Guida per l'utente per gateway di nastri virtuali

AWS Storage Gateway

Versione API 2013-06-30

AWS Storage Gateway: Guida per l'utente per gateway di nastri virtuali

Table of Contents

La documentazione del gateway di file Amazon S3 è stata spostata in Cos'è un gateway di file Amazon S3?

La documentazione del gateway di file Amazon FSx è stata spostata in Cos'è un gateway di file Amazon FSx?

La documentazione del gateway di volumi è stata spostata in Cos'è un gateway di volumi?

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.

Cos'è un gateway di nastri virtuali?

AWS Storage Gateway collega un'appliance software locale con lo storage basato sul cloud per fornire una perfetta integrazione con le funzionalità di sicurezza dei dati tra l'ambiente IT locale e l'infrastruttura di storage. AWS Puoi utilizzare il servizio per archiviare i dati nel cloud Amazon Web Services per uno spazio di archiviazione scalabile e a costi contenuti che contribuisce a mantenere la sicurezza dei dati.

AWS Storage Gateway offre soluzioni di storage di file basate su file (Amazon S3 File e Amazon FSx File), basate su volume (memorizzate nella cache e archiviate) e su nastro.

Argomenti

Gateway di nastri virtuali

Gateway di nastri virtuali: un gateway di nastri virtuali fornisce archiviazione su nastri virtuali con backup del cloud.

Con un gateway di nastri virtuali, è possibile archiviare in modo conveniente e durevole i dati di backup in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Un gateway di nastri virtuali fornisce un'infrastruttura di nastri virtuali perfettamente scalabile in base alle esigenze aziendali ed elimina gli oneri operativi di provisioning, dimensionamento e manutenzione di un'infrastruttura di nastri fisici.

È possibile implementare Storage Gateway in locale come appliance VM in esecuzione su VMware ESXi, KVM o hypervisor Microsoft Hyper-V, come appliance hardware o come istanza Amazon EC2. AWS Distribuisci il gateway su un'istanza EC2 per il provisioning di volumi di archiviazione iSCSI in AWS. È possibile usare i gateway in hosting su istanze EC2 per il ripristino di emergenza e il mirroring dei dati, nonché per fornire archiviazione alle applicazioni in hosting su Amazon EC2.

Per una panoramica dell'architettura, consulta Come funziona il gateway di nastri virtuali (architettura). Per visualizzare l'ampia gamma di casi d'uso che AWS Storage Gateway contribuisce a realizzare, consulta AWS Storage Gateway.

Documentazione: per la documentazione del gateway di nastri virtuali, consulta Creazione di un gateway di nastri virtuali.

È la prima volta che utilizzi Storage Gateway?

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:

- Creazione di un gateway di nastri virtuali fornisce istruzioni su come creare e utilizzare un gateway di nastri virtuali. Mostra come eseguire il backup dei dati su nastri virtuali e archiviare i nastri.

- Gestione del gateway descrive come eseguire le attività di gestione per il 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, consulta Documentazione di riferimento delle API AWS Storage Gateway.

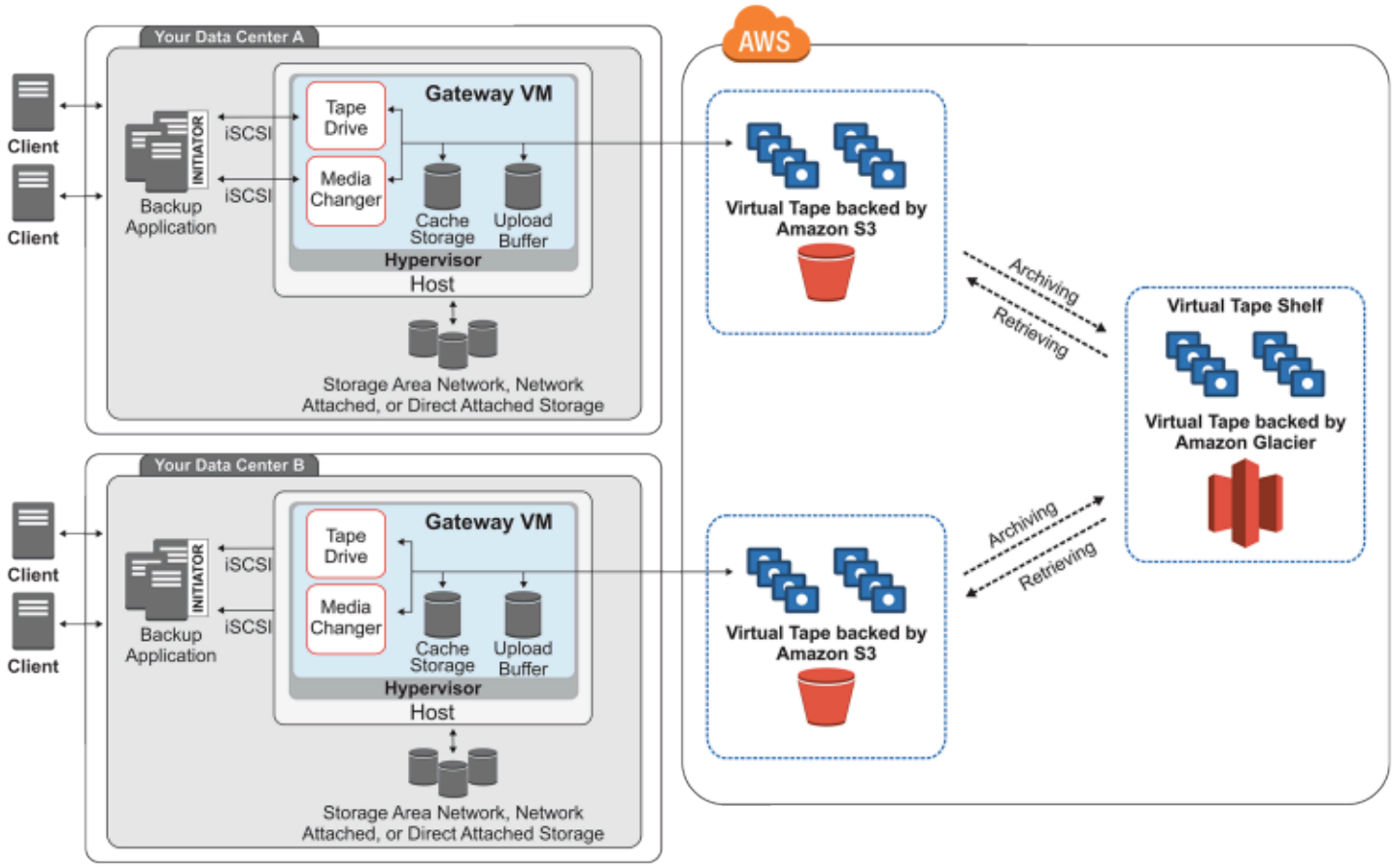
Come funziona il gateway di nastri virtuali (architettura)

Di seguito, puoi trovare una panoramica dell'architettura della soluzione gateway di nastri virtuali.

Gateway di nastri virtuali

Il gateway di nastri virtuali offre una soluzione durevole e conveniente per archiviare i dati nel cloud Amazon Web Services. L'interfaccia della libreria di nastri virtuali (VTL) ti permette di usare l'infrastruttura di backup basato su nastri esistente per archiviare i dati nei nastri virtuali che crei nel gateway di nastri virtuali. Ogni gateway di nastri virtuali è preconfigurato con un'unità di sostituzione dei supporti e unità a nastro. Queste unità sono disponibili per le applicazioni di backup client esistenti come dispositivi iSCSI. Puoi aggiungere nastri in base alle esigenze per archiviare i dati.

Il diagramma seguente fornisce una panoramica dell'implementazione del gateway di nastri virtuali.



Il diagramma mostra i seguenti componenti del gateway di nastri virtuali:

- Nastro virtuale: un nastro virtuale è come un nastro fisico. Tuttavia, i dati del nastro virtuale vengono archiviati nel cloud Amazon Web Services. Come i nastri fisici, i nastri virtuali possono essere vuoti o avere dati scritti su di essi. È possibile creare nastri virtuali utilizzando la console Storage Gateway oppure in modo programmatico tramite l'API di Storage Gateway. Ciascun gateway può contenere fino a 1.500 nastri o fino a 1 PiB di dati su nastro totali alla volta. Le dimensioni di ciascun nastro virtuale, configurabili al momento della creazione del nastro, vanno da 100 GiB a 15 TiB.
- Libreria di nastri virtuali (VTL): una VTL è come una libreria di nastri fisici disponibile on-premise con bracci robotici e unità a nastro. La VTL contiene la raccolta dei nastri virtuali archiviati. Ogni gateway di nastri virtuali viene fornito con una VTL.

  I nastri virtuali che crei vengono visualizzati nella VTL del gateway. Il backup dei nastri nella VTL viene eseguito da Amazon S3. Man mano che il software di backup scrive i dati sul gateway, il gateway archivia i dati a livello locale e li carica quindi in modo asincrono sui nastri virtuali nella VTL, ovvero Amazon S3.

  - Unità a nastro: un'unità a nastro della VTL è come un'unità a nastro fisica che può eseguire operazioni di I/O e ricerca su un nastro. Ogni VTL viene fornita con un set di 10 unità nastro, a disposizione dell'applicazione di backup come dispositivi iSCSI.
  - Unità di sostituzione dei supporti: un'unità di sostituzione dei supporti della VTL è come un robot che sposta i nastri nelle unità a nastro e negli slot di archiviazione della libreria di nastri fisici. Ogni VTL viene fornita con un'unità di sostituzione dei supporti, a disposizione dell'applicazione di backup come dispositivo iSCSI.
- Archivio: l'archivio è come un sito di nastri offsite. Puoi archiviare i nastri dalla VTL del gateway all'archivio. Se necessario, puoi recuperare i nastri dall'archivio alla VTL del gateway.
  - Archiviazione di nastri: quando il software di backup espelle un nastro, il gateway sposta il nastro nell'archivio per l'archiviazione a lungo termine. L'archivio è situato nella regione AWS in cui viene attivato il gateway. I nastri nell'archivio sono archiviati nello scaffale di nastri virtuali (VTS). Il VTS è supportato da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, il servizio di archiviazione a costi contenuti per l'archiviazione, il backup e la conservazione dei dati a lungo termine.
  - Recupero di nastri: non è possibile leggere direttamente i nastri archiviati. Per leggere un nastro archiviato, per prima cosa è necessario recuperarlo nel gateway di nastri virtuali utilizzando la console Storage Gateway o l'API di Storage Gateway.

    > **Important**
    >
    > È possibile recuperare un nastro archiviato in S3 Glacier Flexible Retrieval, generalmente entro 3-5 ore. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore.

Dopo aver distribuito e attivato un gateway di nastri virtuali, puoi montare le unità nastro virtuali e l'unità di sostituzione dei supporti sui server applicativi on-premise come dispositivi iSCSI. È possibile creare nastri virtuali in base alle esigenze. Dopo di che, è possibile utilizzare l'applicazione software di backup esistente per scrivere i dati sui nastri virtuali. L'unità di sostituzione dei supporti carica e scarica i nastri virtuali nelle unità nastro virtuali per le operazioni di lettura e scrittura.

Allocazione dei dischi locali per la macchina virtuale del gateway

La macchina virtuale del gateway necessita di dischi locali, che allochi per i seguenti scopi:

- Archiviazione della cache: l'archiviazione della cache funge da archiviazione durevole per i dati che aspettano di essere caricati in Amazon S3 dal buffer di caricamento.

  Se l'applicazione legge i dati da un nastro virtuale, il gateway salva i dati nello storage della cache. Il gateway archivia i dati utilizzati di recente nello storage della cache per l'accesso a bassa latenza. Se l'applicazione richiede dati su nastro, il gateway verifica innanzitutto la presenza di dati nella cache prima di scaricarli da AWS.
- Buffer di caricamento: il buffer di caricamento fornisce un'area di gestione temporanea al gateway prima che carichi i dati su un nastro virtuale. Il buffer di caricamento è inoltre fondamentale per la creazione di punti di ripristino da utilizzare per ripristinare i nastri dopo errori imprevisti. Per ulteriori informazioni, consulta È necessario recuperare un nastro virtuale da un gateway di nastri virtuali non funzionante.

Man mano che l'applicazione di backup scrive i dati nel gateway, il gateway copia i dati sia nello storage della cache sia nel buffer di caricamento. Dopo di che riconosce il completamento dell'operazione di scrittura sull'applicazione di backup.

Per le linee guida sulla quantità di spazio su disco da allocare per lo storage della cache e il buffer di caricamento, consulta Determinazione della quantità di archiviazione su disco locale.

Prezzi di Storage Gateway

Per informazioni aggiornate sui prezzi, consulta la sezione Prezzi nella pagina dei dettagli. AWS Storage Gateway

Pianifica l'implementazione di Storage Gateway

Utilizzando l'appliance software Storage Gateway, è possibile connettere l'infrastruttura applicativa locale esistente con uno storage AWS cloud scalabile ed economico che fornisce funzionalità di sicurezza dei dati.

Per distribuire Storage Gateway, è prima necessario scegliere le due caratteristiche seguenti:

1. Il tipo di gateway: questa guida copre i seguenti tipi di gateway:
   - Gateway di nastri virtuali: se cerchi un'alternativa conveniente, durevole, a lungo termine e fuori sede per l'archiviazione dei dati, distribuisci un gateway di nastri virtuali. L'interfaccia della libreria di nastri virtuali (VTL, Virtual Tape Library) ti permette di usare l'infrastruttura software

di backup basato su nastri esistente per archiviare i dati nei nastri virtuali creati. Per ulteriori informazioni, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali. Quando archivi i nastri, non devi preoccuparti di gestirli in locale e di organizzare le spedizioni fuori sede. Per una panoramica dell'architettura, vedi Come funziona un gateway di nastri virtuali (architettura).

2. Opzione di hosting: puoi eseguire Storage Gateway in locale come appliance VM o hardware oppure come istanza AWS Amazon EC2. Per ulteriori informazioni, consulta Requisiti. Se il tuo data center va offline e non hai un host disponibile, puoi distribuire un gateway in un'istanza EC2. Storage Gateway fornisce un'Amazon Machine Image (AMI) che contiene l'immagine della macchina virtuale del VM del gateway.

Quando configuri un host per distribuire un'appliance software gateway, devi inoltre allocare storage sufficiente per la macchina virtuale del gateway.

Prima di continuare con la fase successiva, assicurati di aver completato le operazioni seguenti:

1. Per un gateway distribuito on-premise, scegliere il tipo di host VM e configurarlo. Le opzioni disponibili sono VMware ESXi Hypervisor, Microsoft Hyper-V e KVM Linux. Se distribuisci il gateway protetto un firewall, assicurati che le porte siano accessibili alla macchina virtuale del gateway. Per ulteriori informazioni, consulta Requisiti.
2. Installa il software di backup del tuo client. Per ulteriori informazioni, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Nozioni di base

In questa sezione puoi trovare informazioni su come iniziare a utilizzare Storage Gateway. Per iniziare, devi prima registrarti a AWS. Se sei un nuovo utente, ti consigliamo di leggere la sezione relativa a regioni e requisiti.

Argomenti

Registrati per AWS Storage Gateway

Per utilizzare Storage Gateway, è necessario disporre di un account Amazon Web Services che consenta di accedere a tutte le risorse AWS , ai forum, al supporto e ai report di utilizzo. Non ti verrà addebitato alcun costo per i servizi a meno che tu non decida di utilizzarli. Se disponi già di un account Amazon Web Services, puoi ignorare questa fase.

Registrazione per un account Amazon Web Services

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

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

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

Per informazioni sui prezzi, consulta la pagina Prezzi nella pagina dei dettagli di Storage Gateway.

AWS Regioni

Storage Gateway archivia i dati di volume, istantanee, nastri e file nella AWS regione in cui è attivato il gateway. I dati dei file vengono archiviati nella AWS regione in cui si trova il bucket Amazon S3. È necessario selezionare una AWS regione nella parte superiore destra della console di gestione dello Storage Gateway prima di iniziare a implementare il gateway.

- Storage Gateway: per AWS le regioni supportate e un elenco di endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere AWS Storage Gateway Endpoints and Quotas nel. Riferimenti generali di AWS
- Storage Gateway Hardware Appliance: per AWS le regioni supportate che è possibile utilizzare con l'appliance hardware, vedere AWS Storage Gateway Hardware Appliance Regions nel. Riferimenti generali di AWS

Requisiti

Salvo diversa indicazione, i seguenti requisiti sono comuni a tutte le configurazioni del gateway.

Argomenti

- Requisiti storage e hardware
- Requisiti di rete e firewall
- Hypervisor supportati e requisiti di hosting
- Iniziatori iSCSI supportati
- Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali

Requisiti storage e hardware

Questa sezione illustra requisiti minimi hardware, impostazioni per il gateway e quantità minima di spazio su disco da allocare per l'archiviazione richiesta.

Requisiti hardware per le VM

Durante la distribuzione del gateway, devi accertare che l'hardware sottostante in cui implementi la macchina virtuale del gateway possa dedicare le seguenti risorse minime:

- Quattro processori virtuali assegnati alla macchina virtuale.

- Per e Gateway di nastri virtuali, l'hardware deve dedicare le seguenti quantità di RAM:
  - 16 GiB di RAM riservata per gateway con dimensioni della cache fino a 16 TiB
  - 32 GiB di RAM riservata per gateway con dimensioni della cache da 16 TiB a 32 TiB
  - 48 GiB di RAM riservata per gateway con dimensioni della cache da 32 TiB a 64 TiB
- 80 GiB di spazio su disco per l'installazione dell'immagine della macchina virtuale e dei dati di sistema.

Per ulteriori informazioni, consulta Ottimizzazione delle prestazioni del gateway. Per ulteriori informazioni su come l'hardware influisce sulle prestazioni della macchina virtuale del gateway, vedere AWS Storage Gateway quote.

