di istanza Amazon EC2”.
4. Seleziona Successivo: Configura i dettagli dell'istanza.
5. SulFase 3: Configura i dettagli dell'istanza, scegliere un valore perAssegna automaticamente IP pubblico. Se l'istanza deve essere accessibile dalla rete Internet pubblica, verifica che l'opzione Auto-assign Public IP (Assegna automaticamente indirizzo IP pubblico) sia impostata su Enable (Abilita). Se l'istanza non deve essere accessibile da Internet, scegliere Auto-assign Public IP (Assegna automaticamente indirizzo IP pubblico) per Disable (Disabilita).
6. PerRuolo IAM, scegli ilAWS Identity and Access ManagementRuolo (IAM) che si vuole usare per il gateway.
7. Seleziona Successivo: Aggiunta di storage.
8. SulFase 4: Aggiunta di storage, scegliereAggiunta di nuovo volumeper aggiungere storage all'istanza del gateway di file. È necessario configurare almeno un volume Amazon EBS per lo storage della cache.

   Dimensioni disco consigliate: Cache (minimo) 150 GiB e cache (massimo) 64 TiB

9. SulFase 5: Aggiungi tagpage, puoi aggiungere un tag facoltativo all'istanza. Quindi scegli Next (Successivo): Configura il gruppo di sicurezza.
10. SulFase 6: Configura il gruppo di sicurezzapagina, aggiungi regole del firewall per permettere a tipi specifici di traffico di raggiungere l'istanza. È possibile creare un nuovo gruppo di sicurezza o sceglierne uno esistente.

    > **Important**
    >
    > Oltre alle porte di attivazione di Storage Gateway e di accesso Secure Shell (SSH), i client NFS richiedono accesso ad altre porte. Per informazioni dettagliate, vedere Requisiti di rete e firewall.

11. Scegliere Review and Launch (Analizza e avvia) per controllare la configurazione.
12. SulFase 7: Rivedi l'avvio dell'istanza, scegliereAvvio di.
13. Nella finestra di dialogo Select an existing key pair or create a new key pair (Seleziona una coppia di chiavi esistente o crea una nuova coppia di chiavi) scegliere Choose an existing key pair (Scegli una coppia di chiavi esistente) e quindi selezionare la coppia di chiavi creata durante la configurazione. Al termine, scegliere la casella di conferma e quindi Launch Instances (Avvia istanze).

    Una pagina di conferma indica che l'istanza si sta avviando.
14. Scegliere View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. Nella schermata Instances (Istanze), puoi visualizzare lo stato dell'istanza. L'avvio di un'istanza richiede pochi minuti. Quando viene avviata, lo stato iniziale di un'istanza è pending (in attesa). Una volta avviata l'istanza, lo stato passa a running (in esecuzione) e l'istanza riceve un nome DNS pubblico.
15. Selezionare l'istanza, annotare l'indirizzo IP pubblico nella paginaDescription (Descrizione)tag e torna alConnect to (Connettiti a)AWSpagina nella console Storage Gateway per continuare la configurazione del gateway.

È possibile determinare l'ID AMI da utilizzare per l'avvio di un gateway file utilizzando la console Storage Gateway o interrogando ilAWS Systems Managerstore di parametri.

Per determinare l'ID AMI

1. Accedi allaAWS Management Consolee apri la console Storage Gateway all'indirizzohttps://console.aws.amazon.com/storagegateway/home.

2. Scegliere Crea gateway, scegliere Gateway File, quindi scegliere Avanti.
3. Nella pagina Choose host platform (Scegli piattaforma host) scegliere Amazon EC2.
4. ScegliereAvvia istanzaper avviare un'AMI EC2 Storage Gateway. Si verrà reindirizzati alla pagina dell'AMI EC2 della community, in cui è possibile visualizzare l'ID AMI per ilAWSRegione nell'URL.

   Oppure è possibile interrogare l'archivio dei parametri Systems Manager. Puoi utilizzare il pluginAWS CLIo Storage Gateway API per interrogare il parametro pubblico di Systems Manager nello spazio dei nomi`/aws/service/storagegateway/ami/FILE_S3/latest`. Ad esempio, utilizzando il seguente comando CLI restituisce l'ID dell'AMI corrente nell'interfaccia a riga di comando correnteAWSRegione .

   ```
   aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
   FILE_S3/latest
   ```

   Il comando CLI restituisce un output simile al seguente:

   ```
   {
       "Parameter": {
           "Type": "String",
           "LastModifiedDate": 1561054105.083,
           "Version": 4,
           "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
   FILE_S3/latest",
           "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
           "Value": "ami-123c45dd67d891000"
       }
   }
   ```

Ottenimento di una chiave di attivazione per il gateway

Per ottenere una chiave di attivazione per il gateway, devi inviare una richiesta Web alla macchina virtuale del gateway, che restituisce un reindirizzamento contenente la chiave di attivazione. Questa chiave di attivazione viene passata come uno dei parametri all'operazione API `ActivateGateway` per specificare la configurazione del gateway. Per ulteriori informazioni, consultaActivateGatewaynellaRiferimento dell'API Storage Gateway.

La richiesta inviata alla macchina virtuale del gateway contieneAWSRegione in cui si verifica 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`*.

Argomenti

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

Se non l'hai ancora fatto, installa e configura AWS CLI. A questo scopo, seguire le istruzioni fornite nella Guida per l'utente di AWS Command Line Interface:

- Installazione diAWS Command Line Interface
- Configurazione dellaAWS Command Line Interface

Nell'esempio seguente viene illustrato come utilizzare ilAWS CLIper recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

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" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
```

```
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
    activation_key_param=$(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 usare 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
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Utilizzo diAWS Direct Connectcon Storage Gateway

AWS Direct Connectcollega la rete interna ad Amazon Web Services Cloud. UsandoAWS Direct ConnectCon Storage Gateway è possibile creare una connessione per le esigenze di carichi di lavoro a throughput elevato in modo da fornire una connessione di rete dedicata tra il gateway locale eAWS.

Storage Gateway utilizza endpoint pubblici. Con unAWS Direct ConnectLa connessione attiva è possibile creare un'interfaccia virtuale pubblica per consentire al traffico di essere instradato agli

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 essere ugualeAWSRegione come ilAWS Direct Connectposizione, o può essere in un altroAWSRegione .

La figura seguente mostra un esempio di comeAWS Direct Connectfunziona con Storage Gateway.

La procedura seguente presuppone che è stato creato un funzionamento gateway.