Requisiti per i tipi di istanze Amazon EC2

Durante l'implementazione del gateway su Amazon Elastic Compute Cloud (Amazon EC2), le dimensioni dell'istanza devono essere almeno xlarge affinché il gateway funzioni. Tuttavia, per la famiglia di istanze ottimizzate per il calcolo, le dimensioni devono essere almeno 2xlarge.

Per Tape Gateway, l'istanza Amazon EC2 deve dedicare le seguenti quantità di RAM a seconda della dimensione della cache che intendi utilizzare per il gateway:

- 16 GiB di RAM riservata per gateway con dimensioni della cache fino a 16 TiB
- 32 GiB di RAM riservata per gateway con dimensioni della cache da 16 TiB a 32 TiB
- 48 GiB di RAM riservata per gateway con dimensioni della cache da 32 TiB a 64 TiB

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

Consigliati per i volumi memorizzati nella cache e i tipi di gateway di nastri virtuali

- Famiglia di istanze per uso generico: tipi di istanza m4, m5 o m6.

> **Note**
>
> Non è consigliabile utilizzare il tipo di istanza m4.16xlarge.

- Famiglia di istanze ottimizzate per il calcolo: tipi di istanza c4, c5 o c6. Selezionare le dimensioni istanza 2xlarge o superiori per soddisfare i requisiti della RAM.
- Famiglia di istanze ottimizzate per la memoria: tipi di istanza r3, r5 o r6.

- Famiglia di istanze ottimizzate per l'archiviazione: tipi di istanza i3 o i4.

Requisiti di storage

Oltre agli 80 GiB di spazio su disco per la macchina virtuale, sono necessari anche dischi aggiuntivi 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)	Buffer di caricamento (minimo)	Buffer di caricamento (minimo)	Altri dischi locali richiesti
Gateway di nastri virtuali	150 GiB	64 TiB	150 GiB	2 TiB	—

> **Note**
>
> È possibile configurare una o più unità locali per la cache e il buffer di caricamento, fino alla capacità massima.
> Quando aggiungi la cache o il buffer di caricamento 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 o come buffer di caricamento.

Per informazioni sulle quote del gateway, consulta AWS Storage Gateway quote.

Requisiti di rete e firewall

Il gateway richiede accesso a internet, reti locali, server DNS (Domain Name Service), firewall, router ecc. Di seguito, puoi trovare ulteriori informazioni sulle porte e sulle modalità per consentire l'accesso tramite firewall e router.

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

> **Note**
>
> I requisiti di larghezza di banda della rete variano in base alla quantità di dati caricati e scaricati dal gateway. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway. I modelli di trasferimento dei dati determineranno la larghezza di banda necessaria per supportare il carico di lavoro. In alcuni casi, è possibile distribuire Storage Gateway su Amazon EC2 o utilizzare altri tipi di implementazione

Argomenti

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 dallo Storage Gateway all'endpoint del AWS servizio. Per informazioni sugli endpoint del servizio, consulta Consentire AWS Storage Gateway l'accesso tramite firewall e router.
TCP	80 (HTTP)	In entrata	L'host da cui ci si connette alla console AWS di gestione.	Storage Gateway	Dai sistemi locali per ottenere la chiave di attivazione di Storage Gateway. La porta 80 viene usata solo durante l'attivazione dell'appl

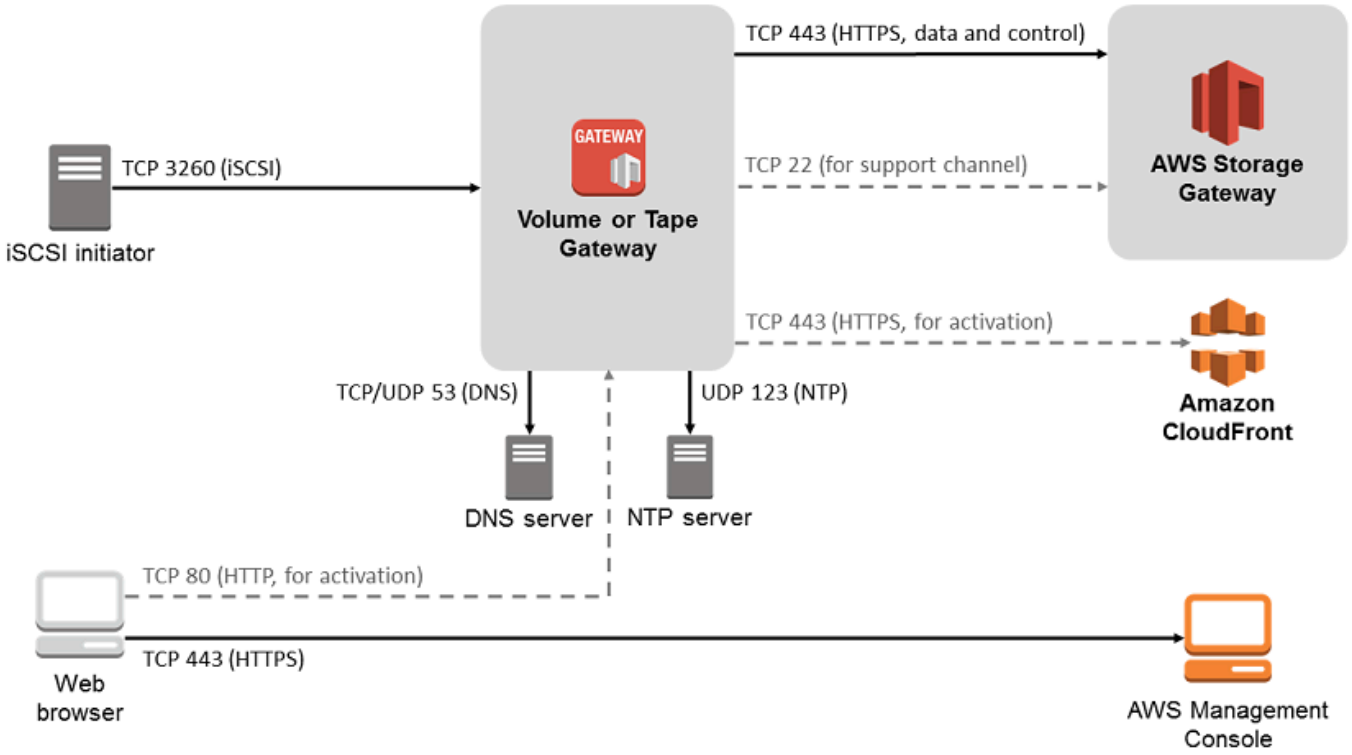
Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					iance Storage Gateway. Storage Gateway non richiede che la porta 80 sia accessibile pubblicamente. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. Se attivi il gateway dalla console di gestione Storage Gateway, l'host da cui ti colleghi alla console deve avere accesso alla porta 80 del gateway.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP/UDP	53 (DNS)	In uscita	Storage Gateway	Server DNS (Domain Name Service)	Per la comunicazione tra Storage Gateway e il server DNS.
TCP	22 (Canale di supporto)	In uscita	Storage Gateway	AWS Support	Consente di accedere AWS Support 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.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
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 volumi e di nastri virtuali

La figura seguente mostra le porte da aprire per e gateway di nastri virtuali.



Oltre alle porte comuni, i e i gateway di nastri virtuali richiedono la seguente porta.

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP	3260 (iSCSI)	In entrata	Iniziatori iSCSI	Storage Gateway	Da sistemi locali per connettersi alle destinazioni iSCSI esposte dal gateway.

Per informazioni dettagliate sui requisiti di porta, consulta Requisiti porta nella sezione Risorse aggiuntive di Storage Gateway.

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

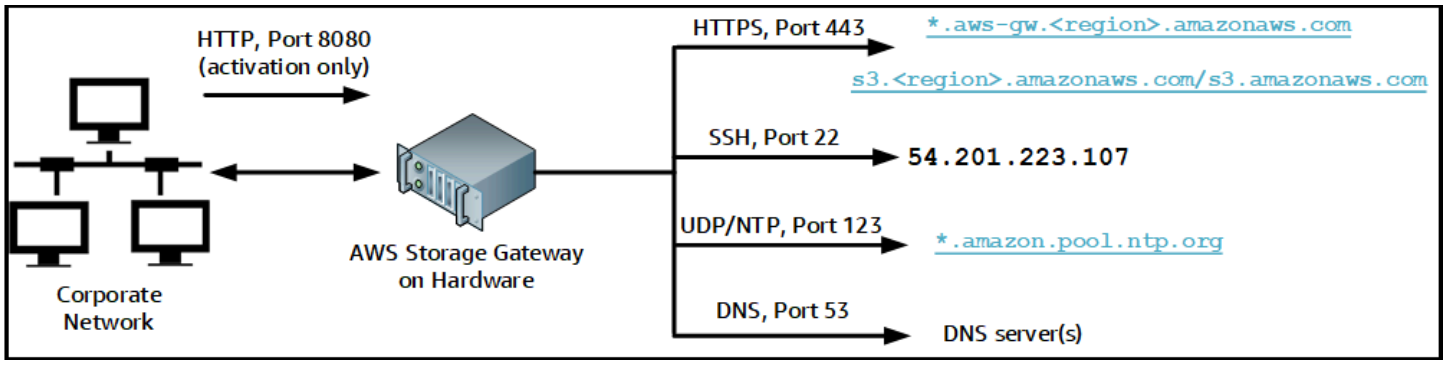
Ogni appliance hardware Storage Gateway richiede i seguenti servizi di rete:

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

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

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

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



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

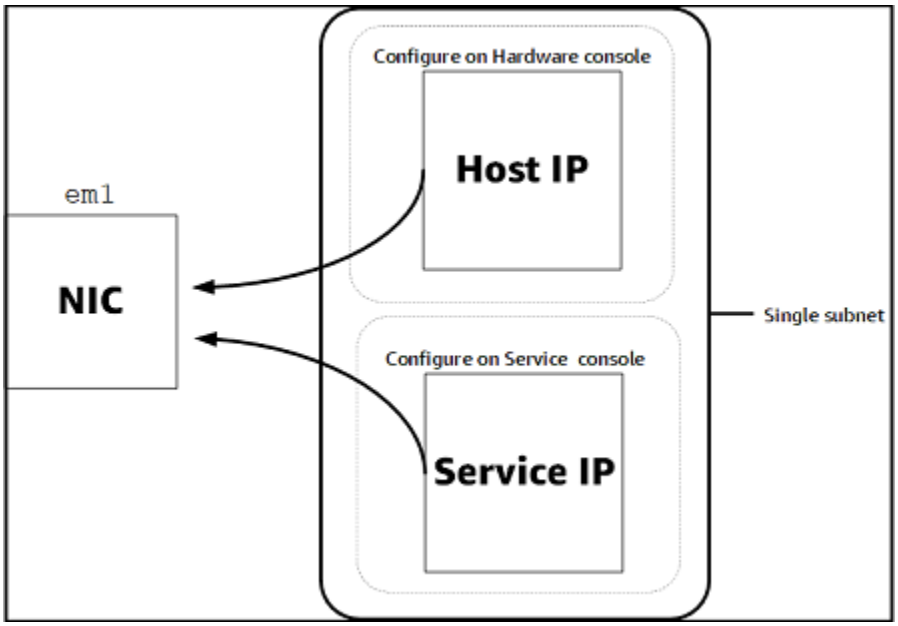
Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
SSH	22	In uscita	Appliance hardware	`54.201.223.107`	Canale di supporto
DNS	53	In uscita	Appliance hardware	Server DNS	Risoluzione dei nomi
UDP/NTP	123	In uscita	Appliance hardware	`*.amazon.pool.ntp.org`	Sincronizzazione oraria
HTTPS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

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

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

> **Note**
>
> Per visualizzare un'illustrazione che mostra la parte posteriore del server con le relative porte, consulta Montaggio su rack dell'appliance 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, consulta Utilizzo dell'appliance hardware Storage Gateway.

Consentire AWS Storage Gateway l'accesso tramite firewall e router

Il gateway richiede l'accesso ai seguenti endpoint di servizio con cui comunicare. AWS Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS.

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

> **Important**
>
> A seconda della AWS regione del gateway, sostituisci la *regione* nell'endpoint di servizio con la stringa regionale corretta.

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

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

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

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

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

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

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

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

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

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

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

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

> **Note**
>
> Se il gateway non è in grado di determinare la AWS regione in cui si trova il bucket S3, questo endpoint di servizio utilizza come impostazione predefinita. `s3.us-east-1.amazonaws.com` Si consiglia di aggiungere consentire l'accesso alla regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`) in aggiunta alle regioni AWS in cui il gateway è attivo e in cui si trova il bucket S3.