Per utilizzareAWS Direct Connectcon Storage Gateway

1. Creare e stabilire unAWS Direct ConnectConnessione tra il data center locale e l'endpoint Storage Gateway. Per ulteriori informazioni su come creare una connessione, consultaNozioni di base suAWS Direct ConnectnellaAWS Direct ConnectGuida per l'utente di .
2. Connect l'appliance Storage Gateway locale alAWS Direct Connectrouter.
3. Creare un'interfaccia virtuale pubblica e configurare il router locale di conseguenza. Per ulteriori informazioni, consultaCreazione di un'interfaccia virtualenellaAWS Direct ConnectGuida per l'utente di .

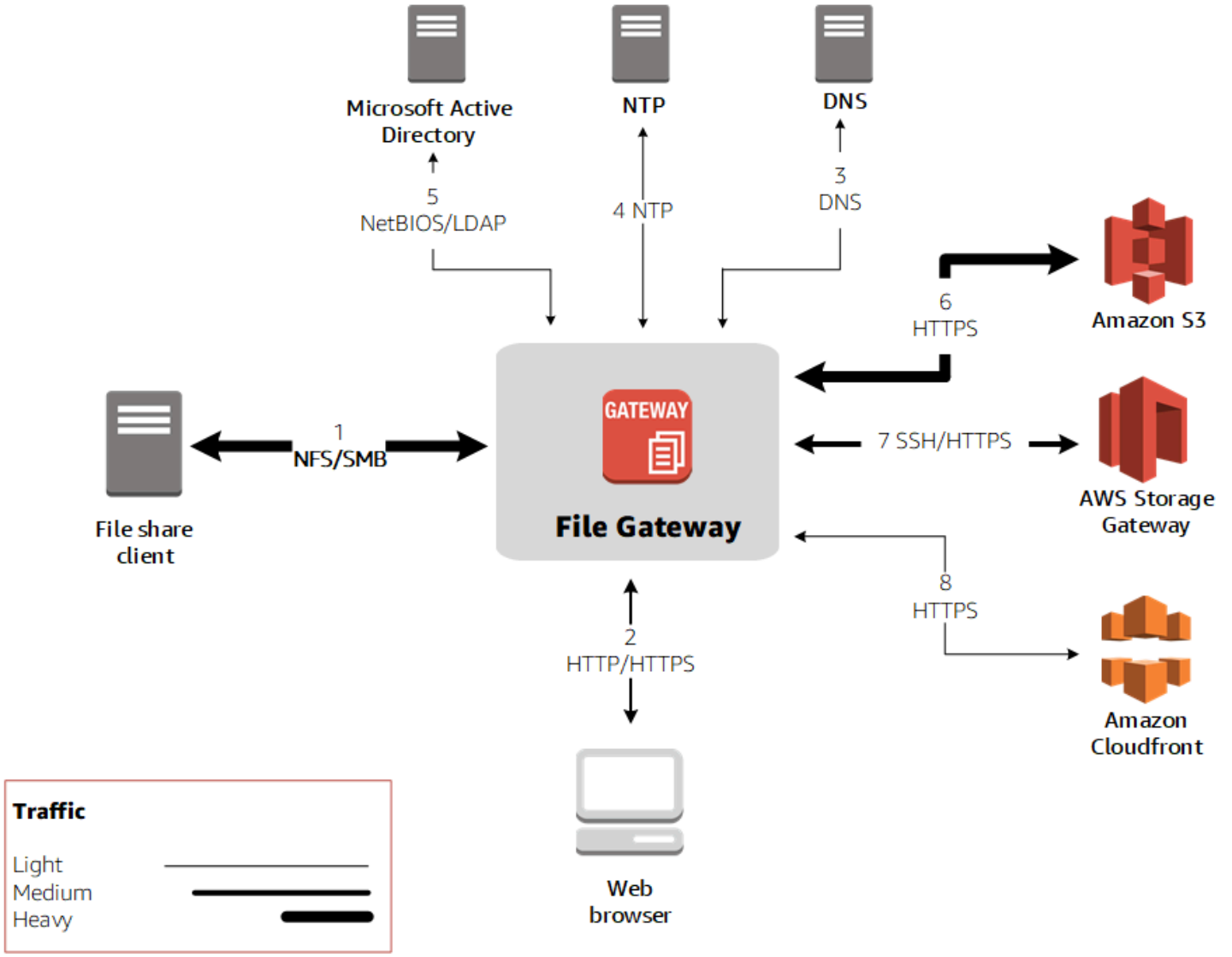
Per informazioni dettagliateAWS Direct Connect, consultaChe cos'èAWS Direct Connect?nellaAWS Direct ConnectGuida per l'utente di.

Requisiti porta

Per il corretto funzionamento di Storage Gateway, sono necessarie le porte seguenti. Alcune porte sono comuni a tutti i tipi di gateway e sono necessarie per tutti i tipi di gateway. Altre porte sono necessarie per determinati tipi di gateway. Questa sezione mostra una figura delle porte necessarie e un elenco delle porte richieste da ogni tipo di gateway.

Gateway di file

La figura seguente mostra le porte da aprire per il funzionamento dei gateway file.



Le seguenti porte sono comuni a tutti i tipi di gateway e sono richieste da tutti i tipi di gateway.

Da	Per	Protocollo	Porta	Modalità di utilizzo	
VM Storage Gateway	Amazon Web Services	TCP (Transmission Control Protocol)	443 (HTTPS)	Per la comunicazione da una macchina virtuale Storage Gateway a	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
				unAWSendpoint del servizio. Per informazioni sugli endpoint del servizio, consulta Consentire ad AWS Storage Gateway l'accesso attraverso firewall e router.	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Browser	VM Storage Gateway	TCP	80 (HTTP)	Tramite sistemi locali per ottenere la chiave di attivazione Storage Gateway. La porta 80 viene usata solo durante l'attivazione di un'appliance Storage Gateway. Per una macchina virtuale Storage Gateway non richiede l'apertura dell'accesso pubblico alla porta 80. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. Se si attiva il gateway	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
				dalla console di gestione Storage Gateway, l'host da cui ci si collega alla console deve avere accesso alla porta 80 del gateway.	
VM Storage Gateway	Server DNS (Domain Name Service)	UDP (User Datagram Protocol)	53 (DNS)	Per la comunicazione tra una macchina virtuale Storage Gateway e il server DNS.	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
VM Storage Gateway	Amazon Web Services	TCP	22 (Canale di supporto)	Consente ad Amazon Web Services Support di accedere 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.	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
VM Storage Gateway	Server NTP (Network Time Protocol)	UDP	123 (NTP)	Utilizzato dai sistemi locale per sincronizzare l'ora della VM con quella dell'host. Una macchina virtuale Storage Gateway è configura ta in modo che possa utilizzare i seguenti server NTP: • 0.amazon. pool.ntp. org • 1.amazon. pool.ntp. org • 2.amazon. pool.ntp. org • 3.amazon. pool.ntp. org	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Storage Gateway Hardware Appliance	Proxy Hypertext Transfer Protocol (HTTP)	TCP	8080 (HTTP)	Richiesto per l'attivazione.	