Di seguito sono riportati gli endpoint del servizio S3 per le regioni AWS GovCloud (US) .

```
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 di servizio FIPS per un bucket S3 nella regione (Stati Uniti occidentali). AWS GovCloud

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

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 AWS le regioni supportate e un elenco di endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere AWS Storage Gateway endpoint e quote nel. Riferimenti generali di AWS
- Storage Gateway Hardware Appliance: per AWS le regioni supportate che è possibile utilizzare con l'appliance hardware, vedere le aree delle appliance hardware Storage Gateway nel. Riferimenti generali di AWS

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

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 la utilizzi per la risoluzione dei problemi. AWS Support Per ulteriori informazioni, consulta Vuoi aiutarci AWS Support a risolvere i problemi del tuo 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

Puoi eseguire Storage Gateway in locale come appliance di macchina virtuale (VM) o appliance hardware fisica o come istanza AWS Amazon EC2.

> **Note**
>
> Quando un produttore termina il supporto generale per una versione di hypervisor, Storage Gateway termina anche il supporto per quella versione. Per informazioni dettagliate sul supporto per versioni specifiche di un hypervisor, consulta la documentazione del produttore.

Storage Gateway supporta le seguenti versioni di hypervisor e host:

- VMware Hypervisor ESXi (versione 7.0 o 8.0): una versione gratuita di VMware è disponibile sul sito Web VMware. Per questa configurazione, è inoltre necessario disporre di un client VMware vSphere per connettersi all'host.
- Microsoft Hypervisor Hyper-V (versione 2012 R2, 2016, 2019 o 2022): una versione standalone gratuita di Hyper-V è disponibile nella pagina Microsoft Download Center. Per questa configurazione, è necessario un Microsoft Hyper-V Manager su un computer client Microsoft Windows per connettersi all'host.
- macchina virtuale basata su kernel (KVM) Linux: una tecnologia di virtualizzazione gratuita e open-source. KVM è incluso in tutte le versioni di Linux 2.6.20 e successive. Storage Gateway è testato e supportato per le distribuzioni CentOS/RHEL 7.7, 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'Amazon Machine Image (AMI) che contiene l'immagine della macchina virtuale del gateway. Solo i file, il volume nella cache e i tipi di gateway di nastri virtuali possono essere distribuiti su Amazon EC2. Per informazioni su come distribuire un gateway su Amazon EC2, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali.
- Appliance hardware Storage Gateway: Storage Gateway fornisce un'appliance hardware fisica come opzione di implementazione on-premise per sedi con un'infrastruttura di macchine virtuali limitata.

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

Iniziatori iSCSI supportati

Quando si implementa un gateway di nastri virtuali, il gateway è preconfigurato con un'unità di sostituzione dei supporti e 10 unità a nastro. Queste unità a nastro e l'unità di sostituzione dei supporti sono disponibili per le tue applicazioni di backup client esistenti quali i dispositivi iSCSI.

Per connetterti a questi dispositivi iSCSI, Storage Gateway supporta i seguenti gli iniziatori iSCSI:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMware ESX Initiator, che fornisce un'alternativa all'utilizzo di iniziatori nei sistemi operativi guest delle tue macchine virtuali

> **Important**
>
> Storage Gateway non supporta Microsoft Multipath I/O (MPIO) tra i client Windows. Storage Gateway supporta la connessione di più host allo stesso volume se gli host coordinano l'accesso utilizzando Windows Server Failover Clustering (WSFC). Tuttavia, non

è possibile connettere più host allo stesso volume, ad esempio condividendo un file system NTFS/ext4 non clusterizzato, senza utilizzare WSFC.

Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali

Puoi usare un'applicazione di backup in lettura, scrittura e gestire i nastri con un gateway di nastri virtuali. Le seguenti applicazioni di backup di terze parti sono supportate per funzionare con gateway di nastri virtuali.

Il tipo di unità di sostituzione dei supporti scelta dipende dall'applicazione di backup che si intende utilizzare. La tabella seguente elenca le applicazioni di backup di terze parti che sono state testate e risultate compatibili con gateway di nastri virtuali. Questa tabella include il tipo di unità di sostituzione dei supporti consigliata per ogni applicazione di backup.

Applicazione di backup	Tipo di unità di sostituzione dei supporti
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` o `STK-L700`
Commvault V11	`STK-L700`
NetWorker Dell EMC 19.5	`AWS-Gateway-VTL`
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus (HPE) Data Protector 9 o 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 o 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Network 6.4 o 7.1	`STK-L700`
Quest NetVault Backup 12.4 o 13.x	`STK-L700`
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`

Applicazione di backup	Tipo di unità di sostituzione dei supporti
Veritas Backup Exec 2014 o 15 o 16 o 20 o 22.x	`AWS-Gateway-VTL`
Veritas Backup Exec 2012 **Note** Veritas ha terminato il supporto per Backup Exec 2012.	`STK-L700`
Veritas NetBackup versione 7.x o 8.x	`AWS-Gateway-VTL`

Important

Consigliamo vivamente di scegliere l'unità di sostituzione dei supporti elencata per la tua applicazione di backup. Altre unità di sostituzione dei supporti potrebbero non funzionare correttamente. Si può scegliere un'unità di sostituzione dei supporti diversa una volta attivato il gateway. Per ulteriori informazioni, consulta Selezione di un'unità di sostituzione dei supporti dopo l'attivazione del gateway.

Accedendo AWS Storage Gateway

È possibile utilizzare la Console di gestione Storage Gateway per eseguire molte 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.

Per consentire l'accesso del browser alla console Storage Gateway, assicurati che il browser abbia accesso all'endpoint dell'API Storage Gateway. Per ulteriori informazioni, consulta Endpoint e quote di Storage Gateway in Documentazione generale di riferimento di AWS .

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

Puoi anche utilizzare gli AWS SDK per sviluppare applicazioni che interagiscono con Storage Gateway. Gli SDK AWS per Java, .NET e PHP integrano l'API di Storage Gateway sottostante per

semplificare le attività di programmazione. Per ulteriori informazioni sul download delle librerie SDK, consulta Librerie e codice di esempio.

Utilizzo dell'appliance hardware Storage Gateway

L'appliance hardware Storage Gateway è un'appliance hardware fisica con il software Storage Gateway preinstallato su una configurazione server convalidata. È possibile gestire le appliance hardware dalla pagina Panoramica delle appliance hardware della console AWS Storage Gateway .

L'appliance hardware è un server 1U ad alte prestazioni che è possibile distribuire nel proprio data center oppure on-premise all'interno di un firewall aziendale. Quando si acquista e attiva l'appliance hardware, il processo di attivazione associa l'appliance hardware con il proprio account Amazon Web Services. Dopo l'attivazione, l'appliance hardware viene visualizzata nella console come un gateway nella pagina Panoramica delle appliance hardware. È possibile configurare l'appliance hardware come gateway di file, gateway di nastri virtuali 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.

Nelle sezioni seguenti, è possibile trovare istruzioni su come ordinare, configurare, attivare, avviare e utilizzare un'appliance hardware Storage Gateway.

Argomenti

Informazioni per ordinare

L'appliance AWS Storage Gateway hardware è disponibile esclusivamente presso i rivenditori. Contatta il tuo rivenditore di fiducia per informazioni sull'acquisto e per richiedere un preventivo.

Regioni supportate AWS

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

Configurazione dell'appliance hardware

Dopo aver ricevuto l'appliance hardware Storage Gateway, si utilizza la console dell'appliance hardware per configurare la rete in modo da fornire una connessione sempre attiva e attivare l'appliance. AWS L'attivazione associa l'appliance con l'account Amazon Web Services utilizzato durante il processo di attivazione. Dopo che l'appliance è attivata, è possibile avviare un gateway di file, di volumi o di nastri virtuali nella console Storage Gateway.

> **Note**
>
> È responsabilità dell'utente assicurarsi che il firmware dell'appliance hardware sia valido. up-to-date

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, consulta Montaggio su rack dell'appliance 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, consulta Configurazione dei parametri di rete.
3. Attiva l'appliance hardware nella pagina di panoramica dell'appliance hardware della console nella AWS regione di tua scelta. Per ulteriori informazioni, consulta Attivazione dell'appliance hardware.
4. Installa lo Storage Gateway sulla tua appliance hardware. Per ulteriori informazioni, consulta 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, macchina virtuale basata su kernel (KVM) Linux o Amazon EC2.

Aumento dello storage della cache utilizzabile

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

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

1. Ripristina le impostazioni di fabbrica dell'appliance hardware. Contattare Amazon Web Services Support 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 appliance ordinato, può essere fornita con una scheda di rete in rame 10G-Base-T o una scheda di rete DA/SFP+ 10G.

- 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 SFP/SFP+ in rame per 1G-Base-T o 10G-Base-T

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

Dopo aver disimballato l'appliance hardware Storage Gateway, seguire le istruzioni contenute nella confezione per montare su rack il server. L'appliance ha un fattore di forma 1U e si inserisce in un rack da 19 pollici standard conforme alla Commissione elettrotecnica internazionale (IEC).

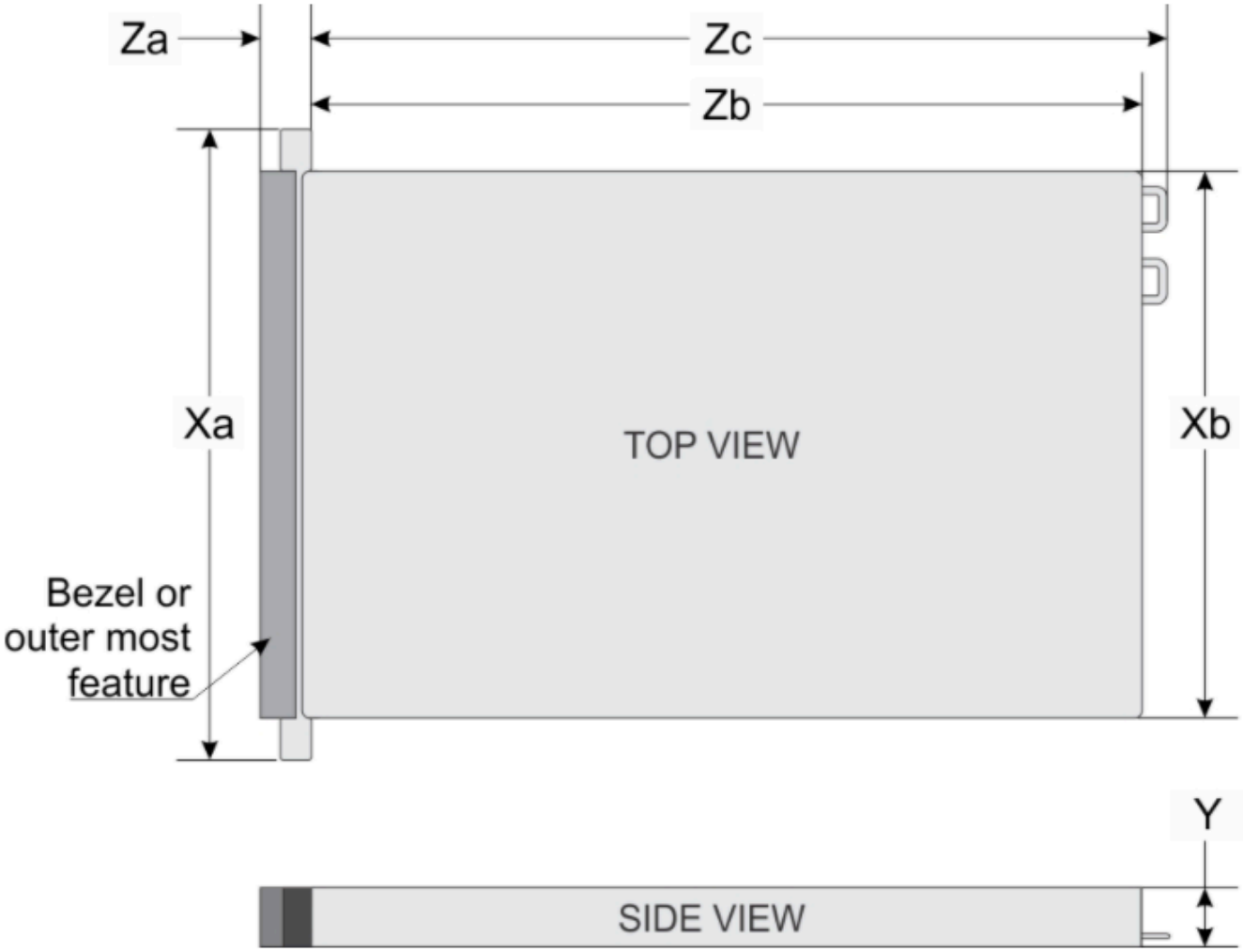
Per installare l'appliance hardware, sono necessari i seguenti componenti:

- Cavi di alimentazione: uno necessario, due consigliati.

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

Dimensioni dell'appliance hardware

dimensioni dell'appliance hardware, comprese le staffe di montaggio e la mascherina.



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)

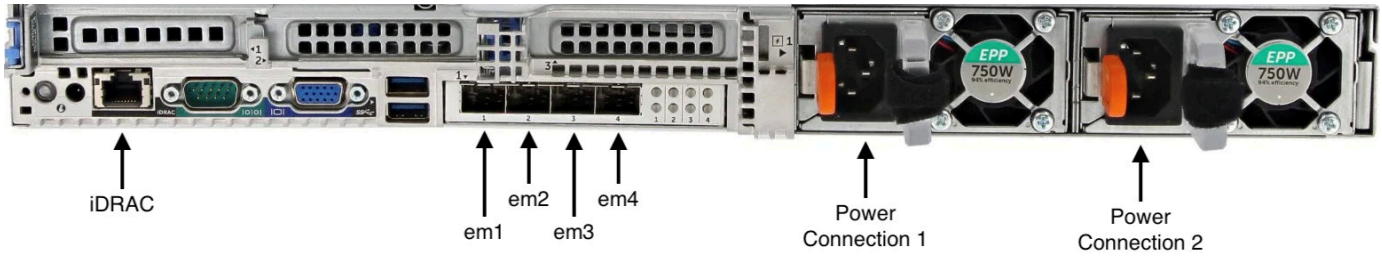
dimensioni dell'appliance hardware, comprese le staffe di montaggio e la mascherina.

Collegare il dispositivo hardware all'alimentazione

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

1. Collegare all'alimentazione ciascuno dei due alimentatori. È possibile collegare un solo alimentatore, ma si consiglia di collegare entrambi gli alimentatori.

   Nell'immagine seguente è possibile visualizzare il dispositivo hardware con i diversi collegamenti.
   appliance hardware posteriore con etichette dei connettori di rete e di alimentazione.

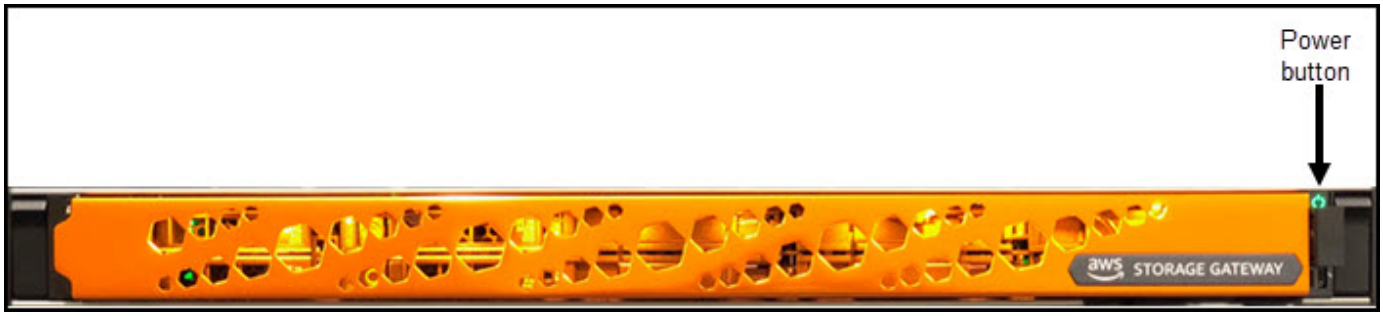
   

   appliance hardware posteriore con etichette dei connettori di rete e di alimentazione.

2. Inserire il cavo Ethernet nella porta `em1` per una connessione Internet sempre attiva. La porta `em1` è la prima delle quattro porte di rete fisiche nella parte posteriore, da sinistra a destra.

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

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



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

Dopo l'avvio del server, la console hardware viene visualizzata sul monitor. La console hardware presenta un'interfaccia utente specifica AWS che è possibile utilizzare per configurare i parametri di rete iniziali. È possibile configurare questi parametri per collegare l'appliance ad AWS e aprire un canale di supporto per la risoluzione dei problemi da parte di Amazon Web Services Support.

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.

Impostare una password per la prima volta

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

schermata di dialogo per l'impostazione della password della console dell'appliance hardware.

schermata di dialogo per l'impostazione della password della console dell'appliance hardware.

A questo punto sei nella console hardware, come mostrato di seguito.
menu principale della console dell'appliance hardware che mostra le connessioni e le opzioni di menu.

menu principale della console dell'appliance hardware che mostra le connessioni e le opzioni di menu.

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'appliance 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 connettersi ad AWS.

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.
   schermata della console dell'appliance hardware per la configurazione di rete.

schermata della console dell'appliance hardware per la configurazione di rete.

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 configuri un'altra interfaccia, questa deve fornire la stessa connessione sempre attiva agli AWS endpoint elencati nei requisiti.

schermata della console dell'appliance hardware per la configurazione della NIC su un IP statico.

schermata della console dell'appliance hardware per la configurazione della NIC su un IP statico.

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, immettilo nella pagina Hardware della AWS Storage Gateway console per attivare l'appliance hardware. Il processo di attivazione consente di verificare che il dispositivo hardware abbia le opportune credenziali di sicurezza e di registrare il dispositivo sul proprio account AWS .

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

Attivazione del dispositivo hardware per Gateway di archiviazione

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

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

2. Dal menu di navigazione a sinistra della pagina, scegli Hardware.
3. Scegli Attiva dispositivo.

4. Per Indirizzo IP, inserisci l'indirizzo IP che hai configurato per il dispositivo hardware, quindi scegli Connetti.

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

   Il fuso orario determina quando l'hardware effettua gli aggiornamenti; con l'orario pianificato per impostazione predefinita sulle 2 di notte ora locale. Idealmente, se il fuso orario è impostato correttamente, per impostazione predefinita gli aggiornamenti avverranno al di fuori dell'orario di lavoro.
7. Consulta i parametri di attivazione nella sezione relativa ai dettagli dell'apparecchiatura hardware. Puoi scegliere Precedente per tornare indietro e apportare modifiche, se necessario. Altrimenti, scegli Attiva per completare l'attivazione.

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

A questo punto, l'appliance è associata all'account. La fase successiva consiste nel configurare e avviare un Gateway di file S3, un Gateway di file FSx, un Gateway di nastri virtuali o un Gateway di volumi sul nuovo dispositivo.

Approfondimenti

Creazione di un gateway

Creazione di un gateway

È possibile creare un gateway di file S3, gateway di file FSx, gateway di nastri virtuali o gateway di volumi sull'appliance hardware.

Per creare un gateway sull'appliance hardware

1. Accedere AWS Management Console e aprire la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.

2. Scegliere Hardware.
3. Seleziona l'appliance hardware attivata su cui desideri creare il gateway, quindi scegli Crea gateway.
4. Segui le procedure descritte in Creazione del gateway per configurare, connettere e configurare il tipo di gateway scelto.

Al termine della creazione del gateway nella console Storage Gateway, il software Storage Gateway inizia automaticamente l'installazione sull'appliance hardware. È possibile che ci vogliano da 5 a 10 minuti prima che un gateway appaia come online nella 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 relativa interfaccia di rete fisica. Dopo aver attivato l'appliance e avviato lo Storage Gateway su di essa, è necessario assegnare un altro indirizzo IP alla macchina virtuale Storage Gateway in esecuzione sull'appliance hardware. Per assegnare un indirizzo IP statico a un gateway installato sull'appliance hardware, configurare l'indirizzo IP dalla console locale per il 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.

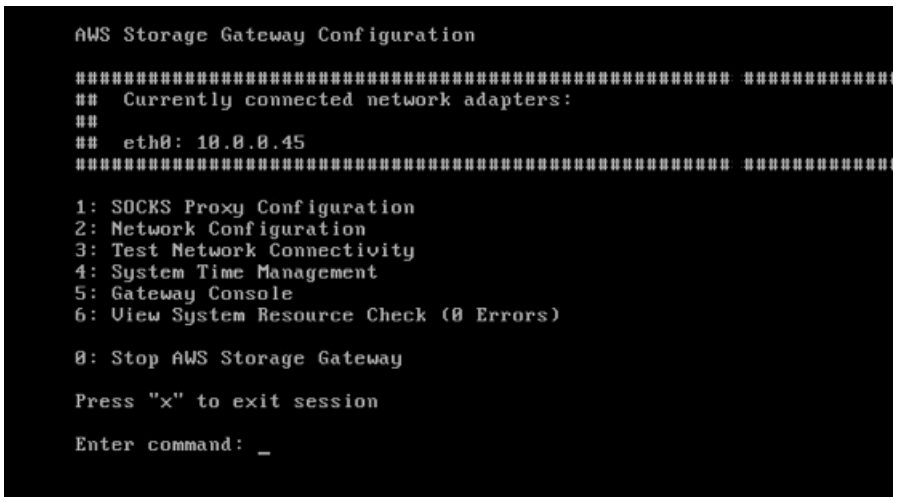
Per configurare l'indirizzo IP sull'appliance per farla funzionare con le applicazioni.