La tabella seguente elenca le porte che devono essere aperte per un gateway file quando si usa il protocollo NFS (Network File System) o SMB (Server Message Block). Queste regole per le porte fanno parte della definizione del gruppo di sicurezza.

Re	Elemento di rete	Tipo di condivisione file	Protocollo	Porta	In entrat	In uscita	Obbligatorio?	Note
1	Client della condivisione file	NFS	Dati TCP/UDP	111	✓	✓	✓	Trasferimento dei dati della condivisione file (solo per NFS)
			TCP/UDP per NFS	2049	✓	✓	✓	Trasferimento dei dati della condivisione file (solo per NFS)
			TCP/UDP per NFSv3	2004	✓	✓	✓	Trasferimento dei dati della condivisione file (solo per NFS)
		SMB	TCP/UDP per SMBv2	139	✓	✓	✓	Servizio della sessione di trasferimento dei dati della condivisione file (solo per

Re	Elemento di rete	Tipo di condivisione file	Protocollo	Porta	In entrat	In uscita	Obbligatorio?	Note
								SMB). Sostituisce le porte 137-139 per Microsoft Windows NT e versioni successive
			TCP/UDP per SMBv3	445	✓	✓	✓	Servizio della sessione di trasferimento dei dati della condivisione file (solo per SMB). Sostituisce le porte 137-139 per Microsoft Windows NT e versioni successive
2	Browser	NFS ed SMB	TCP/HTTP	80	✓	✓	✓	Amazon Web Services Management Console (solo attivazione)
			TCP/ HTTPS	443	✓	✓	✓	Amazon Web Services Management Console (tutte le altre operazioni)
3	DNS	NFS ed SMB	DNS TCP/ UDP	53	✓	✓	✓	Risoluzione dei nomi IP

Re	Elemento di rete	Tipo di condivisione file	Protocollo	Porta	In entrat	In uscita	Obbligatorio?	Note
4	NTP	NFS ed SMB	NTP UDP	123	✓	✓	✓	Servizio di sincronizzazione di data e ora
5	Microsoft Active Directory	SMB	UDP per NetBIOS	137	✓	✓	✓	Nome del servizio (non usato per NFS)
			UDP per NetBIOS	138	✓	✓	✓	Servizio datagramma
			LDAP TCP	389	✓	✓		Directory System Agent (DSA); connessione client
			LDAPS TCP	636	✓	✓		LDAP: LDAP (Lightweight Directory Access Protocol) su SSL (Secure Socket Layer)
6	Amazon S3	NFS ed SMB	Dati HTTPS	443	✓	✓	✓	Trasferimento dei dati di storage
7	Storage Gateway	NFS ed SMB	TCP/SSH	22	✓	✓	✓	Canale di supporto
			TCP/ HTTPS	443	✓	✓	✓	Controllo della gestione
8	Amazon CloudFront	NFS ed SMB	TCP/ HTTPS	443	✓	✓	✓	Per l'attivazione

Connessione al 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:

- Host VMware: 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: Ottenimento di 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.

Ottenimento di un indirizzo IP da un host Amazon EC2

Per ottenere l'indirizzo IP dell'istanza Amazon EC2, il gateway viene distribuito su EC2 e collegato alla console locale dell'istanza EC2. Quindi ottenere l'indirizzo IP nella parte superiore della pagina della console. Per istruzioni, consultare .

È anche possibile ottenere 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. Aprire 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. Aprire 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.
4. Dopo l'attivazione del gateway, scegliere il gateway appena attivato, quindi scegliere la scheda VTL devices (Dispositivi VTL) nel riquadro inferiore.
5. Ottenere i nomi di tutti i dispositivi VTL.
6. Per ogni destinazione, eseguire il comando seguente per configurare la destinazione.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```

7. Per ogni destinazione, eseguire il comando seguente per accedere.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   Il gateway è ora connesso utilizzando l'indirizzo IP elastico dell'istanza EC2.

Comprendere gli ID risorsa e le risorse Storage Gateway

In Storage Gateway, la risorsa principale è unGatewayma altri tipi di risorse includono:volume,nastro virtuale,Destinazione iSCSI, edispositivo vtl. In questo caso, si parla di risorse secondarie, che non esistono a meno che non siano state associate a un gateway.

A risorse e risorse secondarie sono associati Amazon Resource Name (ARN) univoci, come illustrato nella tabella seguente.

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`*
ARN volume	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
ARN nastro	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:tape/`*`tapebarcode`*
ARN di destinazione (destinazione iSCSI)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*
ARN dispositivi VTL	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

Storage Gateway supporta anche l'uso di istanze EC2, volumi EBS e snapshot. Queste risorse sono risorse Amazon EC2 utilizzate in Storage Gateway.

Utilizzo degli ID risorsa

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. Un ID volume assume il formato `vol-3344CCDD`, dove `vol` è l'identificativo della risorsa per i volumi.

Per i nastri virtuali, è possibile anteporre un prefisso contenente un massimo di quattro caratteri per l'ID di codici a barre per organizzare i nastri.

Gli ID della risorsa Storage Gateway sono maiuscoli. Tuttavia, quando usi 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**
>
> Gli ID per i volumi Storage Gateway e per le snapshot 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 utilizzare questi ID più lunghi in modo da testare i sistemi con il nuovo formato. Per ulteriori informazioni, consulta Longer EC2 and 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, consultaAnnuncio: Heads-up: volume Storage Gateway più lunghi e ID snapshot in arrivo nel 2016.

Tagging delle risorse 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 un gateway di file, puoi usare 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 perAWSutilizzare.
- I caratteri validi per la proprietà di chiave sono lettere e numeri UTF-8, spazi e i caratteri speciali + - = . _ : / e @.

Utilizzo dei tag

Puoi lavorare con i tag utilizzando la console Storage Gateway, l'API Storage Gateway oInterfaccia 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. Aprire la console Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
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. Aprire la console Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
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. Scegliere l'icona a forma di matita accanto al tag che si desidera modificare, quindi modificare il tag.
5. Al termine della modifica dei tag, scegliere Save (Salva).