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 the section called “Impostazione della password della console locale dalla console Storage Gateway”.

5. Passare alla pagina Impostazioni di rete della console locale del gateway, come mostrato di seguito.
   pagina di configurazione della console locale del gateway che mostra le opzioni, inclusa la configurazione di rete.



   pagina di configurazione della console locale del gateway che mostra le opzioni, inclusa la configurazione di rete.

6. Digitare 2 per andare alla pagina Network Configuration (Configurazione di rete) mostrata di seguito.
   pagina di configurazione della console locale del gateway con opzioni DHCP e IP statico.

   pagina di configurazione della console locale del gateway con opzioni DHCP e IP statico.

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. Continua l'installazione nella pagina Configurazione del gateway per il tipo di gateway in uso. Per le istruzioni, consulta Configurazione del gateway di nastri virtuali e .

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.

Rimuovere un gateway da un'appliance hardware

1. Nella pagina Hardware della console Storage Gateway, scegliere l'appliance hardware che si desidera eliminare.
2. Per Actions (Operazioni), selezionare Remove Gateway (Rimuovi gateway). Viene visualizzata la finestra di dialogo di conferma.
3. Verifica di voler rimuovere il software del gateway dall'appliance hardware specificata, quindi digita la parola remove nella casella di conferma e scegli Rimuovi.

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

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

Eliminazione dell'appliance hardware

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

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

Per eliminare l'appliance hardware

1. Se è stato installato un gateway nell'appliance hardware, è necessario prima rimuovere il gateway per eliminare l'appliance. Per istruzioni su come rimuovere un gateway dall'appliance hardware, consulta Rimozione di un gateway dall'appliance hardware.
2. Nella pagina Hardware della console Storage Gateway scegliere l'appliance hardware che si desidera eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.

4. Verifica di voler eliminare l'appliance hardware specificata, quindi digita la parola delete nella casella di conferma e scegli Elimina.

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

Creazione del gateway

Gli argomenti di panoramica di questa pagina forniscono un riepilogo di alto livello di come funziona il processo di creazione dello Storage Gateway. Per step-by-step le procedure per creare un tipo specifico di gateway utilizzando la console Storage Gateway, vedere Creazione di un gateway a nastro .

Panoramica - Attivazione del gateway

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

Configurazione di un gateway

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

Connect a AWS

Il passaggio successivo consiste nel connettere il gateway a AWS. A tale scopo, devi innanzitutto scegliere il tipo di endpoint di servizio che desideri utilizzare per le comunicazioni tra l'appliance virtuale gateway e AWS i servizi nel cloud. Questo endpoint può essere accessibile dalla rete Internet pubblica o solo dall'interno del tuo Amazon VPC, dove hai il pieno controllo sulla configurazione di sicurezza della rete. È quindi necessario specificare l'indirizzo IP del gateway o la relativa chiave di attivazione, che è possibile ottenere collegandosi alla console locale sull'appliance gateway.

Rivedi e attiva

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

Panoramica - Configurazione del gateway

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

Panoramica - Risorse di archiviazione

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

Creazione di un gateway di nastri virtuali

In questa sezione, puoi trovare le istruzioni su come creare e utilizzare un gateway di nastri virtuali in AWS Storage Gateway.

Argomenti

Creazione di un gateway

In questa sezione, puoi trovare le istruzioni su come scaricare, distribuire e attivare un gateway di nastri virtuali standard.

Argomenti

- Connect Tape Gateway a AWS
- Revisione delle impostazioni e attivazione del gateway di nastri virtuali
- Configurazione del gateway di nastri virtuali

Configurare un gateway di nastri virtuali

Per configurare un nuovo gateway di nastri virtuali

1. Apri AWS Management Console https://console.aws.amazon.com/storagegateway/home/ e scegli Regione AWS dove vuoi creare il tuo gateway.
2. Scegli Crea gateway per aprire la pagina Configura gateway.
3. Nella sezione Impostazioni gateway, procedi nel seguente modo:
   a. Per Gateway name (Nome gateway), inserire un nome per il gateway. È possibile cercare questo nome per trovare il gateway nelle pagine di elenco della console Storage Gateway.
   b. Per il fuso orario del gateway, scegli il fuso orario locale per la parte del mondo in cui desideri implementare il gateway.
4. Nella sezione Opzioni gateway, per Tipo di gateway, scegli gateway di nastri virtuali.
5. Nella sezione Opzioni piattaforma, procedi nel modo seguente:
   a. Per Piattaforma host, scegli la piattaforma su cui desideri implementare il gateway, quindi segui 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: scarica, implementa e configura la macchina virtuale gateway utilizzando VMware ESXi.
      - Microsoft Hyper-V: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Microsoft Hyper-V.
      - Linux KVM: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Linux KVM.
      - Amazon EC2: configura e avvia un'istanza Amazon EC2 per ospitare il tuo gateway. Questa opzione non è disponibile per i gateway di volumi archiviati.
      - Dispositivo hardware: ordina un dispositivo hardware fisico dedicato da AWS cui ospitare il gateway.

b. Per Conferma la configurazione del gateway, seleziona la casella di controllo per confermare di aver eseguito i passaggi di implementazione per la piattaforma host scelta. Questo passaggio non è applicabile alla piattaforma host dell'appliance hardware.

6. Nella sezione Impostazioni dell'applicazione di backup, per Applicazione di backup, scegli l'applicazione che desideri utilizzare per eseguire il backup dei dati del nastro sui nastri virtuali associati al gateway di nastri virtuali.
7. Scegli Successivo per continuare.

Ora che il gateway è configurato, devi scegliere come connetterlo e comunicare. AWS Per istruzioni, consulta Connect your Tape Gateway a AWS.

Connect Tape Gateway a AWS

Per connettere un nuovo Tape Gateway a AWS

1. Completa la procedura descritta in Configurazione di un gateway di nastri virtuali se non l'hai già fatto. Al termine, scegliere Avanti per aprire la AWS pagina Connect to nella console Storage Gateway.
2. Nella sezione Opzioni endpoint, per Service endpoint, scegli il tipo di endpoint con cui il gateway utilizzerà per comunicare. AWS Puoi scegliere tra le seguenti opzioni:

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

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

   - VPC ospitato: il gateway comunica AWS tramite una connessione privata con il VPC, consentendoti di controllare le impostazioni di rete. Se si seleziona questa opzione, è

necessario specificare un endpoint VPC esistente scegliendo l'ID dell'endpoint VPC dal menu a discesa o fornendo il nome DNS o l'indirizzo IP dell'endpoint VPC.

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

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

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

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

4. Scegli Successivo per continuare.

Ora che hai scelto la modalità di connessione del gateway, devi attivare il gateway. AWS Per le istruzioni, consulta Revisione delle impostazioni e attivazione del gateway di nastri virtuali.

Revisione delle impostazioni e attivazione del gateway di nastri virtuali

Per attivare un nuovo gateway di nastri virtuali

1. Se non è già stato fatto, completare le procedure descritte negli argomenti seguenti:

   - Configurare un gateway di nastri virtuali
   - Connect Tape Gateway a AWS

   Al termine, scegliere Avanti per aprire la pagina Rivedi e attiva nella console Storage Gateway.

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

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

4. Scegli Attiva gateway per procedere.

Ora che hai attivato il gateway, devi eseguire la prima configurazione per allocare i dischi di archiviazione locali e configurare la registrazione. Per le istruzioni, consulta Configurazione del gateway di nastri virtuali.

Configurazione del gateway di nastri virtuali

Per eseguire la prima configurazione su un nuovo gateway di nastri virtuali

1. Se non è già stato fatto, completare le procedure descritte negli argomenti seguenti:

   - Configurare un gateway di nastri virtuali
   - Connect Tape Gateway a AWS
   - Rivedi le impostazioni e attiva il gateway di nastri virtuali

   Al termine, scegliere Avanti per aprire la pagina Configura gateway nella console Storage Gateway.
2. Nella sezione Configura storage, utilizza i menu a discesa per allocare almeno un disco con almeno 165 GiB di capacità per CACHE STORAGE e almeno un disco con almeno 150 GiB di capacità per UPLOAD BUFFER. I dischi locali elencati in questa sezione corrispondono allo spazio di archiviazione fisico fornito sulla piattaforma host.
3. Nella sezione dei gruppi di CloudWatch log, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del tuo gateway. Puoi scegliere tra le seguenti opzioni:

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

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

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

     > **Note**
     >
     > Questa funzionalità richiede le autorizzazioni relative alle CloudWatch policy, che non vengono concesse automaticamente come parte della policy di accesso completo preconfigurata di Storage Gateway. Assicurati che la tua politica di sicurezza conceda le seguenti autorizzazioni prima di tentare di creare allarmi consigliati: CloudWatch
     >
     > - `cloudwatch:PutMetricAlarm` - crea allarmi
     > - `cloudwatch:DisableAlarmActions`- disattiva le azioni di allarme
     > - `cloudwatch:EnableAlarmActions`- attiva le azioni di allarme
     > - `cloudwatch:DeleteAlarms` - elimina allarmi

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

5. (Facoltativo) Nella sezione Tag, scegli Aggiungi nuovo tag, quindi inserisci una coppia chiave-valore con distinzione tra maiuscole e minuscole per aiutarti a cercare e filtrare il gateway nelle pagine di elenco nella console Storage Gateway. Ripeti questo passaggio per aggiungere quanti tag necessiti.
6. Scegli Configura per completare la creazione del gateway.

   Per verificare lo stato del nuovo gateway, cercalo nella pagina di panoramica del gateway dello Storage Gateway.

Dopo aver creato il gateway, è necessario creare nastri virtuali da utilizzare. Per le istruzioni, consulta Creazione di nastri.

Creazione di un pool di nastri personalizzato

In questa sezione viene descritto come creare un nuovo pool di nastri personalizzati in AWS Storage Gateway.

Argomenti

Scelta di un tipo di pool di nastri

AWS Storage Gateway utilizza i pool di nastri per determinare la classe di storage in cui archiviare i nastri quando vengono espulsi. Storage Gateway offre due pool di nastri standard:

- Glacier Pool: archivia il nastro nella classe di archiviazione S3 Glacier Flexible Retrieval. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per più archivi attivi in cui è possibile recuperare i nastri, generalmente entro 3-5 ore. Per ulteriori informazioni, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.
- Deep Archive Pool: archivia il nastro nella classe di archiviazione S3 Glacier Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. È possibile recuperare i nastri archiviati in S3 Glacier Deep Archive, generalmente entro 12 ore. Per informazioni dettagliate, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.

Se si archivia un nastro in S3 Glacier Flexible Retrieval, è possibile spostarlo in S3 Glacier Deep Archive in un secondo momento. Per ulteriori informazioni, consulta Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive.

Storage Gateway supporta anche la creazione di pool di nastri personalizzati, che consentono di attivare il blocco della conservazione dei nastri per impedire che i nastri archiviati vengano eliminati o spostati in un altro pool per un periodo di tempo fisso, fino a 100 anni. Ciò include il blocco dei controlli di autorizzazione su chi può eliminare i nastri o modificare le impostazioni di conservazione.

Utilizzo del blocco di conservazione dei nastri

Con il blocco di conservazione dei nastri, è possibile bloccare i nastri archiviati. Il blocco di conservazione dei nastri è un'opzione per i nastri in un pool di nastri personalizzato. I nastri con il blocco di conservazione dei nastri attivato non possono essere eliminati o spostati in un altro pool per un periodo di tempo prestabilito, fino a 100 anni.

È possibile configurare il blocco di conservazione dei nastri in una delle due modalità seguenti:

- Modalità di governance: se configurati in modalità di governance, solo gli utenti AWS Identity and Access Management (IAM) con le autorizzazioni necessarie `storagegateway:BypassGovernanceRetention` possono rimuovere i nastri dal pool. Se utilizzi l' AWS Storage Gateway API per rimuovere il nastro, devi anche impostare su`BypassGovernanceRetention`. `true`
- Modalità di conformità: se configurato in modalità di conformità, la protezione non può essere rimossa da nessun utente, incluso l' Account AWS root.

  Quando un nastro è bloccato in modalità conformità, il relativo tipo di blocco di conservazione non può essere modificato e il periodo di conservazione non può essere abbreviato. Il tipo di blocco in modalità conformità garantisce che un nastro non possa essere sovrascritto o eliminato per tutta la durata del periodo di conservazione.

> **Important**
>
> La configurazione di un pool personalizzato non può essere modificata dopo la sua creazione.

È possibile attivare il blocco di conservazione dei nastri quando si crea un pool di nastri personalizzato. Tutti i nuovi nastri collegati a un pool personalizzato ereditano il tipo di blocco di conservazione, il periodo e la classe di archiviazione per quel pool.

È inoltre possibile attivare il blocco di conservazione dei nastri sui nastri archiviati prima del rilascio di questa funzionalità spostando i nastri tra il pool predefinito e un pool personalizzato creato dall'utente. Se il nastro è archiviato, il blocco di conservazione dei nastri ha effetto immediato.

> **Note**
>
> Se trasferisci nastri archiviati tra le classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, ti viene addebitato un costo per lo spostamento del nastro. Non sono previsti costi aggiuntivi per spostare un nastro da un pool predefinito a un pool personalizzato se la classe di archiviazione rimane la stessa.

Creazione di un pool di nastri personalizzato

Utilizza i seguenti passaggi per creare un pool di nastri personalizzato usando la console AWS Storage Gateway .

Per creare un pool di nastri personalizzato

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione a sinistra, scegliere la scheda Libreria di nastri e quindi la scheda Pool.
3. Scegliere Crea pool per aprire il pannello Crea pool.
4. In Nome, inserisci un nome univoco per identificare il tuo pool di nastri personalizzato. Il nome del pool deve contenere da 2 a 100 caratteri.
5. Per Classe di archiviazione, scegli Glacier o Glacier Deep Archive.
6. Per Tipo di blocco di conservazione, scegli Nessuno, Conformita o Governance.

   > **Note**
   >
   > Se scegli Conformità, il blocco di conservazione dei nastri non può essere rimosso da nessun utente, incluso l' Account AWS root.

7. Se scegli un tipo di blocco di conservazione dei nastri, inserisci il Periodo di conservazione in giorni. Il periodo massimo di conservazione è 36.500 giorni (100 anni).
8. (Facoltativo) Per Tag, scegli Aggiungi nuovo tag per aggiungere un tag al tuo pool di nastri personalizzato. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare i pool di nastri personalizzato.

Inserire una Chiave e, facoltativamente, un Valore per il tag. Puoi aggiungere fino a 50 tag al pool di nastri.

9. Scegli Crea pool per creare il tuo nuovo pool di nastri personalizzato.

Creazione di nastri