Come Per eliminare un tag

1. Aprire la console Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
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).

consultare anche

Utilizzo dei tag per controllare l'accesso al gateway e alle risorse

Lavorare con componenti open source perAWS Storage Gateway

In questa sezione è possibile trovare informazioni sugli strumenti e le licenze di terze parti da cui dipendiamo per fornire funzionalità Storage Gateway.

Argomenti

Componenti open source per Storage Gateway

Diversi strumenti e licenze di terze parti vengono utilizzati per fornire funzionalità per il gateway del volume, il gateway a nastro e Amazon S3 File Gateway.

Utilizzare i seguenti collegamenti per scaricare il codice sorgente per determinati componenti software open source inclusi conAWS Storage Gatewaysoftware:

- Per i gateway distribuiti su VMware ESXi:sources.tar
- Per i gateway distribuiti su Microsoft Hyper-V:sources_hyperv.tar
- Per i gateway distribuiti su Linux Kernel-based Virtual Machine:sources_KVM.tar

Questo prodotto include software sviluppato dal progetto OpenSSL per l'uso nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consultaLicenze di terze parti.

Componenti open source per Amazon S3 File Gateway

Diversi strumenti e licenze di terze parti vengono utilizzati per fornire la funzionalità di Amazon S3 File Gateway (S3 File Gateway).

Usa i collegamenti seguenti per scaricare il codice sorgente per determinati componenti software open source inclusi con il software S3 File Gateway:

- Per Amazon S3 File Gateway:sgw-file-s3-open-source.tgz

Questo prodotto include software sviluppato dal progetto OpenSSL per l'uso nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consultaLicenze di terze parti.

Quote

Quote per le condivisioni di file

La tabella seguente elenca le quote per le condivisioni dei file.

Descrizione	Gateway di file
Il numero massimo di condivisioni di file per il bucket Amazon S3. È disponibile una mappatura one-to-one tra una condivisione file e un bucket S3	1
Il numero massimo di condivisioni di file per il gateway	10
La dimensione massima di un file singolo che corrisponde alla dimensione massima di un oggetto singolo in Amazon S3 **Note** Se scrivi un file di dimensioni superiori a 5 TB, ricevi un messaggio di errore che indica che il file è troppo grande e vengono caricati solo i primi 5 TB.	5 TB
Lunghezza massima del percorso **Note** I client non sono autorizzati a creare un percorso che superi questa lunghezza ; farlo genera un errore. Questo limite è valido per entrambi i protocolli supportati da gateway di file, NFS e SMB.	1024 byte

Dimensioni disco locali consigliate per il gateway

La tabella seguente contiene le dimensioni consigliate per lo storage su disco locale per il gateway distribuito.

Tipo di gateway	Cache (minimo)	Cache (massimo)	Altri dischi locali richiesti
Gateway file S3	150 GiB	64 TiB	—

> **Note**
>
> Puoi configurare una o più unità locali per la cache fino alla capacità massima.
> Quando aggiungi la cache a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza Amazon EC2). Non modificare la dimensione dei dischi esistenti se i dischi sono stati allocati in precedenza come cache.

Utilizzo delle classi di storage

Storage Gateway supporta le classi di storage Amazon S3 Standard, Amazon S3 Standard - Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering e classi di storage S3 Glacier. Per ulteriori informazioni sulle classi di storage, consultaClassi di storage di Amazon S3nellaManuale utente di Amazon Simple Storage Service.

Argomenti

- Utilizzo di classi di storage con un gateway di file
- Utilizzo della classe di storage GLACIER con il gateway di file

Utilizzo di classi di storage con un gateway di file

Quando si crea o si aggiorna una condivisione file, è possibile selezionare una classe di storage per gli oggetti. È possibile scegliere la classe di storage Amazon S3 Standard o una delle classi di storage S3 Standard - accesso infrequente, One Zone — IA S3 o Intelligent-Tiering S3. Gli oggetti archiviati in una di queste classi di storage possono essere trasferiti in GLACIER utilizzando una policy del ciclo di vita

Classe di storage di Amazon S3	Considerazioni
Standard	Selezionare Standard per archiviare i file ad accesso frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Questa è la classe di storage predefinita. Per ulteriori informazioni, consulta Prezzi di Amazon S3.
S3 Intelligent-Tiering	Scegli Intelligent-Tiering per ottimizzare i costi di storage spostando automaticamente i dati nel livello di accesso allo storage più convenien te. Gli oggetti archiviati nella classe di storage Intelligent-Tiering possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione, la richiesta o la transizione degli oggetti tra le classi di storage entro 30 giorni. Esiste una durata minima di archiviazione di 30 giorni e gli oggetti eliminati prima di 30 giorni comportan o un addebito proporzionale pari al costo di archiviazione per i giorni rimanenti. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Gli oggetti di dimensioni inferiori a 128 KB non sono idonee al tiering automatico nella classe di storage Intelligent-Tiering. Questi oggetti vengono addebitati alle tariffe di accesso frequenti e si applicano le tariffe di cancellaz ione anticipata. S3 Intelligent-Tiering ora supporta un livello di Accesso all'archivio e un livello Deep Archive Access. S3 Intelligent-Tiering sposta automatic amente gli oggetti a cui non è stato eseguito

Classe di storage di Amazon S3	Considerazioni
	l'accesso per 90 giorni al livello Accesso di archiviazione e quelli a cui non è stato eseguito l'accesso per 90 giorni al livello Accesso di archiviazione profonda. Ogni volta che un oggetto in uno dei livelli di accesso all'archi vio viene ripristinato, l'oggetto passa al livello Accesso frequente entro poche ore ed è pronto per essere recuperato. Questo crea errori di timeout per utenti o applicazioni che tentano di accedere ai file tramite una condivisione di file se l'oggetto esiste solo in uno dei due livelli di archivio. Non utilizzare i livelli di archivio con S3 Intelligent-Tiering se le applicazioni accedono ai file tramite le condivisioni di file presentate dal gateway di file. Quando le operazioni sui file che aggiornano i metadati (ad esempio proprietario, timestamp , autorizzazioni e ACL) vengono eseguite con i file gestiti dal gateway di file, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. È necessario convalida re il modo in cui le operazioni dei file influisco no sulla creazione di oggetti prima di utilizzar e questa classe di storage in produzione, poiché si applicano le tariffe di eliminazione Per ulteriori informazioni, consulta Prezzi di Amazon S3.