In questa sezione viene descritto come creare nuovi nastri virtuali usando AWS Storage Gateway. È possibile creare nuovi nastri virtuali manualmente utilizzando la AWS Storage Gateway console o l'API Storage Gateway. È inoltre possibile configurare il gateway di nastri virtuali per crearli automaticamente, il che aiuta a ridurre la necessità di una gestione manuale dei nastri, semplifica le installazioni di grandi dimensioni e aiuta a dimensionare le esigenze di storage on-premise e di archiviazione.

Il gateway di nastri virtuali supporta write-once-read-many (WORM) e blocco di conservazione dei nastri su nastri virtuali. I nastri virtuali attivati da WORM aiutano a garantire che i dati sui nastri attivi nella libreria di nastri virtuali non possano essere sovrascritti o cancellati. Per ulteriori informazioni sulla protezione WORM per nastri virtuali, vedere la sezione seguente,. the section called “Protezione su nastro WORM”

Con Tape Retention Lock, è possibile specificare la modalità e il periodo di conservazione sui nastri virtuali archiviati, evitando che vengano eliminati per un periodo di tempo fisso fino a 100 anni. Include controlli di autorizzazione su chi può eliminare i nastri o modificare le impostazioni di conservazione. Per ulteriori informazioni sul recupero di nastri, consulta the section called “Blocco di conservazione dei nastri”.

> **Note**
>
> Il costo viene calcolato solo per la quantità di dati scritti nel nastro e non per la capacità del nastro.
> Puoi usare AWS Key Management Service (AWS KMS) per crittografare i dati scritti su un nastro virtuale archiviato in Amazon Simple Storage Service (Amazon S3). Attualmente, puoi farlo utilizzando l' AWS Storage Gateway API o AWS Command Line Interface ()AWS CLI. Per ulteriori informazioni, consulta CreateTapeso create-tapes.

Argomenti

- Protezione su nastro WORM (Write Once, Read Many)
- Creazione manuale di nastri
- Consentire la creazione automatica di nastri

Protezione su nastro WORM (Write Once, Read Many)

È possibile impedire la sovrascrittura o la cancellazione dei nastri virtuali attivando la protezione WORM per i nastri virtuali in. AWS Storage Gateway La protezione WORM per nastri virtuali viene attivata durante la creazione di nastri.

I dati scritti su nastri virtuali WORM non possono essere sovrascritti. Solo i nuovi dati possono essere aggiunti ai nastri virtuali WORM e i dati esistenti non possono essere cancellati. L'attivazione della protezione WORM per i nastri virtuali consente di proteggere tali nastri mentre sono in uso attivo, prima che vengano espulsi e archiviati.

La configurazione WORM può essere impostata solo al momento della creazione dei nastri e tale configurazione non può essere modificata dopo la creazione dei nastri.

Creazione manuale di nastri

È possibile creare nuovi nastri virtuali manualmente utilizzando la AWS Storage Gateway console o l'API Storage Gateway. La console offre una comoda interfaccia per la creazione di nastri con la flessibilità di specificare un prefisso per un codice a barre a nastro generato casualmente. Se è necessario personalizzare completamente i codici a barre del nastro (ad esempio, in modo che corrispondano al numero di serie di un nastro fisico corrispondente), è necessario utilizzare l'API. Per ulteriori informazioni sulla creazione di nastri utilizzando l'API Storage Gateway, vedere CreateTapeWithBarcodelo Storage Gateway API Reference.

Per creare nastri virtuali manualmente utilizzando la console Storage Gateway

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere la scheda Gateways (Gateway).
3. Scegliere Create tapes (Crea nastri) per aprire la finestra di dialogo Create tapes (Crea nastri).
4. Per Gateway, scegliere un gateway. Il nastro viene creato per questo gateway.
5. Per Tipo di nastro, scegli Standard per creare nastri virtuali standard. Scegliete WORM per creare nastri virtuali WORM (Write Once Read Many).

6. Per Number of tapes (Numero di nastri), scegliere il numero di nastri che si vuole creare. Per ulteriori informazioni sulle quote dei nastri, consulta AWS Storage Gateway quote.
7. In Capacità, immettere le dimensioni del nastro virtuale che si desidera creare. I nastri devono avere dimensioni maggiori di 100 GiB. Per informazioni sulle quote di capacità, consulta AWS Storage Gateway quote.
8. In Barcode prefix (Prefisso codice a barre), digitare il prefisso che si vuole aggiungere al codice a barre dei nastri virtuali.

   > **Note**
   >
   > I nastri virtuali sono identificati in modo univoco da un codice a barre ed è possibile aggiungere un prefisso al codice a barre. E' possibile utilizzare un prefisso per identificare meglio i nastri virtuali. Il prefisso deve contenere lettere maiuscole (A–Z) e deve essere costituito da uno a quattro caratteri.

9. Per Pool, scegli Glacier Pool, Deep Archive Pool o un pool personalizzato che hai creato. Questo pool rappresenta la classe di storage in cui il nastro sarà archiviato quando viene espulso dal software di backup.

   - Scegli Glacier Pool se desideri archiviare il nastro nella classe di archiviazione S3 Glacier Flexible Retrieval. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per più archivi attivi in cui è possibile recuperare un nastro, generalmente entro 3-5 ore. Per ulteriori informazioni, consulta Classi di archiviazione nella Guida per l'utente di Amazon Simple Storage Service.
   - Scegliere Deep Archive Pool se si desidera archiviare il nastro nella classe di archiviazione S3 Glacier Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore. Per ulteriori informazioni , consulta Classi di archiviazione nella Guida per l'utente di Amazon Simple Storage Service.
   - Scegli un pool personalizzato, se disponibile. Puoi configurare pool di nastri personalizzati per utilizzare Deep Archive Pool o Glacier Pool. I nastri vengono archiviati nella classe di storage configurata quando vengono espulsi dal software di backup.

Se si archivia un nastro in S3 Glacier Flexible Retrieval, è possibile spostarlo in S3 Glacier Deep Archive in un secondo momento. Per ulteriori informazioni, consulta Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive.

> **Note**
>
> I nastri creati prima del 27 marzo 2019 sono archiviati direttamente in S3 Glacier Flexible Retrieval quando il software di backup li espelle.

10. (Facoltativo) Per Tags scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag al tuo nastro. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare i nastri.
11. Scegliere Create tapes (Crea nastri).
12. Nel riquadro di navigazione, scegliere Tape Library (Libreria di nastri) e scegliere Tapes (Nastri) per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.

Lo stato dei nastri virtuali è inizialmente impostato su CREATING (CREAZIONE IN CORSO) quando i nastri virtuali sono in fase di creazione. Al termine della creazione, lo stato dei nastri passa a AVAILABLE (DISPONIBILE). Per ulteriori informazioni, consulta Gestione del gateway di nastri virtuali.

Consentire la creazione automatica di nastri

Il gateway di nastri virtuali può creare automaticamente nuovi nastri virtuali per mantenere il numero minimo di nastri disponibili configurati. Quindi rende questi nuovi nastri disponibili per l'importazione dall'applicazione di backup in modo che i processi di backup possano essere eseguiti senza interruzioni. La creazione automatica di nastri elimina la necessità di script personalizzati oltre al processo manuale di creazione di nuovi nastri virtuali.

Il gateway di nastri virtuali genera automaticamente un nuovo nastro quando ha un numero inferiore di nastri rispetto al numero minimo di nastri disponibili specificato per la creazione automatica del nastro. Un nuovo nastro viene generato quando:

- Un nastro viene importato da uno slot di importazione/esportazione.
- Un nastro viene importato nell'unità nastro.

Il gateway mantiene un numero minimo di nastri con il prefisso del codice a barre specificato nella politica di creazione automatica del nastro. Se il numero di nastri è inferiore al numero minimo di nastri con il prefisso del codice a barre, il gateway crea automaticamente un numero sufficiente di nuovi nastri pari al numero minimo di nastri specificato nella politica di creazione automatica del nastro.

Quando si espelle un nastro e questo entra nello slot di importazione/esportazione, quel nastro non viene conteggiato ai fini del numero minimo di nastri specificato nella politica di creazione automatica del nastro. Solo i nastri nello slot di importazione/esportazione vengono considerati "disponibili". L'esportazione di un nastro non avvia la creazione automatica del nastro. Solo le importazioni influiscono sul numero di nastri disponibili.

Lo spostamento di un nastro dallo slot di importazione/esportazione a un'unità nastro o a uno slot di archiviazione riduce il numero di nastri nello slot di importazione/esportazione con lo stesso prefisso di codice a barre. Il gateway crea nuovi nastri per mantenere il numero minimo di nastri disponibili per quel prefisso del codice a barre.

Per consentire la creazione automatica di nastri

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere la scheda Gateways (Gateway).
3. Scegliere il gateway per il quale si desidera creare automaticamente i nastri.
4. Nel menu Azioni, scegli Configura la creazione automatica del nastro.

   Viene visualizzata la pagina di creazione automatica del nastro. Qui è possibile configurare, modificare o eliminare le opzioni di creazione automatica del nastro.
5. Per consentire la creazione automatica del nastro, scegli Aggiungi nuovo elemento, quindi configura le impostazioni per la creazione automatica del nastro.
6. Per Tipo di nastro, scegli Standard per creare nastri virtuali standard. Scegli WORM per creare nastri virtuali write-once-read-many(WORM).
7. In Numero minimo di nastri, immettere il numero minimo di nastri virtuali che devono essere sempre disponibili sul gateway di nastri virtuali. L'intervallo valido per questo valore è un minimo di 1 e un massimo di 10.

8. Per Capacità, immettere la dimensione, in byte, della capacità del nastro virtuale. L'intervallo valido è un minimo di 100 Gib e un massimo di 15 TiB.
9. In Barcode prefix (Prefisso codice a barre), digitare il prefisso che si vuole aggiungere al codice a barre dei nastri virtuali.

   > **Note**
   >
   > I nastri virtuali sono identificati in modo univoco da un codice a barre ed è possibile aggiungere un prefisso al codice a barre. Il prefisso è facoltativo, ma può essere usato per identificare meglio i nastri virtuali. Il prefisso deve contenere lettere maiuscole (A–Z) e deve essere costituito da uno a quattro caratteri.

10. Per Pool, scegli Glacier Pool, Deep Archive Pool o un pool personalizzato che hai creato. Questo pool rappresenta la classe di storage in cui il nastro sarà archiviato quando viene espulso dal software di backup.

    - Scegli Glacier Pool se desideri archiviare il nastro nella classe di archiviazione S3 Glacier Flexible Retrieval. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per più archivi attivi in cui è possibile recuperare un nastro, generalmente entro 3-5 ore. Per ulteriori informazioni, consulta Classi di archiviazione nella Guida per l'utente di Amazon Simple Storage Service.
    - Scegliere Deep Archive Pool se si desidera archiviare il nastro nella classe di archiviazione S3 Glacier Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore. Per ulteriori informazioni , consulta Classi di archiviazione nella Guida per l'utente di Amazon Simple Storage Service.
    - Scegli un pool personalizzato, se disponibile. Puoi configurare pool di nastri personalizzati per utilizzare Deep Archive Pool o Glacier Pool. I nastri vengono archiviati nella classe di storage configurata quando vengono espulsi dal software di backup.

    Se si archivia un nastro in S3 Glacier Flexible Retrieval, è possibile spostarlo in S3 Glacier Deep Archive in un secondo momento. Per ulteriori informazioni, consulta Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive.

> **Note**
>
> I nastri creati prima del 27 marzo 2019 sono archiviati direttamente in S3 Glacier Flexible Retrieval quando il software di backup li espelle.

11. Al termine della configurazione delle impostazioni, scegli Salva modifiche.
12. Nel riquadro di navigazione, scegliere Tape Library (Libreria di nastri) e scegliere Tapes (Nastri) per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.

    Lo stato dei nastri virtuali è inizialmente impostato su CREATING (CREAZIONE IN CORSO) quando i nastri virtuali sono in fase di creazione. Al termine della creazione, lo stato dei nastri passa a AVAILABLE (DISPONIBILE). Per ulteriori informazioni, consulta Gestione del gateway di nastri virtuali.

    Per ulteriori informazioni sulla modifica dei criteri di creazione automatica dei nastri o sull'eliminazione della creazione automatica di nastri da un gateway di nastri virtuali, vedere Gestione della creazione automatica di nastri.

Fase successiva

Utilizzo del gateway di nastri virtuali

Utilizzo del gateway di nastri virtuali

Di seguito sono disponibili istruzioni su come usare il gateway di nastri virtuali.

Argomenti

- Connessione dei dispositivi VTL
- Utilizzo del software di backup per testare la configurazione del gateway
- Cosa fare in seguito?

Connessione dei dispositivi VTL

Di seguito vengono fornite le istruzioni su come connettere i dispositivi VTL (Virtual Tape Library, libreria di nastri virtuali) al client Microsoft Windows o Red Hat Enterprise Linux (RHEL).

Argomenti

Connessione a un client Microsoft Windows

La procedura seguente mostra un riepilogo delle operazioni da eseguire per connettersi a un client Windows.

Per connettere i dispositivi VTL a un client Windows

1. Avvia `iscsicpl.exe`.

   > **Note**
   >
   > Per eseguire l'iniziatore iSCSI, è necessario disporre di diritti di amministratore nel computer client.

2. Avviare il servizio iniziatore iSCSI Microsoft.
3. Nella finestra di dialogo iSCSI Initiator Properties (Proprietà iniziatore iSCSI) scegliere la scheda Discovery (Individuazione) e quindi scegliere Discover Portal (Individua portale).
4. Specificare l'indirizzo IP del gateway di nastri virtuali in Indirizzo IP o nome DNS.
5. Scegliere la scheda Targets (Destinazioni) e quindi scegliere Refresh (Aggiorna). Le 10 unità nastro e l'unità di sostituzione dei supporti verranno visualizzate nella casella Discovered targets (Destinazioni individuate). Lo stato della destinazione è Inactive (Inattivo).
6. Scegliere il primo dispositivo e connettersi. I dispositivi devono essere connessi uno per volta.
7. Connettere tutte le destinazioni.

In un client Windows il fornitore di driver per l'unità nastro deve essere Microsoft. Usare la procedura seguente per verificare il fornitore di driver e aggiornare il driver e il fornitore, se necessario:

Per verificare e aggiornare il driver e il fornitore

1. Nel client Windows avviare Gestione dispositivi.
2. Espandere Tape drives (Unità nastro), aprire il menu contestuale (clic con il pulsante destro del mouse) per un'unità nastro e scegliere Properties (Proprietà).
3. Nella scheda Driver della finestra di dialogo Device Properties (Proprietà dispositivo) verificare che per Driver Provider (Fornitore driver) sia indicato Microsoft.
4. Se in Driver Provider (Fornitore driver) non è indicato Microsoft, impostare il valore come illustrato di seguito:
   a. Scegliere Update Driver (Aggiorna driver).
   b. Nella finestra di dialogo Update Driver Software (Aggiornamento software driver) scegliere Browse my computer for driver software (Cerca software driver nel computer).
   c. Nella finestra di dialogo Update Driver Software (Aggiornamento software driver) scegliere Let me pick from a list of device drivers on my computer (Seleziona da un elenco di driver di dispositivo nel computer).
   d. Scegliere LTO Tape drive (Unità nastro LTO) e quindi Next (Avanti).
5. Scegliere Close (Chiudi) per chiudere la finestra Update Driver Software (Aggiornamento software driver) e verificare che il valore di Driver Provider (Fornitore driver) sia ora impostato su Microsoft.
6. Ripetere la procedura per aggiornare il driver e il fornitore per tutte le unità nastro.

Connessione a un client Linux

La procedura seguente mostra un riepilogo delle operazioni da eseguire per connettersi a un client RHEL.

Per connettere i dispositivi VTL a un client Linux

1. Installare il pacchetto RPM `iscsi-initiator-utils`.

   Puoi utilizzare il seguente comando per installare il pacchetto.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Assicurati che il daemon iSCSI sia in esecuzione.

Per RHEL 5 o 6, utilizzare il seguente comando.