Classe di storage di Amazon S3	Considerazioni
S3 Standard-IA	Selezionare Standard-IA per archiviare i dati degli oggetti ad accesso poco frequente in modo ridondante in più zone di disponibilità geograficamente distinte. Gli oggetti archiviati nella classe di storage Standard-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione, la richiesta, il recupero o la transizione degli oggetti tra le classi di storage entro 30 giorni. La durata minima di conservazione è di 30 giorni. Gli oggetti eliminati prima di 30 giorni comportano un addebito proporzionale pari al costo di archiviazione per i giorni rimanenti. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Gli oggetti di dimensioni inferiori a 128 KB vengono addebitati 128 KB e si applicano le tariffe di cancellazione anticipata. Quando le operazioni sui file che aggiornano i metadati (ad esempio proprietario, timestamp , autorizzazioni e ACL) vengono eseguite con i file gestiti dal gateway di file, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. È necessario convalida re il modo in cui le operazioni dei file influisco no sulla creazione di oggetti prima di utilizzar e questa classe di storage in produzione, poiché si applicano le tariffe di eliminazione Per ulteriori informazioni, consulta Prezzi di Amazon S3.

Classe di storage di Amazon S3	Considerazioni
S3 One Zone-IA	Scegliere One Zone-IA per archiviare i file ad accesso non frequente in una singola zona di disponibilità. Gli oggetti archiviati nella classe di storage One Zone-IA possono comportare costi aggiuntivi per la sovrascrittura, l'eliminazione, la richiesta , il recupero o la transizione degli oggetti tra le classi di storage entro 30 giorni. Esiste una durata minima di archiviazione di 30 giorni e gli oggetti eliminati prima di 30 giorni comportan o un addebito proporzionale pari al costo di archiviazione per i giorni rimanenti. Considera la frequenza con cui questi oggetti cambiano, la durata di conservazione degli oggetti e la frequenza con cui è necessario accedervi. Gli oggetti di dimensioni inferiori a 128 KB vengono addebitati 128 KB e si applicano le tariffe di cancellazione anticipata. Quando le operazioni sui file che aggiornano i metadati (ad esempio proprietario, timestamp , autorizzazioni e ACL) vengono eseguite con i file gestiti dal gateway di file, l'oggetto esistente viene eliminato e viene creata una nuova versione dell'oggetto in questa classe di storage Amazon S3. È necessario convalida re il modo in cui le operazioni dei file influisco no sulla creazione di oggetti prima di utilizzar e questa classe di storage in produzione, poiché si applicano le tariffe di eliminazione Per ulteriori informazioni, consulta Prezzi di Amazon S3.

Anche se è possibile scrivere oggetti direttamente da una condivisione file alla classe di storage S3 Standard - accesso infrequente, One Zone — IA S3 o S3 Intelligent-Tiering, è consigliabile utilizzare una policy del ciclo di vita per trasferire gli oggetti anziché scrivere direttamente dalla condivisione file, specialmente se si prevede di aggiornare o eliminare gli oggetti. oggetto entro 30 giorni dall'archiviazione. Per informazioni sui criteri del ciclo di vita, consultaGestione del ciclo di vita degli oggetti.

Utilizzo della classe di storage GLACIER con il gateway di file

Se si sposta un file a S3 Glacier tramite le policy del ciclo di vita Amazon S3 e il file è visibile ai client di condivisione file tramite la cache, si ottengono errori I/O quando si aggiorna il file. È consigliabile impostare CloudWatch Events per ricevere una notifica quando si ottengono questi errori I/O e utilizzare la notifica per eseguire un'operazione. Ad esempio, puoi agire per ripristinare l'oggetto archiviato in Amazon S3. Dopo che gli oggetti sono ripristinati su S3, i client della condivisione file possono accedervi e aggiornarli tramite la condivisione file.

Per informazioni su come ripristinare gli oggetti archiviati, consultaRipristino di oggetti archiviatinellaManuale utente di Amazon Simple Storage Service.

Riferimento API per Storage Gateway

Oltre a usare la console, puoi usare l'API di AWS Storage Gateway per configurare e gestire i gateway a livello di programmazione. Questa sezione descrive le operazioni AWS Storage Gateway, la firma delle richieste per l'autenticazione e la gestione degli errori. Per informazioni sulle regioni e sugli endpoint disponibili per Storage Gateway, consultaAWS Storage GatewayEndpoint e quotenellaAWSRiferimenti generali.

> **Note**
>
> Puoi anche utilizzare l'AWSSDK durante lo sviluppo di applicazioni con Storage Gateway. LaAWSGli SDK per Java, .NET e PHP integrano l'API di Storage Gateway sottostante, semplificando le attività di programmazione. Per ulteriori informazioni sul download delle librerie SDK, consulta Librerie e codice di esempio.

Argomenti

AWS Storage GatewayIntestazioni obbligatorie delle richieste

Questa sezione descrive le intestazioni obbligatorie che devi inviare con ogni richiesta POST aAWS Storage Gateway. 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 usate nell'operazione ActivateGateway.

```
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 intestazioni seguenti devono essere incluse con le richieste POST diAWS Storage Gateway. Le intestazioni mostrate di seguito che iniziano con «x-amz» sonoAWSintestazioni specifiche. Tutte le altre intestazioni elencate sono intestazioni comuni usate in transazioni HTTP.

Intestazione	Descrizione
`Authorization`	L'intestazione di autorizzazione contiene diverse informazioni sulla richiesta che consentonoAWS Storage Gatewayper determinare se la richiesta è un'operazione valida 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/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Nella sintassi precedente abbiamo specificato YourAccessKey, l'anno, il mese e il giorno (yyyymmdd), la regione e CalculatedSignature. Il formato dell'intestazione di autorizzazione è determinato dai requisiti dellaAWSProcesso di firma V4. I dettagli sulla firma vengono approfonditi nell'argomento Firmare le richieste.
`Content-Type`	Utilizzaapplication/x-amz-json-1.1 come tipo di contenuto per tutte le richieste aAWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Intestazione	Descrizione
`Host`	Utilizzare l'intestazione host per specificare l'AWS Storage Gatewayendpoint in cui invii la richiesta. Ad esempio:`storagegateway.us-east-2.amazonaws.com` è l'endpoint della regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili perAWS Storage Gatewayconsulta[AWS Storage GatewayEndpoint e quote]nellaAWSRiferimenti generali. `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 un`x-amz-date` l'intestazione è presente, laAWS Storage Gatewayignora qualsiasi `Date`intestazione durante l'autenticazione della richiesta. `x-amz-date` deve avere il formato di base ISO8601, ovvero AAAAMMGG'T'HHMMSS'Z'. Se le intestazioni `Date` e `x-amz-date` vengono usate entrambe, il formato dell'intestazione Date non deve essere 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 di operationName, ad esempio "ActivateGateway", è disponibile nell'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, devi 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 Secret Access Key. 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 utilizzandoAWSSignature Version 4. La procedura per il calcolo di una firma può essere suddivisa in tre fasi:

- Task 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 lo stesso formato quando ricalcola una firma da confrontare con quella che hai inviato.
- Task 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.
- Task 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 a partire dalla chiave di accesso segreta e utilizzando la stringa di ambito credenziali per creare una serie di codici di autenticazione dei messaggi basati su hash (HMAC).

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. Altri calcoli di riferimento sono descritti in Suite di test Signature Version 4 nel glossario di Amazon Web Services.

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 Task 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. Ciò è dovuto alla mancanza di parametri di query per questa API (o qualsiasi API Storage Gateway).

La stringa di firma per Task 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 Task 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 errori di AWS Storage Gateway. 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'API ActivateGateway.

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 dell'API di AWS Storage Gateway. Quando un'operazione di AWS Storage Gateway 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 oAWSL'ID chiave di accesso fornito non esiste nei nostri record.	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. Verifica la tuaAWSChiave di accesso e 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 una valida (registrata)AWSID chiave di accesso o 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`	LaAWSAccess Key Id necessita di una sottoscrizione al servizio.	400 Richiesta non valida

Eccezione	Messaggio	Codice di stato HTTP
`ThrottlingException`	Velocità superata.	400 Richiesta non valida
`UnknownOperationException`	È stata specificata un'operazione sconosciuta. Le operazioni valide sono elencate in Operazioni in 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 delle operazioni di AWS Storage Gateway e le API che possono 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
`ActivationKeyNotFound`	La chiave di attivazione specificata non è stata trovata.	ActivateGateway

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`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
`DiskSizeGreaterThanVolumeMaxSize`	La dimensione del disco specificata è superiore alla dimensione massima del volume.	CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`DiskSizeLessThanVolumeSize`	La dimensione del disco specificata è inferiore alla dimensione del volume.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	Le informazioni sul certificato specificate sono duplicate.	ActivateGateway
Conflitto di configurazione endpoint associazione file system	La configurazione dell'endpoint esistente dell'associazione file system è in conflitto con la configurazione specificata.	File system associato
Indirizzo di punta per l'associazione di file system già in uso	L'indirizzo IP dell'endpoint specificato è già in uso.	File system associato
Indirizzo IP del punto finale dell'associazione file system mancante	L'indirizzo IP dell'endpoint dell'associazione file system è mancante.	File system associato
Associazione file system non trovata	L'associazione del file system specificata non è stata trovata.	Aggiorna l'associazione file system Dissociate file system Descrivi le associazioni di file system
File system non trovato	Il file system specificato non è stato trovato.	File system associato

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
`MaximumVolumeCount Exceeded`	Il numero massimo di volumi è stato superato.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	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
`SnapshotInProgress Exception`	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:

- Content-Type: application/x-amz-json-1.1
- 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.

Type: 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.

Type: Raccolta

errorCode

Uno dei codici di errore delle operazioni .

Type: Stringa

errorDetails

Questo campo non viene usato nella versione corrente dell'API.

Type: Stringa

message

Uno dei messaggi dei codici di errore delle operazioni in .

Type: Stringa

Esempi di risposta di errore

Il seguente corpo JSON viene restituito se si utilizza l'API DescribeStorediSCSIVolumes 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."
}
```

Operazioni in Storage Gateway

Per un elenco delle operazioni di Storage Gateway, consultaOperazioninellaAWS Storage GatewayDocumentazione di riferimento API.

Cronologia dei documenti per i .AWSStorage Gateway

- Versione API: 30-06-2013
- Ultimo aggiornamento della documentazione: 12 ottobre 2021

La tabella che segue descrive le modifiche importanti apportate in ogni versione diAWSGuida per l'Storage Gatewaydopo aprile 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

update-history-change	update-history-description	update-history-date
Procedure di creazione gateway aggiornate	La procedura per la creazione di un nuovo gateway è stato aggiornata in modo da rifletter e le modifiche nella console Storage Gateway. Per ulteriori informazioni, consultaCreare e attivare un gateway file Amazon S3.	12 ottobre 2021
Support per la chiusura forzata di file su condivisioni file SMB	Ora è possibile utilizzare le impostazioni del gruppo locale per assegnare le autorizza zioni di amministrazione del gateway. Gli amministratori gateway possono utilizzare lo snap-in Microsoft Managemen t Console cartelle condivise per chiudere forzatamente i file aperti e bloccati sulle condivisioni di file SMB. Per ulteriori informazioni, consultaConfigurazione di gruppi locali per il gateway.	12 ottobre 2021

Supporto del registro di controllo per le condivisioni file NFS	È ora possibile configurare le condivisioni file NFS per generare log di audit che forniscono dettagli sull'acce sso degli utenti a file e cartelle all'interno di una condivisi one di file. Puoi utilizzar e questi log per monitorar e le attività degli utenti e agire se vengono identificati modelli di attività inappropr iati. Per ulteriori informazioni, consultaInformazioni sui log di controllo del gateway di file.	12 ottobre 2021
Supporto per alias del punto di accesso	Le condivisioni di file gateway di file ora possono connetter si allo storage Amazon S3 utilizzando alias del punto di accesso in stile bucket. Per ulteriori informazioni, consultaCreare una condivisi one file.	12 ottobre 2021
Supporto per endpoint e access point VPC	Le condivisioni di file gateway di file possono ora connetter si a bucket S3 tramite punti di accesso o endpoint di interfaccia nel tuo VPC alimentato daAWS PrivateLi nk. Per ulteriori informazioni, consultaCreare una condivisi one file.	7 luglio 2021

Supporto di bloccaggio opportunistico	Le condivisioni file gateway di file possono ora utilizzare il blocco opportunistico per ottimizzare la strategia di buffering dei file, migliorando le prestazioni nella maggior parte dei casi, in particolare per quanto riguarda i menu contestuali di Windows. Per ulteriori informazioni, consultaCreare una condivisione di file SMB.	7 luglio 2021
Conformità agli standard FedRAMP	Storage Gateway è ora conforme a FedRAMP. Per ulteriori informazioni, consultaConvalida della conformità per Storage Gateway.	24 novembre 2020
Limitazione della larghezza di banda basata su pianificazione	Storage Gateway supporta ora la limitazione della larghezza di banda basata su pianificazione per gateway di nastri e volumi. Per ulteriori informazioni, consultaPianificazione della limitazione della larghezza di banda utilizzando la console Storage Gateway.	9 novembre 2020