```
sudo /etc/init.d/iscsi status
```

Per RHEL 7, utilizzare il seguente comando.

```
sudo service iscsid status
```

3. Scopri il volume ole destinazioni del dispositivo VTL definiti per un gateway. Utilizzare il seguente comando di individuazione.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

L'output del comando di individuazione sarà simile all'output di esempio seguente.

Per i gateway di volumi: `[GATEWAY_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume`

Per i gateway di nastri virtuali: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

4. Connessione a una destinazione.

Specificare il valore di *[GATEWAY_IP]* corretto e l'IQN nel comando di connessione.

Utilizza il seguente comando.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Verificare che il volume sia collegato al computer client (l'iniziatore). A tale scopo, utilizzare il comando seguente.

```
ls -l /dev/disk/by-path
```

L'output del comando dovrebbe essere simile all'output di esempio seguente.

`lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda`

Per i gateway di volumi è consigliabile personalizzare le impostazioni iSCSI dopo aver configurato l'iniziatore, come illustrato in Personalizzazione delle impostazioni iSCSI di Linux.

Verificare che il dispositivo VTL sia collegato al computer client (l'iniziatore). A tale scopo, utilizzare il comando seguente.

```
ls -l /dev/tape/by-path
```

L'output del comando dovrebbe essere simile all'output di esempio seguente.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
```

```
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
 -> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
 -> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
 -> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
 -> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
 -> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```

Fase successiva

[Utilizzo del software di backup per testare la configurazione del gateway]

Utilizzo del software di backup per testare la configurazione del gateway

Per testare la tua configurazione del gateway di nastri virtuali, segui questa procedura utilizzando l'applicazione di backup:

1. Configurare l'applicazione di backup per rilevare i dispositivi di storage.

   > **Note**
   >
   > Per migliorare le prestazioni I/O, ti consigliamo di impostare la dimensione del blocco delle unità nastro nella tua applicazione di backup su 1 MB. Per ulteriori informazioni, consulta Utilizzare una dimensione del blocco maggiore per le unità nastro.

2. Backup dei dati su nastro.
3. Archiviazione del nastro.
4. Recupero del nastro dall'archivio.
5. Ripristino dei dati dal nastro.

Per testare la configurazione, usare un'applicazione di backup compatibile, come descritto di seguito.

> **Note**
>
> Salvo diversamente specificato, tutte le applicazioni di backup sono state qualificate su Microsoft Windows.

Argomenti

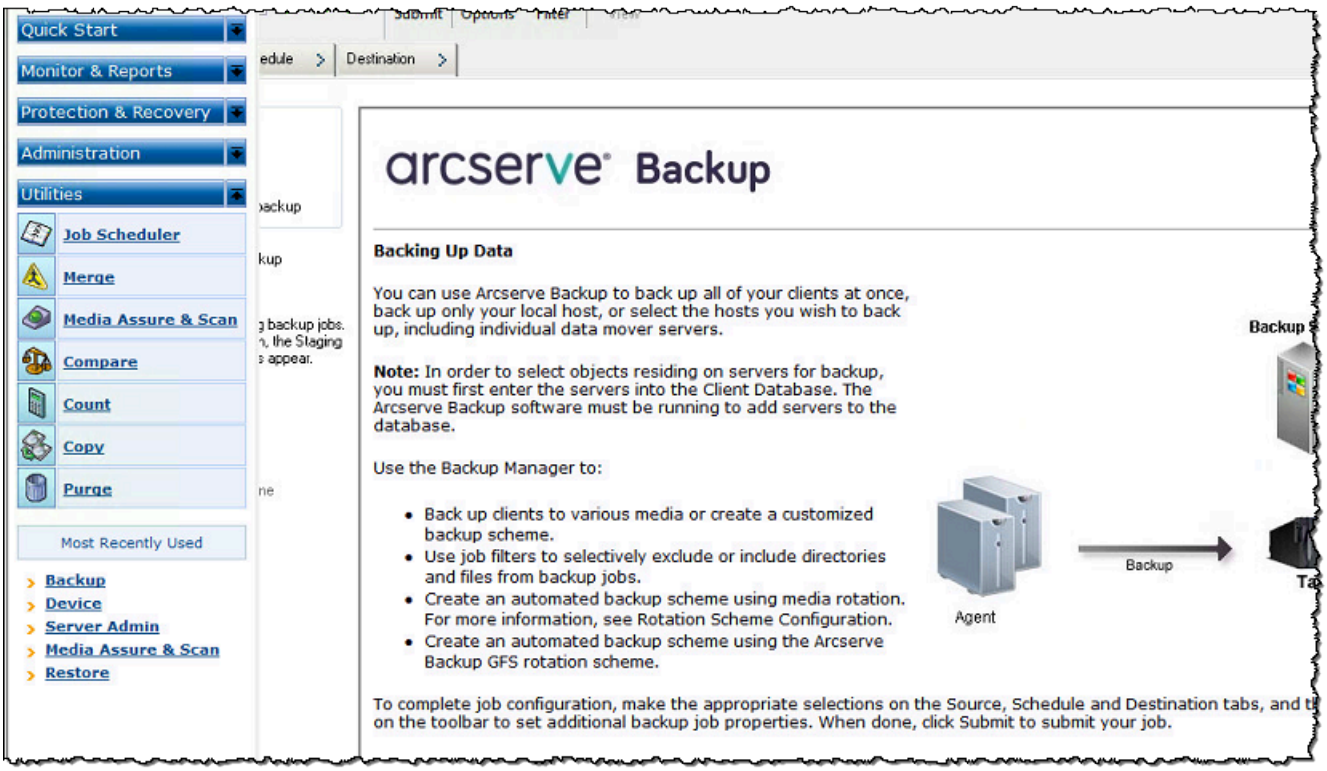
- Test della configurazione utilizzando Quest NetVault Backup
- Test della configurazione tramite Veeam Backup & Replication
- Test della configurazione tramite Veritas Backup Exec
- Test della configurazione utilizzando Veritas NetBackup

Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Test della configurazione tramite Arcserve Backup r17.0

Puoi eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi della libreria di nastri virtuali (VTL) utilizzando Arcserve Backup r17.0. In questo argomento viene illustrata la documentazione di base per configurare Arcserve Backup con un gateway di nastri virtuali ed eseguire un'operazione di backup e ripristino. Per informazioni dettagliate su come usare Arcserve Backup r17.0, consulta la documentazione di Arcserve Backup r17 nella guida per l'amministrazione di Arcserve.

Lo screenshot seguente mostra i menu di Arcserve.



Argomenti

- Configurazione di Arcserve per l'uso con i dispositivi VTL
- Caricamento di nastri in un pool di supporti
- Backup dei dati su nastro
- Archiviazione di un nastro
- Ripristino dei dati da un nastro

Configurazione di Arcserve per l'uso con i dispositivi VTL

Dopo aver connesso i dispositivi della libreria di nastri virtuali al client, esegui la scansione per la ricerca dei dispositivi.

Per eseguire la scansione per la ricerca dei dispositivi VTL

1. In Arcserve Backup Manager scegliere il menu Utilities (Utilità).
2. Scegliere Media Assure and Scan (Controllo e ricerca supporti).

Caricamento di nastri in un pool di supporti

Quando il software Arcserve si connette al gateway e i nastri diventano disponibili, Arcserve carica automaticamente i nastri. Se il gateway non viene trovato nel software Arcserve, prova a riavviare il motore dei nastri in Arcserve.

Per riavviare il motore dei nastri

1. Scegliere Quick Start (Avvio rapido), scegliere Administration (Amministrazione) e quindi scegliere Device (Dispositivo).
2. Nel menu di navigazione, aprire il menu contestuale (clic con il pulsante destro del mouse) per il gateway e scegliere uno slot di importazione/esportazione.
3. Scegliere Quick Import (Importazione rapida) e assegnare il nastro a uno slot vuoto.
4. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il gateway e scegliere Inventory/Offline Slots (Slot offline/Inventario).
5. Scegliere Quick Inventory (Inventario rapido) per recuperare le informazioni sui supporti dal database.

Se si aggiunge un nuovo nastro, è necessario eseguire la scansione del gateway per il nuovo nastro affinché venga visualizzato in Arcserve. Se i nuovi nastri non vengono visualizzati, è necessario importarli.

Per importare i nastri

1. Scegliere il menu Quick Start (Avvio rapido), scegliere Back up (Backup) e quindi scegliere Destination tap (Destinazione).
2. Scegliere il gateway, aprire il menu contestuale (clic con il pulsante destro del mouse) per un nastro e quindi scegliere Import/Export Slot (Slot importazione/esportazione).
3. Aprire il menu contestuale (clic con il pulsante destro del mouse) per ogni nuovo nastro e scegliere Inventory (Inventario).
4. Aprire il menu contestuale (clic con il pulsante destro del mouse) per ogni nuovo nastro e scegliere Format (Formato).

Il codice a barre di ogni nastro viene ora visualizzato nella console Storage Gateway e ogni nastro è pronto per l'uso.

Backup dei dati su nastro

Quando i nastri sono stati caricati in Arcserve, è possibile eseguire il backup dei dati. Il processo di backup equivale a quello di backup dei nastri fisici.

Per eseguire il backup dei dati su un nastro

1. Dal menu Quick Start (Avvio rapido) aprire la sessione di ripristino di un backup.
2. Scegliere la scheda Source (Origine) e quindi scegliere il file system o il sistema di database di cui eseguire il backup.
3. Scegliere la scheda Schedule (Pianificazione) e scegliere il metodo di ripetizione da usare.
4. Scegliere la scheda Destination (Destinazione) e quindi scegliere il nastro da usare. Se i dati di cui si esegue il backup hanno dimensioni superiori alla capacità del nastro, Arcserve richiede di montare un nuovo nastro.
5. Scegliere Submit (Invia) per eseguire il backup dei dati.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente.

Archiviazione di un nastro

Quando archivi un nastro, il gateway di nastri virtuali sposta il nastro dalla libreria di nastri allo storage offline. Prima di espellere e archiviare un nastro, controlla i relativi contenuti.

Per archiviare un nastro

1. Dal menu Quick Start (Avvio rapido) aprire la sessione di ripristino di un backup.
2. Scegliere la scheda Source (Origine) e quindi scegliere il file system o il sistema di database di cui eseguire il backup.
3. Scegliere la scheda Schedule (Pianificazione) e scegliere il metodo di ripetizione da usare.
4. Scegliere il gateway, aprire il menu contestuale (clic con il pulsante destro del mouse) per un nastro e quindi scegliere Import/Export Slot (Slot importazione/esportazione).
5. Assegnare una porta di inserimento/espulsione per caricare il nastro. Lo stato nella console Storage Gateway cambia in Archive (Archivio). Il processo di archiviazione potrebbe richiedere alcuni minuti.

Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro non è più elencato nella VTL ma è archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Ripristino dei dati da un nastro

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato su un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.

2. Usare Arcserve per ripristinare i dati. Questo processo equivale a quello di ripristino dei dati da nastri fisici. Per istruzioni, consulta la documentazione di Arcserve Backup r17.

Per ripristinare i dati da un nastro, usa la procedura seguente.

Per ripristinare i dati da un nastro

1. Dal menu Quick Start (Avvio rapido) aprire una sessione di ripristino.
2. Scegliere la scheda Source (Origine) e quindi scegliere il file system o il sistema di database da ripristinare.
3. Scegliere la scheda Destination (Destinazione) e accettare le impostazioni predefinite.
4. Scegliere la scheda Schedule (Pianificazione), scegliere il metodo di ripetizione da utilizzare e quindi scegliere Submit (Invia).

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione tramite Bacula Enterprise

Puoi eseguire il backup dei dati su nastri virtuali, archiviare nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Bacula Enterprise versione 10. In questo argomento viene illustrata la documentazione di base su come configurare l'applicazione di backup Bacula versione 10 per un gateway di nastri virtuali ed eseguire operazioni di backup e ripristino. Per informazioni dettagliate su come utilizzare Bacula versione 10, consulta Manuali e documentazione sui sistemi Bacula o contattare Bacula Systems.

> **Note**
>
> Bacula è supportata solo su Linux.

Impostazione di Bacula Enterprise

Dopo aver connesso i dispositivi della libreria di nastri virtuali (VTL) al client Linux, puoi configurare il software Bacula in modo che riconosca i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client, consulta Connessione dei dispositivi VTL.

Per impostare Bacula

1. Ottieni una copia con licenza del software di backup Bacula Enterprise da Bacula Systems.
2. Installa il software Bacula Enterprise sul computer in locale o nel cloud.

   Per informazioni su come ottenere il software di installazione, vedere Enterprise Backup per Amazon S3 e Storage Gateway. Per linee guida aggiuntive sull'installazione, consulta il whitepaper di Bacula Utilizzo dei servizi cloud e dello storage di oggetti con Bacula Enterprise Edition.

Configurazione di Bacula per gestire i dispositivi VTL

Quindi, configurare Bacula per gestire i tuoi dispositivi VTL. In seguito, è possibile individuare i passaggi di configurazione di base.

Per configurare Bacula

1. Installare Bacula Director e il daemon Bacula Storage. Per istruzioni consultare il capitolo 7 del whitepaper di Bacula Utilizzo dei servizi cloud e dello storage di oggetti con Bacula Enterprise Edition.
2. Collegare il sistema su cui è in esecuzione Bacula Director e configurare l'iniziatore iSCSI. Per farlo, utilizzare lo script fornito nella fase 7.4 del whitepaper di Bacula Utilizzo dei servizi cloud e dello storage di oggetti con Bacula Enterprise Edition.
3. Configurare i dispositivi di storage. Utilizzare lo script fornito nel whitepaper di Bacula illustrato in precedenza.
4. Configurare il Bacula Director locale, aggiungere le destinazioni di storage e definire i pool di supporti per i nastri. Utilizzare lo script fornito nel whitepaper di Bacula illustrato in precedenza.

Backup dei dati su nastro

1. Crea nastri nella console Storage Gateway. Per informazioni su come creare i nastri, consulta Creating Tapes (crea Nastri)
2. Trasferimento di nastri dallo slot I/O allo slot di storage utilizzando il comando seguente.

   ```
   /opt/bacula/scripts/mtx-changer
   ```

   Ad esempio, il comando seguente trasferisce i nastri dallo slot I/O 1601 allo slot di storage 1.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

3. Avviare la console Bacula utilizzando il comando seguente.

   ```
   /opt/bacula/bin/bconsole
   ```

   > **Note**
   >
   > Quando si crea e si trasferisce un nastro a Bacula, utilizzare il comando della console Bacula (bconsole) `update slots storage=VTL` in modo che Bacula sia a conoscenza dei nuovi nastri creati.

4. Etichettare il nastro con il codice a barre usando il nome del volume o etichettarlo utilizzando il seguente comando bconsole.

   ```
   label storage=VTL pool=pool.VTL barcodes === label the tapes with the
   barcode as the volume name / label
   ```

5. Montare il nastro usando il comando seguente.

   ```
   mount storage=VTL slot=1 drive=0
   ```

6. Creare un processo di backup che utilizza i pool di supporti creati e scrivere i dati su un nastro virtuale utilizzando le stesse procedure valide per i nastri fisici.

7. Smontare il nastro dalla console Bacula utilizzando il comando seguente.

   ```
   umount storage=VTL slot=1 drive=0
   ```

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup avrà esito negativo e lo stato del nastro in Bacula Enterprise passerà a COMPLETO. Se si sa che il nastro non è stato utilizzato completamente, è possibile modificare manualmente lo stato del nastro su APPEND e continuare il processo di backup utilizzando lo stesso nastro. È inoltre possibile continuare il lavoro su un nastro diverso se sono disponibili altri nastri con stato APPEND.

Archiviazione di un nastro

Quando tutte le attività di backup per un determinato nastro vengono eseguite ed è possibile archiviare il nastro, utilizzare lo script mtx-changer per spostare il nastro dallo slot di storage allo slot I/O. Questa operazione è analoga all'azione di estrazione in altre applicazioni di backup.

Per archiviare un nastro

1. Trasferimento di nastri dallo slot di storage allo slot I/O utilizzando il comando `/opt/bacula/scripts/mtx-changer`.

   Ad esempio, il comando seguente trasferisce un nastro dallo slot di storage 1 allo slot I/O 1601.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1 1601
   ```

2. Verificare che il nastro sia archiviato nello storage offline (S3 Glacier Flexible Retrieval oppure S3 Glacier Deep Archive) e che abbia lo stato Archived (Archiviato).

Ripristino di dati da un nastro archiviato e recuperato

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Ripristina i dati utilizzando il software Bacula:

   a. Importazione dei nastri nello slot di storage utilizzando il comando `/opt/bacula/scripts/mtx-changer` per trasferire i nastri dallo slot I/O.

      Ad esempio, il comando seguente trasferisce i nastri dallo slot I/O 1601 allo slot di storage 1.

      ```
      /opt/bacula/scripts/mtx-changer transfer 1601 1
      ```

   b. Utilizzare la console Bacula per aggiornare gli slot e quindi montare il nastro.

   c. Eseguire il comando di ripristino per ripristinare i dati. Per le istruzioni, consultare la documentazione di Bacula.

Test della configurazione tramite Commvault

Puoi eseguire il backup dei dati su nastri virtuali, archiviare nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Commvault versione 6.4. In questo argomento, è possibile trovare la documentazione di base su come configurare l'applicazione di backup Commvault per un gateway di nastri virtuali, eseguire un archivio di backup e recuperare i dati dai nastri archiviati. Per informazioni dettagliate su come utilizzare Commvault, consulta Commvault Quick Start Guide sul sito Web di Commvault.

Argomenti

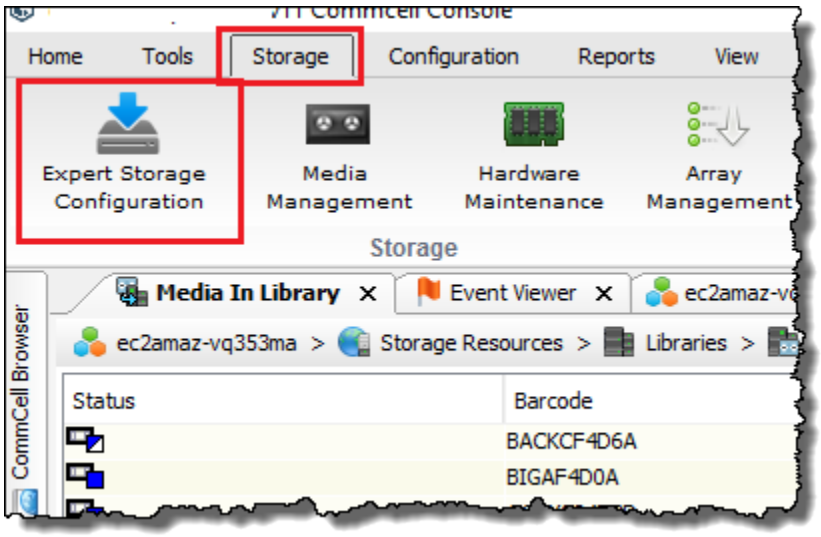
Configurazione di Commvault per l'uso con i dispositivi VTL

Dopo aver connesso i dispositivi della libreria di nastri virtuali al client Windows, puoi configurare Commvault per riconoscere i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL a un client Windows.

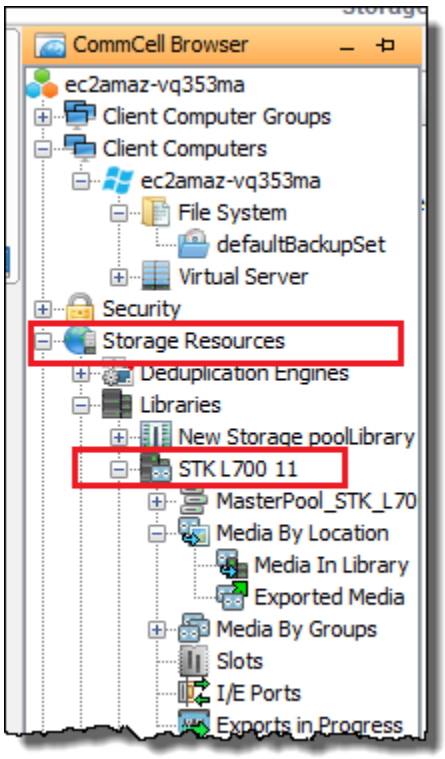
L'applicazione di backup Commvault non riconosce automaticamente i dispositivi VTL. È necessario aggiungere manualmente i dispositivi per esporli all'applicazione di backup Commvault e quindi individuare i dispositivi VTL.

Per configurare Commvault

1. Nel menu principale della CommCell console, scegli Archiviazione, quindi scegli Expert Storage Configuration per aprire la MediaAgents finestra di dialogo Seleziona.



2. Selezionare l'agente dei supporti da utilizzare, quindi selezionare Add (Aggiungi), poi OK.
3. Nella finestra di dialogo Expert Storage Configuration (Configurazione Expert Storage), selezionare Start (Avvia), quindi Detect/Configure Devices (Rileva/configura dispositivi).
4. Lasciare selezionate le opzioni Device Type (Tipo dispositivo), selezionare Exhaustive Detection (Rilevamento completo), quindi OK.
5. Nella finestra di dialogo di conferma Confirm Exhaustive Detection (Conferma rilevamento completo), selezionare Yes (Sì).
6. Nella finestra di dialogo Device Selection (Selezione dispositivi), selezionare la libreria e tutte le unità, quindi OK. Attendere che vengano rilevati i dispositivi, quindi selezionare Close (Chiudi) per chiudere il report di log.
7. Fare clic con il pulsante destro del mouse sulla libreria, quindi scegliere Configure (Configura), poi Yes (Sì). Chiudere la finestra di dialogo di configurazione.
8. Nella finestra di dialogo Does this library have a barcode reader? (Questa libreria dispone di un lettore di codici a barre?), scegliere Yes (Sì), quindi per tipo di dispositivo scegliere IBM ULTRIUM V5.
9. Nel CommCell browser, scegli Risorse di archiviazione, quindi scegli Librerie per visualizzare la tua libreria di nastri.



10. Per vedere i nastri nella libreria, aprire il menu contestuale (clic con il pulsante destro del mouse) per la libreria, quindi selezionare Discover Media (Scopri supporto), Media location (Posizione supporto), Media Library (Libreria supporti).
11. Per montare i nastri, aprire il menu contestuale (clic con il pulsante destro del mouse) per il supporto, quindi selezionare Load (Carica).

Creazione di una policy di storage e di un client secondario

Ogni processo di backup e ripristino è associato a una policy di storage e una policy di client secondario.

Una policy di storage consente di mappare il percorso originale dei dati al supporto.

Per creare una policy di storage

1. Nel CommCell browser, scegli Politiche.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per Storage Policies (Policy di storage), quindi scegliere New Storage Policy (Nuova policy di storage).
3. Nella procedura guidata per la creazione di policy di storage, selezionare Data Protection and Archiving (Archiviazione e protezione dati), quindi Next (Avanti).

4. Digitare un nome per Storage Policy Name (Nome policy di storage), quindi selezionare Incremental Storage Policy (Policy di storage incrementale). Per associare questa policy di storage ai caricamenti incrementali, scegliere una delle opzioni. Altrimenti, lasciare le opzioni deselezionate, quindi scegliere Next (Avanti).
5. Nella finestra di dialogo Do you want to Use Global Deduplication Policy? (Utilizzare la policy di deduplicazione globale?) scegliere le preferenze di Deduplication (Deduplicazione), quindi scegliere Next (Avanti).
6. Da Library for Primary Copy (Libreria per copia primaria), scegliere la libreria VTL, quindi Next (Avanti).
7. Verificare che le impostazioni dell'agente dei supporti siano corrette, quindi selezionare Next (Avanti).
8. Verificare che le impostazioni del pool di lavoro siano corrette, quindi selezionare Next (Avanti).
9. Configurare le policy di conservazione in iData Agent Backup data (Dati di backup agente iData), quindi Next (Avanti).
10. Rivedere le impostazioni di crittografia, quindi selezionare Next (Avanti).
11. Per vedere la policy di storage, selezionare Storage Policies (Policy di storage).