Notifica di caricamento file per il gateway di file	Il gateway file ora fornisce una notifica di caricamento dei file, che ti avvisa quando un file è stato completamente caricato su Amazon S3 dal gateway file. Per ulteriori informazioni, consultaRicevere notifica di caricamento file.	9 novembre 2020
Enumerazione basata sull'accesso per il gateway di file	Il gateway file ora fornisce un'enumerazione basata sull'accesso, che filtra l'enumerazione di file e cartelle su una condivisi one di file SMB in base agli ACL della condivisione. Per ulteriori informazioni, consultaCreazione di una condivisione file SMB.	9 novembre 2020
Migrazione gateway di file	Il gateway file ora fornisce un processo documentato per la sostituzione di un gateway di file esistente con un nuovo gateway di file. Per ulteriori informazioni, consultaSostituzi one di un gateway di file con un nuovo gateway di file.	30 ottobre 2020
Prestazioni di lettura della cache fredda del gateway di file 4x incremento	Storage Gateway ha aumentato le prestazioni di lettura della cache fredda 4x. Per ulteriori informazioni, consultaGuida alle prestazioni per gateway di file.	31 agosto 2020

Ordinare l'apparecchio hardware tramite la console	Ora è possibile ordinare l'apparecchio hardware tramite ilAWSConsole Storage Gateway. Per ulteriori informazioni, consultaUtilizzo dell'appliance hardware Storage Gateway.	12 agosto 2020
Support per gli endpoint Federal Information Processing Standard (FIPS) in nuoviAWSRegioni	Puoi ora 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, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	31 luglio 2020

Support per più condivisioni di file associate a un singolo bucket Amazon S3	Il gateway file ora supporta la creazione di più condivisioni di file per un singolo bucket S3 e la sincronizzazione della cache locale del gateway di file con un bucket basato sulla frequenza di accesso alle directory. È possibile limitare il numero di bucket necessari per gestire le condivisioni di file create sul gateway di file. È possibile definire più prefissi S3 per un bucket S3 e mappare un singolo prefisso S3 a una singola condivisione di file gateway. È inoltre possibile definire i nomi delle condivisioni di file gateway indipendenti dal nome del bucket per adattarsi alla convenzione di denominazione della condivisione file locale. Per ulteriori informazioni, consultaCreazione di una condivisione file NFSoCreazione di una condivisione file SMB.	7 luglio 2020

Archiviazione cache locale del gateway di file 4x incremento	Storage Gateway ora supporta una cache locale fino a 64 TB per il gateway di file, migliorando le prestazio ni per le applicazioni locali fornendo accesso a bassa latenza a dataset di lavoro più grandi. Per ulteriori informazi oni, consultaDimensioni disco locali consigliate per il gatewaynellaGuida per l'Storage Gateway.	7 luglio 2020
Visualizzazione degli allarmi di Amazon CloudWatch nella console Storage Gateway	Puoi ora visualizzare gli allarmi CloudWatch nella console Storage Gateway. Per ulteriori informazioni, consultaInformazioni sugli allarmi CloudWatch.	29 maggio 2020
Supporto per gli endpoint Federal Information Processin g Standard (FIPS)	Puoi ora attivare un gateway con endpoint FIPS nelle regioni AWS GovCloud (US). Per scegliere un endpoint FIPS per un gateway di file, consulta Scelta di un endpoint del servizio. Per scegliere un endpoint FIPS per un gateway di volume, consulta Scelta di un endpoint di servizio. Per scegliere un endpoint FIPS per un gateway di nastri, consulta Scelta di un endpoint di servizio.	22 maggio 2020

NovitàAWSRegioni	Storage Gateway è ora disponibile nelle regioni Africa (Città del Capo) e UE (Milano). Per ulteriori informazioni, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	7 maggio 2020
Supporto per classe di storage S3 Intelligent-Tiering	Storage Gateway supporta ora la classe di storage 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, consultaLa classe di storage che ottimizza automaticamente gli oggetti con accesso più o meno frequente nellaAmazon Simple Storage Service.	30 aprile 2020

NovitàAWSRegion	Storage Gateway è ora disponibile nella regioneAWSRegione GovCloud (Stati Uniti orientali) di GovCloud. Per ulteriori informazioni, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	12 marzo 2020
Supporto per hypervisor macchina virtuale basata su kernel (KVM) Linux	Storage Gateway offre ora la possibilità di distribuire un gateway locale nella piattaforma di virtualizzazione KVM. I gateway distribuiti in KVM hanno tutte le stesse funzionalità e caratteristiche dei gateway locali esistenti. Per ulteriori informazioni, consultaHypervisor supportati e requisiti di hostingnellaGuida per l'Storage Gateway.	4 febbraio 2020

Supporto per VMware vSphere High Availability	Un Storage Gateway di file fornisce ora il supporto per la disponibilità elevata su VMware per proteggere i carichi di lavoro di storage da errori hardware, hypervisor o di rete. Per ulteriori informazioni, consultaUtilizzare VMware vSphere High Availability con Storage GatewaynellaGuida per l'Storage Gateway. Questa versione include inoltre i miglioramenti delle prestazioni. Per ulteriori informazioni, consultaPrestazioninellaGuida per l'Storage Gateway.	20 novembre 2019
NovitàRegione AWSper gateway di nastri	Il gateway di nastri è ora disponibile nella regione Sud America (San Paolo). Per ulteriori informazioni, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	24 settembre 2019

Support per Amazon CloudWatch Logs	Ora puoi configurare i gateway di file con Amazon CloudWatch Log Groups per ricevere notifiche sugli errori e sullo stato del gateway e delle relative risorse. Per ulteriori informazioni, consultaRicevere una notifica sullo Health e gli errori del gateway con i gruppi di log di Amazon CloudWatchnellaGuida per l'utente Storage Gateway.	4 settembre 2019
NovitàRegione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	14 agosto 2019
NovitàRegione AWS	Storage Gateway è ora disponibile nella regione Medio Oriente (Bahrein). Per ulteriori informazioni, consultaAWSEndpoint e quote Storage GatewaynellaAWSRiferimenti generali.	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 della condivisione di file SMB per le ACL di Microsoft Windows	Per i gateway di file, ora è possibile utilizzare le liste di controllo accessi (ACL) di Microsoft Windows per controllare l'accesso alle condivisioni file SMB (Server Message Block). Per ulteriori informazioni, consulta Utilizzo di Microsoft Windows ACL per controllare l'accesso a una condivisione di file SMB.	8 maggio 2019
Supporto del gateway di file per l'autorizzazione basata su tag	Il gateway di file ora supporta l'autorizzazione basata su tag. È possibile controlla re l'accesso alle risorse di gateway di file in base ai tag su queste 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 di Storage Gateway Hardware Appliance	Storage Gateway Hardware Appliance è ora disponibile in Europa. Per ulteriori informazioni, consultaAWSRegioni AWS Storage Gateway HardwarenellaAWSRiferimenti generali. Inoltre, ora è possibile aumentare lo storage utilizzabile sull'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. Per ulteriori informazioni, consulta Configurazione dell'appliance hardware.	25 febbraio 2019
Support per Dispositivo hardware Storage Gateway	Storage Gateway Hardware Appliance include il software Storage Gateway preinstallato su un server di terze parti. È possibile gestire l'appliance dalla AWS Management Console. L'appliance può ospitare gateway di file, nastri e volumi. Per ulteriori informazioni, consultaUtilizzo dell'appliance hardware Storage Gateway.	18 settembre 2018

Supporto per il protocollo SMB (Server Message Block)	I gateway di file hanno aggiunto il supporto per il protocollo SMB (Service Message Block) alle condivisi oni file. Per ulteriori informazi oni, consulta Creazione di una condivisione file.	20 giugno 2018

Aggiornamenti precedenti

La tabella che segue descrive le modifiche importanti apportate in ogni versione diAWSGuida per l'Storage Gatewayprima di maggio 2018.

Modifica	Descrizione	Data della modifica
Support per la classe di storage S3 One Zone-IA	Per i gateway file puoi ora scegliere S3 One Zone-IA come classe di storage predefinita per le condivisioni file. Usando questa classe di storage, puoi archiviar e i dati degli oggetti in un'unica zona di disponibilità in Amazon S3. Per ulteriori informazioni, consultare Creazione di una condivisione file.	4 Aprile 2018
Novità Regione AWS	Il gateway di nastri è ora disponibile nella regione Asia Pacifico (Singapore). Per informazioni dettagliate, vedere Regioni AWS supportate.	3 Aprile 2018
Support per la notifica dell'aggi ornamento della cache, i Pagamenti a carico del richiedente e le liste di controllo degli accessi	Con i gateway file puoi ora ricevere notifiche quando il gateway completa l'aggiornamento della cache per il bucket Amazon S3. Per ulteriori informazioni, consultaRefreshCache.htmlnellaRiferimento per Storage Gateway. Per i gateway di file, ora è possibile specificare che il richiedente o il lettore paga le tariffe di accesso al posto del proprietario del bucket.	1 marzo 2018

Modifica	Descrizione	Data della modifica
predefinite per bucket Amazon S3	Con i gateway file puoi ora abilitare il controllo completo al proprietario del bucket S3 mappato alla condivisione file NFS. Per ulteriori informazioni, consultare Creazione di una condivisione file.	
Novità Regione AWS	Storage Gateway è ora disponibile nella regione UE (Parigi). Per informazioni dettagliate, vedere Regioni AWS supportate.	18 dicembre 2017
Supporto per la notifica di caricamento dei file e il rilevamento del tipo MIME	I gateway file permettono ora di ricevere una notifica quando tutti i file scritti nella condivisione file NFS sono stati caricati in Amazon S3. Per ulteriori informazioni, consultaNotifyWhenUploadednellaRiferimento per Storage Gateway. I gateway di file permettono ora il rilevamento del tipo MIME per gli oggetti caricati in base alle estensioni dei file. Per ulteriori informazioni, consultare Creazione di una condivisione file.	21 Novembre 2017
Supporto per VMware ESXi Hypervisor versione 6.5	AWSStorage Gateway supporta ora VMware ESXi Hypervisor versione 6.5. Questa si aggiunge alle versioni 4.1, 5.0, 5.1, 5.5 e 6.0. Per ulteriori informazioni, consultare 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, consultare Hypervisor supportati e requisiti di hosting.	22 giugno 2017
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Mumbai). Per informazioni dettagliate, vedere Regioni AWS supportate.	02 maggio 2017

Modifica	Descrizione	Data della modifica
Aggiornamenti alle impostazioni della condivisione file Supporto per l'aggiornamento della cache per le condivisioni file	I gateway di file aggiungono ora opzioni di montaggio alle impostazioni della condivisione file. Puoi ora impostare opzioni di squash e di sola lettura per la condivisione file. Per ulteriori informazioni, consultare Creazione di una condivisione file. I gateway di file possono ora individuare nel bucket Amazon S3 oggetti aggiunti o rimossi dall'ultima volta in cui il gateway ha elencato il contenuto del bucket e ha memorizzato nella cache i risultati. Per ulteriori informazioni, consulta RefreshCache nella documenta zione di riferimento delle API.	28 marzo 2017
Supporto per i gateway di file in Amazon EC2	AWSStorage Gateway offre ora la possibilità di distribuire un gateway file in Amazon EC2. Puoi avviare un gateway di file in Amazon EC2 usando l'AMI (Storage Gateway Amazon Machine Image) ora disponibile come AMI della community. Per informazi oni su come creare un gateway di file e distribuirlo in un'istanza EC2, consulta Creare e attivare un gateway Amazon S3 File Gateway. Per informazioni su come avviare l'AMI di un gateway di file, consulta Distribuz ione di un gateway di file su un host Amazon EC2. Inoltre, il gateway file supporta ora la configurazione del proxy HTTP. Per ulteriori informazioni, consultare Instradamento del gateway distribuito su EC2 tramite un proxy HTTP.	08 febbraio 2017
Novità Regione AWS	Storage Gateway è ora disponibile nella regione UE (Londra). Per informazioni dettagliate, vedere Regioni AWS supportate.	13 dicembre 2016

Modifica	Descrizione	Data della modifica
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Canada (Centrale). Per informazioni dettagliate, vedere Regioni AWS supportate.	08 dicembre 2016
Supporto per il gateway di file	Oltre ai gateway di volumi e ai gateway di nastri, Storage Gateway offre ora File Gateway. Un gateway file combina un servizio e un'appliance 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 consente l'accesso a oggetti in Amazon S3 come file in un punto di montaggio NFS.	29 Novembre 2016

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.