È possibile creare una policy di client secondario e associarla alle policy di storage. Una policy di client secondario consente di configurare client di file system simili da un modello centralizzato, in modo che non sia necessario configurare più file system simili manualmente.

Per creare una policy del client secondario

1. Nel CommCell browser, scegli Computer client, quindi scegli il tuo computer client. Scegli File System, quindi scegli defaultBackupSet.
2. Fate clic con il pulsante destro del mouse defaultBackupSet, scegliete Tutte le attività, quindi scegliete Nuovo client secondario.
3. Nella casella delle proprietà del subclient, digitate un nome in SubClient Nome, quindi scegliete OK.
4. Scegliere Browse (Sfoglia), andare ai file di cui eseguire il backup, selezionare Add (Aggiungi), quindi chiudere la finestra di dialogo.
5. Nella casella delle proprietà Subclient (Client secondario), selezionare la scheda Storage Device (Dispositivo di storage), selezionare una policy di storage da Storage policy (Policy di storage), quindi OK.

6. Nella finestra Backup Schedule (Pianificazione di backup) visualizzata, associare il nuovo client secondario a una pianificazione di backup.
7. Selezionare Do Not Schedule (Non pianificare) per i backup una tantum oppure on demand, quindi selezionare OK.

   Ora dovresti vedere il tuo subclient nella defaultBackupSetscheda.

Backup dei dati su nastro in Commvault

È possibile creare un processo di backup e scrivere i dati su un nastro virtuale usando le stesse procedure usate con nastri fisici. Per ulteriori informazioni, consulta la documentazione di Commvault.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. In alcuni casi, è possibile selezionare un'opzione per riprendere il processo fallito. In caso contrario, devi inviare un nuovo lavoro. Se Commvault contrassegna il nastro come inutilizzabile dopo un errore di lavoro, è necessario ricaricare il nastro nell'unità per continuare a scrivere su di esso. Se sono disponibili più nastri, Commvault potrebbe continuare il processo di backup fallito su un nastro diverso.

Archiviazione di un nastro in Commvault

Il processo di archiviazione viene avviato mediante l'espulsione del nastro. Quando archivi un nastro, il gateway di nastri virtuali sposta il nastro dalla libreria di nastri allo storage offline. Prima di espellere e archiviare un nastro, controlla prima il contenuto del nastro.

Per archiviare un nastro

1. Nel CommCell browser, scegli Risorse di archiviazione, Librerie, quindi scegli La tua libreria. Scegliere Media By Location (Supporto per posizione), quindi Media In Library (Supporti in libreria).
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro da archiviare, scegliere All Tasks (Tutte le attività), Export (Esporta), infine OK.

Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato

diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro esportato non è più elencato nella libreria di nastri virtuali.

Nel software Commvault verificare che il nastro non sia più nello slot di storage.

Nel riquadro di navigazione della console Storage Gateway selezionare Tapes (Nastri). Verificare che lo stato del nastro archiviato sia ARCHIVED (ARCHIVIATO).

Ripristino dei dati da un nastro

È possibile ripristinare i dati da un nastro che non è mai stato archiviato e recuperato o da un nastro archiviato e recuperato. Per i nastri che non sono mai stati archiviati e recuperati (nastri non recuperati), sono disponibili due opzioni per ripristinare i dati:

- Ripristino mediante client secondario
- Ripristino mediante ID processo

Per ripristinare i dati da un nastro non richiamato dal client secondario

1. Nel CommCell browser, scegli Computer client, quindi scegli il tuo computer client. Scegli File System, quindi scegli defaultBackupSet.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il client secondario, scegliere Browse and Restore (Sfoglia e ripristina), quindi View Content (Visualizza contenuto).
3. Selezionare i file che si desidera ripristinare, quindi selezionare Recover All Selected (Ripristina tutte le voci selezionate).
4. Selezionare Home (Home page), quindi Job Controller (Controller processo) per monitorare lo stato del processo di ripristino.

Per ripristinare i dati da un nastro non richiamato dall'ID del processo

1. Nel CommCell browser, scegli Computer client, quindi scegli il tuo computer client. Fai clic con il pulsante destro del mouse su File System, scegliere View (Visualizza), quindi Backup History (Cronologia di backup).
2. Nella categoria Backup Type (Tipo di backup), scegliere il tipo di processi di backup desiderati, quindi OK. Viene visualizzata una scheda con la cronologia dei processi di backup.
3. Trovare il Job ID (ID processo) da ripristinare, fare clic con il pulsante destro del mouse su di esso, quindi selezionare Browse and Restore (Sfoglia e ripristina).

4. Nella finestra di dialogo Browse and Restore Options (Opzioni di ricerca e ripristino), selezionare View Content (Visualizza contenuto).
5. Selezionare i file che si desidera ripristinare, quindi selezionare Recover All Selected (Ripristina tutte le voci selezionate).
6. Selezionare Home (Home page), quindi Job Controller (Controller processo) per monitorare lo stato del processo di ripristino.

Per ripristinare i dati da un nastro archiviato e recuperato

1. Nel CommCell browser, scegli Risorse di archiviazione, scegli Librerie e quindi scegli La tua libreria. Scegliere Media By Location (Supporto per posizione), quindi Media In Library (Supporti in libreria).
2. Fare clic con il pulsante destro del mouse sul nastro richiamato, selezionare All Tasks (Tutte le attività), quindi selezionare Catalog (Catalogo).
3. Nella finestra di dialogo Catalog Media (Supporti catalogo), selezionare Catalog only (Solo catalogo), quindi OK.
4. Selezionare CommCell Home (Home page), quindi Job Controller (Controller processo) per monitorare lo stato del processo di ripristino.
5. Dopo l'esito positivo del processo, aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro, selezionare View (Visualizza), quindi View Catalog Contents (Visualizza contenuti catalogo). Prendere nota del valore Job ID (ID processo) per utilizzarlo in seguito.
6. Selezionare Recatalog/Merge (Ricataloga/Unisci). Verificare che sia selezionato Merge only (Unisci solo) nella finestra di dialogo Catalog Media (Supporti catalogo).
7. Selezionare Home (Home page), quindi Job Controller (Controller processo) per monitorare lo stato del processo di ripristino.
8. Una volta completato il processo, scegli CommCell Home, scegli Pannello di controllo, quindi scegli Browse/Search/Recovery.
9. Selezionare Show aged data during browse and recovery (Mostra dati vecchi durante la ricerca e il ripristino), selezionare OK, quindi chiudere il Control Panel (Pannello di controllo).
10. Nel CommCell browser, fai clic con il pulsante destro del mouse su Computer client, quindi scegli il tuo computer client. Scegli View (Visualizza), quindi Job History (Cronologia processi).
11. Nella finestra di dialogo Job History Filter (Filtro cronologia processi) scegliere Advanced (Avanzate).
12. Scegliere Include Aged Data (Includi dati vecchi) e selezionare OK.

13. Nella finestra di dialogo Job History (Cronologia processi), selezionare OK per aprire la scheda history of jobs (Cronologia dei processi).
14. Trovare il processo da ripristinare, aprire il menu contestuale (clic con il pulsante destro del mouse) per il processo, quindi selezionare Browse and Restore (Sfoglia e ripristina).
15. Nella finestra di dialogo Browse and Restore (Sfoglia e ripristina), selezionare View Content (Visualizza contenuto).
16. Selezionare i file che si desidera ripristinare, quindi selezionare Recover All Selected (Ripristina tutte le voci selezionate).
17. Selezionare Home (Home page), quindi Job Controller (Controller processo) per monitorare lo stato del processo di ripristino.

Test della configurazione utilizzando Dell EMC NetWorker

È possibile eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi VTL (Virtual Tape Library) utilizzando Dell EMC 19.5. NetWorker In questo argomento, è possibile trovare la documentazione di base su come configurare il NetWorker software Dell EMC per funzionare con un Tape Gateway ed eseguire un backup, incluso come configurare i dispositivi di storage, scrivere dati su un nastro, archiviare un nastro e ripristinare i dati da un nastro.

Per informazioni dettagliate su come installare e utilizzare il NetWorker software Dell EMC, consulta la Guida all'amministrazione.

Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

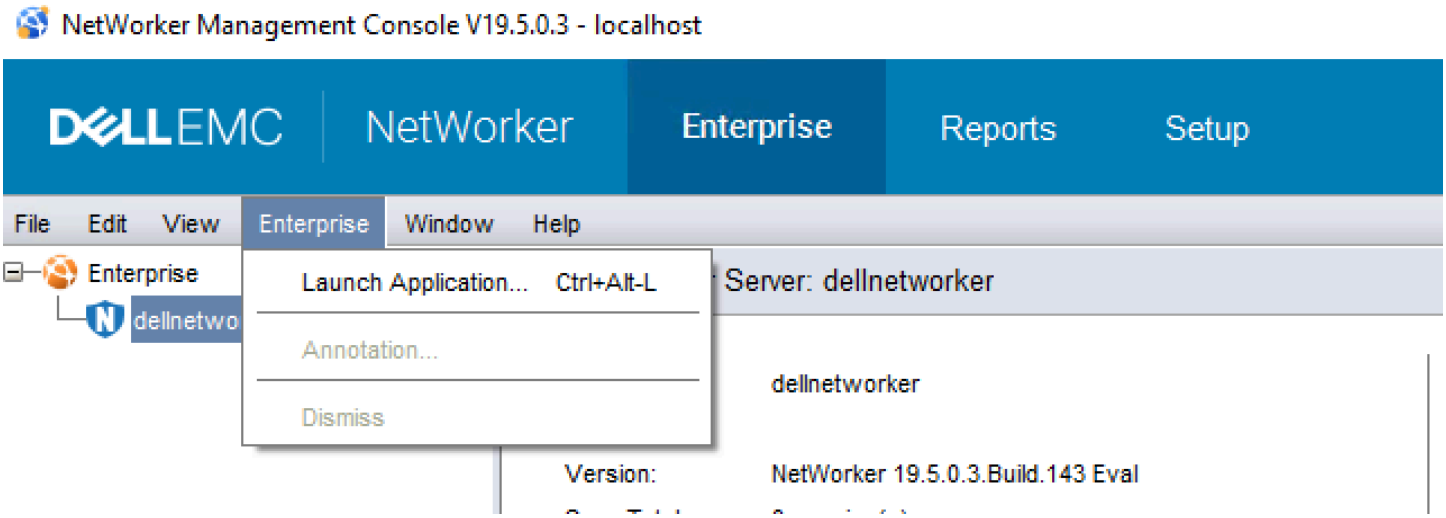
- Configurazione per lavorare con i dispositivi VTL
- Consentire l'importazione di nastri WORM in Dell EMC NetWorker
- Backup dei dati su nastro in Dell EMC NetWorker
- Archiviazione di un nastro in Dell EMC NetWorker
- Ripristino dei dati da un nastro archiviato in Dell EMC NetWorker

Configurazione per lavorare con i dispositivi VTL

Dopo aver connesso i dispositivi della libreria di nastri virtuali (VTL) al client Microsoft Windows, puoi configurarlo per riconoscere i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

non riconosce automaticamente i dispositivi gateway di nastri virtuali. Per esporre i dispositivi VTL al NetWorker software e far sì che il software li rilevi, configurate manualmente il software. Qui di seguito, partiamo dal presupposto che tu abbia installato correttamente il software e che conosca già la Management Console. Per ulteriori informazioni sulla console di gestione, consultare la sezione relativa all'interfaccia della console di NetWorker gestione della Dell EMC NetWorker Administration Guide.

La schermata seguente mostra Dell EMC NetWorker 19.5.



Per configurare il NetWorker software Dell EMC per dispositivi VTL

1. Avvia l'applicazione Dell EMC NetWorker Management Console, scegli Enterprise dal menu, quindi scegli localhost dal riquadro di sinistra.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per localhost, quindi selezionare Launch Application (Avvia applicazione).
3. Selezionare la scheda Devices (Dispositivi), aprire il menu contestuale (clic con il pulsante destro del mouse) per Libraries (Librerie), quindi Scan for Devices (Scansione dispositivi).
4. Nella procedura guidata per la scansione dei dispositivi, selezionare Start Scan (Inizia scansione), quindi selezionare OK dalla finestra di dialogo visualizzata.

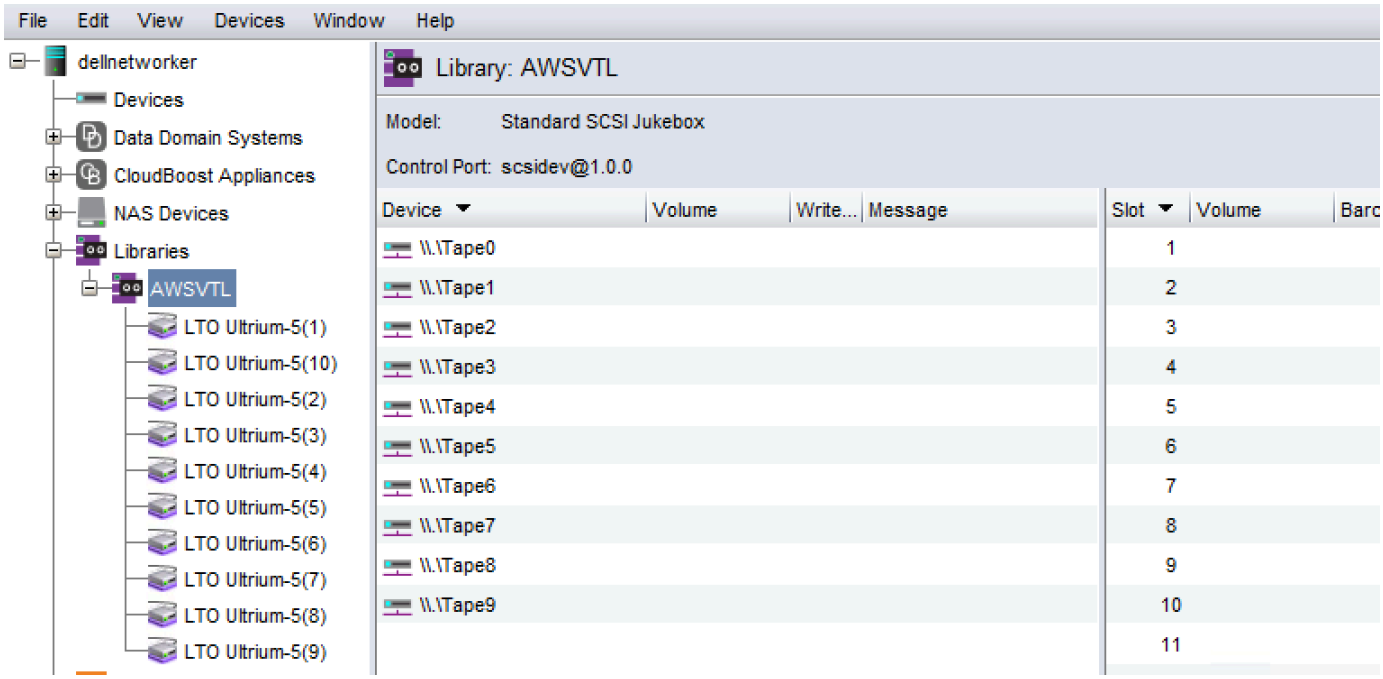
5. Espandere l'albero delle cartelle Libraries (Librerie) per visualizzare tutte le librerie e premere F5 per riaggiornare. Questo processo potrebbe richiedere alcuni secondi per caricare i dispositivi nella libreria.

6. Apri una finestra di comando (CMD.exe) con privilegi di amministratore ed esegui l'utilità «jbconfig» installata con Dell EMC 19.5. NetWorker

```
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>jbconfig

Jbconfig is running on host dellnetworker (Windows Server 2019 Datacenter 10.0),
  and is using dellnetworker as the NetWorker server.

        1) Configure an Autodetected SCSI Jukebox.
        2) Configure an Autodetected NDMP SCSI Jukebox.
        3) Configure an SJI Jukebox.
        4) Configure an STL Silo.
        5) Exit.

which activity do you want to perform? [1]
14484:jbconfig: Scanning SCSI buses; this may take a while ...
Installing 'Standard SCSI Jukebox' jukebox - scsidev@1.0.0.

What name do you want to assign to this jukebox device? AWSVTL
15814:jbconfig: Attempting to detect serial numbers on the jukebox and drives ...

15815:jbconfig: Will try to use SCSI information returned by jukebox to configure drives.

Turn NetWorker auto-cleaning on (yes / no) [yes]? no

The following drive(s) can be auto-configured in this jukebox:
 1> LTO Ultrium-5 @ 1.1.0 ==> \\.\Tape0
 2> LTO Ultrium-5 @ 1.2.0 ==> \\.\Tape1
 3> LTO Ultrium-5 @ 1.3.0 ==> \\.\Tape2
 4> LTO Ultrium-5 @ 1.4.0 ==> \\.\Tape3
 5> LTO Ultrium-5 @ 1.5.0 ==> \\.\Tape4
 6> LTO Ultrium-5 @ 1.6.0 ==> \\.\Tape5
 7> LTO Ultrium-5 @ 1.7.0 ==> \\.\Tape6
 8> LTO Ultrium-5 @ 1.8.0 ==> \\.\Tape7
 9> LTO Ultrium-5 @ 1.9.0 ==> \\.\Tape8
10> LTO Ultrium-5 @ 1.10.0 ==> \\.\Tape9
These are all the drives that this jukebox has reported.
```

```
To change the drive model(s) or configure them as shared or NDMP drives,
 you need to bypass auto-configure. Bypass auto-configure? (yes / no) [no]


Jukebox has been added successfully

The following configuration options have been set:

> Jukebox description to the control port and model.
> Autochanger control port to the port at which we found it.
> Autocleaning off.
> Barcode reading to on.
> Volume labels that match the barcodes.

You can review and change the characteristics of the autochanger and its
        associated devices using the NetWorker Management Console.

Would you like to configure another jukebox? (yes/no) [no]

C:\Users\Administrator>_
```

7. Al termine di "jbconfig", torna alla GUI di Networker e premi F5 per eseguire l'aggiornamento.
8. Scegliere la libreria per visualizzare i nastri nel riquadro a sinistra e l'elenco degli slot di volume vuoti corrispondente nel riquadro di destra. In questa schermata, è selezionata la libreria "»AWSVTL.



9. Nell'elenco dei volumi, selezionare i volumi che si desidera abilitare (i volumi selezionati appaiono evidenziati), aprire il menu contestuale (clic con il pulsante destro del mouse) per i

volumi selezionati, quindi scegliere Deposit (Deposita). Questa operazione sposta il nastro dallo slot I/O allo slot di volume.

10. Nella finestra di dialogo visualizzata, selezionare Yes (Sì), quindi nella finestra di dialogo Load the Cartridges into (Carica cartucce in) selezionare Yes (Sì).
11. Se non vi sono altri nastri da depositare, selezionare No o Ignore (Ignora). Altrimenti, selezionare Yes (Sì) per depositare nastri aggiuntivi.

Consentire l'importazione di nastri WORM in Dell EMC NetWorker

Ora sei pronto per importare i nastri dal tuo Tape Gateway nella libreria Dell EMC. NetWorker

I nastri virtuali sono nastri Write Once Read Many (WORM), ma Dell EMC NetWorker prevede nastri non WORM. Affinché Dell EMC funzioni con NetWorker i nastri virtuali, è necessario attivare l'importazione dei nastri in pool di supporti non WORM.

Abilitare l'importazione di nastri WORM in pool di supporti non WORM

1. Su NetWorker Console, scegli Media, apri il menu contestuale (fai clic con il pulsante destro del mouse) per localhost, quindi scegli Proprietà.
2. Nella finestra Proprietà del NetWorker server, scegli la scheda Configurazione.
3. Nella sezione Worm tape handling (Gestione nastro Worm), eliminare il contenuto della finestra WORM tapes only in WORM pools (Nastri WORM solo nei pool WORM), quindi selezionare OK.

Backup dei dati su nastro in Dell EMC NetWorker

Il backup dei dati su nastro è un processo in due fasi.

1. Etichetta i nastri su cui desideri eseguire il backup dei dati, crea il pool di supporti e aggiungi i nastri al pool.

   Puoi creare un pool di supporti e scrivere i dati su un nastro virtuale seguendo le stesse procedure che utilizzi con nastri fisici. Per informazioni dettagliate, consultare la sezione Backup dei dati della Dell EMC NetWorker Administration Guide.
2. Scrivi dati sul nastro. È possibile eseguire il backup dei dati utilizzando l'applicazione NetWorker utente Dell EMC anziché la Dell EMC NetWorker Management Console. L'applicazione NetWorker utente Dell EMC viene installata come parte dell' NetWorkerinstallazione.

> **Note**
>
> L'applicazione NetWorker utente Dell EMC viene utilizzata per eseguire i backup, ma è possibile visualizzare lo stato dei processi di backup e ripristino nella EMC Management Console. Per visualizzare lo stato, selezionare il menu Devices (Dispositivi) e visualizzare lo stato nella finestra Log.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup avrà esito negativo e lo stato del nastro in Bacula Enterprise passerà a COMPLETO. È possibile archiviare il nastro o continuare a leggere i dati da esso. È possibile riprendere il processo di backup sospeso su un altro nastro.

Archiviazione di un nastro in Dell EMC NetWorker

Quando si archivia un nastro, Tape Gateway lo sposta dalla libreria di NetWorker nastri Dell EMC allo storage offline. Puoi iniziare l'archiviazione di nastri estraendo un nastro dall'unità nastro nello slot di storage. Quindi estrai il nastro dallo slot all'archivio utilizzando l'applicazione di backup, ovvero il software Dell EMC. NetWorker

Per archiviare un nastro utilizzando Dell EMC NetWorker

1. Nella scheda Dispositivi della finestra NetWorker Amministrazione, scegli localhost o il tuo server EMC, quindi scegli Librerie.
2. Selezionare la libreria importata dalla libreria di nastri virtuali.
3. Dall'elenco dei nastri sui quali sono stati scritti i dati, aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro che si desidera archiviare, quindi selezionare Eject/ Withdraw (Espelli/Ritira).
4. Nella casella di conferma visualizzata, fare clic su OK.

Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro esportato non è più elencato nella libreria di nastri virtuali.

Nel NetWorker software Dell EMC, verifica che il nastro non sia più nello slot di archiviazione.

Nel riquadro di navigazione della console Storage Gateway selezionare Tapes (Nastri). Verificare che lo stato del nastro archiviato sia ARCHIVED (ARCHIVIATO).

Ripristino dei dati da un nastro archiviato in Dell EMC NetWorker

Il ripristino dei dati archiviati è un processo in due fasi:

1. Recupera il nastro archiviato sul gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizza il NetWorker software Dell EMC per ripristinare i dati. A questo scopo, devi ripristinare una cartella, come fai per il ripristino dei dati da nastri fisici. Per istruzioni, vedere la sezione Utilizzo del programma NetWorker utente della Guida all' NetWorker amministrazione di Dell EMC.

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione mediante IBM Spectrum Protect

È possibile eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi VTL (Virtual Tape Library) utilizzando IBM Spectrum Protect with. AWS Storage Gateway IBM Spectrum Protect era precedentemente noto come Tivoli Storage Manager.

Questo argomento contiene informazioni di base su come configurare il software di backup IBM Spectrum Protect versione 8.1.10 per un gateway di nastri virtuali. Include anche informazioni di base sull'esecuzione di operazioni di backup e ripristino con IBM Spectrum Protect. Per ulteriori informazioni su come amministrare il software di backup IBM Spectrum Protect, consulta la Panoramica delle attività di amministrazione di IBM Spectrum Protect.

Il software di backup IBM Spectrum Protect supporta i seguenti sistemi operativi AWS Storage Gateway .

- Microsoft Windows Server
- Red Hat Linux

Per informazioni sui dispositivi supportati da IBM Spectrum Protect per Windows, consulta Dispositivi supportati da IBM Spectrum Protect (precedentemente Tivoli Storage Manager) per AIX, HP-UX, Solaris e Windows.

Per informazioni sui dispositivi supportati da IBM Spectrum Protect per Linux, consulta Dispositivi supportati per Linux da IBM Spectrum Protect (precedentemente Tivoli Storage Manager).

Argomenti

Impostazione di IBM Spectrum Protect

Dopo aver connesso i dispositivi VTL al client, è possibile configurare il software IBM Spectrum Protect versione 8.1.10 per riconoscerli. Per ulteriori informazioni su come connettere i dispositivi VTL al client, consulta Connessione dei dispositivi VTL.

Impostazione di IBM Spectrum Protect

1. Ottieni una copia con licenza del software IBM Spectrum Protect versione 8.1.10 di IBM.
2. Installare il software IBM Spectrum Protect nel tuo ambiente on-premise o nell'istanza EC2 Amazon nel cloud. Per ulteriori informazioni, consulta la documentazione di installazione e aggiornamento di IBM per IBM Spectrum Protect.

   Per ulteriori informazioni sulla configurazione del software IBM Spectrum Protect, consulta Configurazione delle librerie di nastri virtuali del gateway di nastri virtuali AWS per un server IBM Spectrum Protect.

Configurazione di IBM Spectrum Protect per i dispositivi VTL

Quindi, configurare IBM Spectrum Protect per lavorare con i dispositivi VTL. Puoi configurare IBM Spectrum Protect per utilizzare dispositivi VTL su Microsoft Windows o Red Hat Linux.

Configurazione di IBM Spectrum Protect for Windows

Per istruzioni complete su come configurare IBM Spectrum Protect su Windows, consulta Tape Device Driver-W12 6266 for Windows 2012 sul sito Web Lenovo. Di seguito è riportata la documentazione di base sul processo.

Per configurare IBM Spectrum Protect for Microsoft Windows

1. Selezionare il pacchetto driver corretto per l'unità di sostituzione dei supporti. Per il driver del dispositivo su nastro, IBM Spectrum Protect richiede la versione W12 6266 per Windows 2012. Per istruzioni su come ottenere i driver, consulta Tape Device Driver-W12 6266 per Windows 2012 sul sito Web di Lenovo.

   > **Note**
   >
   > Assicurati di installare il set di driver "non esclusivo".

2. Sul computer, aprire Computer Management (Gestione computer), espandere Media Changer devices (Dispositivi unità di sostituzione dei supporti) e verificare che il tipo di unità di sostituzione dei supporti sia elencato come IBM 3584 Tape Library (Libreria su nastro IBM 3584).
3. Verificare che il codice a barre per qualsiasi nastro nella libreria di nastri virtuale sia la massimo di otto caratteri. Se tenti di assegnare al nastro un codice a barre che contiene più di 8 caratteri, potrebbe essere visualizzato questo messaggio di errore: `"Tape barcode is too long for media changer"`.
4. Verificare che tutte le unità nastro e le unità di sostituzione dei supporti appaiano in IBM Spectrum Protect. A tale scopo, utilizzare il comando seguente: `\Tivoli\TSM \server>tsmdlst.exe`

Configurazione di IBM Spectrum Protect for Linux

Di seguito è riportata la documentazione di base sulla configurazione di IBM Spectrum da utilizzare con i dispositivi VTL su Linux.

Impostazione di IBM Spectrum Protect for Linux

1. Accedi a IBM Fix Central sul sito Web di supporto IBM e scegli Select product (Seleziona prodotto).
2. Per Product Group (Gruppo di prodotti), scegliere System Storage (Storage di sistema).
3. Per Select from System Storage (Seleziona da storage di sistema), scegliere Tape systems (Sistemi a nastro).
4. Per Tape systems (Sistemi a nastro), scegliere Tape drivers and software (Driver nastro e software).

5. Per Select from Tape drivers and software (Seleziona da driver e software nastro), scegliere Tape device drivers (Driver dispositivo nastro).
6. Per Platform (Piattaforma), scegliere il sistema operativo e scegliere Continue (Continua).
7. Scegliere la versione del driver del dispositivo che si desidera scaricare. Quindi segui le istruzioni nella pagina di download di Fix Central per scaricare e configurare IBM Spectrum Protect.
8. Verificare che il codice a barre per qualsiasi nastro nella libreria di nastri virtuale sia la massimo di otto caratteri. Se tenti di assegnare al nastro un codice a barre che contiene più di 8 caratteri, potrebbe essere visualizzato questo messaggio di errore: `"Tape barcode is too long for media changer"`.

Scrittura di dati su un nastro in IBM Spectrum Protect

Puoi scrivere i dati su un nastro virtuale del gateway di nastri virtuali utilizzando la stessa procedura e le stesse policy di backup che si applicano ai nastri fisici. Creazione della configurazione necessaria per le operazioni di backup e ripristino. Per ulteriori informazioni sulla configurazione di IBM Spectrum Protect, consulta Panoramica delle attività di amministrazione per IBM Spectrum Protect.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Se il processo di backup fallisce, lo stato del nastro in IBM Spectrum Protect cambia in. ReadOnly Se si è certi che il nastro non è stato utilizzato completamente, è possibile ripristinare manualmente lo stato del nastro e riprendere o inviare nuovamente il processo di backup utilizzando lo stesso nastro. ReadWrite IBM Spectrum Protect potrebbe continuare il processo di backup non riuscito su un nastro diverso se sono disponibili altri nastri in stato. ReadWrite

Ripristino di dati da un nastro archiviato in IBM Spectrum Protect

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Ripristina i dati utilizzando il software di backup IBM Spectrum Protect. L'operazione viene effettuata creando un punto di ripristino, come nel caso del ripristino di dati da nastri fisici. Per

ulteriori informazioni sulla configurazione di IBM Spectrum Protect, consulta Panoramica delle attività di amministrazione per IBM Spectrum Protect.

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione tramite Micro Focus (HPE) Data Protector

Puoi eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Micro Focus (HPE) Data Protector v9.x. In questo argomento, puoi trovare la documentazione di base su come configurare il software Micro Focus (HPE) Data Protector per un gateway di nastri virtuali ed eseguire un'operazione di backup e ripristino. Per informazioni dettagliate su come usare il software Micro Focus (HPE) Data Protector, consulta la documentazione di Hewlett Packard. Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

- Configurazione di Micro Focus (HPE) Data Protector per l'uso con i dispositivi VTL
- Preparazione dei nastri virtuali per l'uso con HPE Data Protector
- Caricamento di nastri in un pool di supporti
- Backup dei dati su nastro
- Archiviazione di un nastro
- Ripristino dei dati da un nastro

Configurazione di Micro Focus (HPE) Data Protector per l'uso con i dispositivi VTL

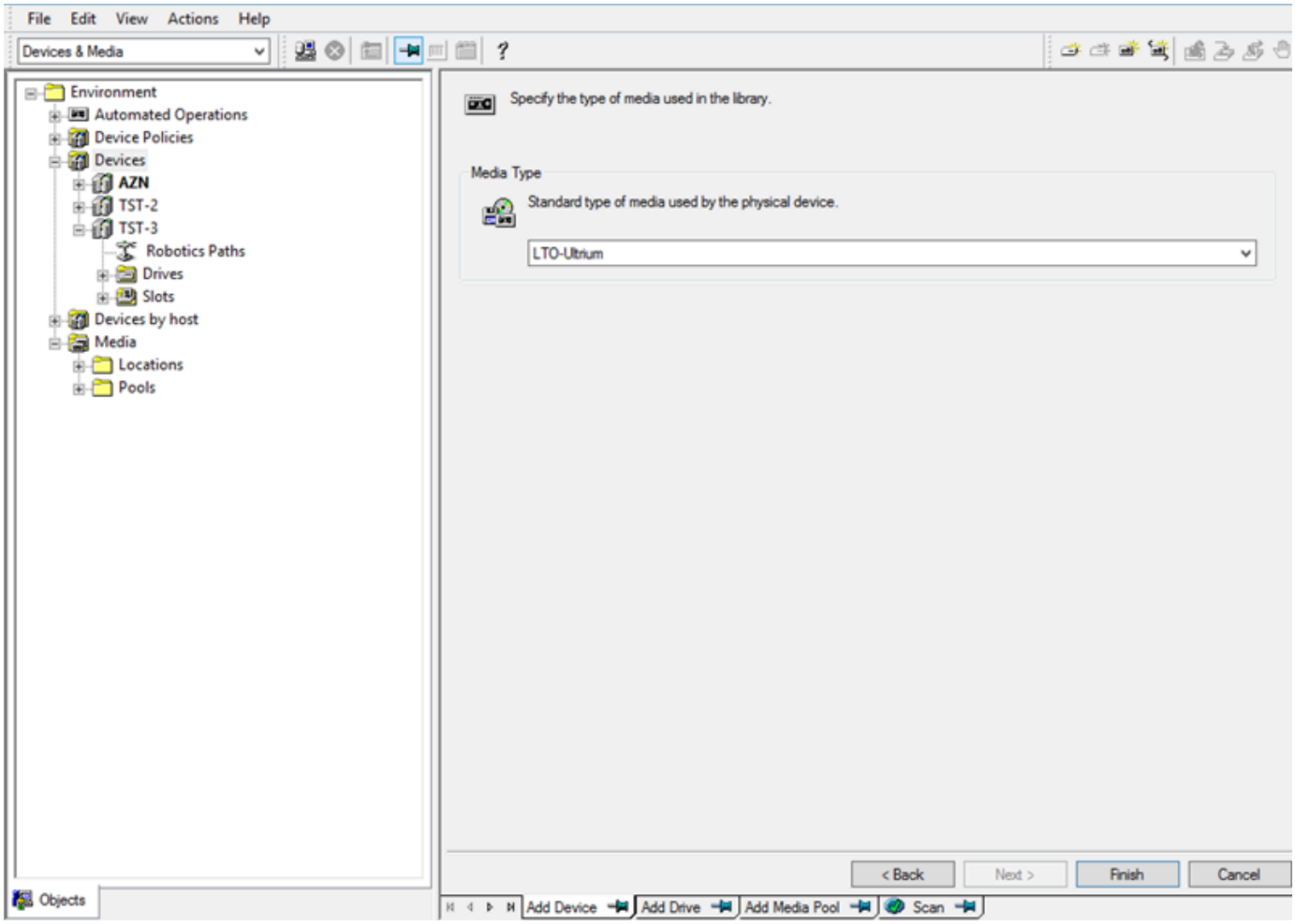
Dopo aver connesso i dispositivi della libreria di nastri virtuali al client, puoi configurare Micro Focus (HPE) Data Protector per riconoscere i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client, consulta Connessione dei dispositivi VTL.

Il software Micro Focus (HPE) Data Protector non riconosce automaticamente i dispositivi del gateway di nastri virtuali. Per fare in modo che il software riconosca questi dispositivi, è necessario aggiungerli manualmente e quindi individuare i dispositivi VTL, come descritto di seguito.

Per aggiungere i dispositivi VTL

1. Nella finestra principale di Micro Focus (HPE) Data Protector scegliere Devices & Media (Dispositivi e supporti) in alto a sinistra.

   Aprire il menu contestuale (clic con il pulsante destro del mouse) per Devices (Dispositivi) e scegliere Add Device (Aggiungi dispositivo).



2. Nella scheda Add Device (Aggiungi dispositivo) digitare un valore per Device Name (Nome dispositivo). Per Device Type (Tipo dispositivo), scegliere SCSI Library (Libreria SCSI) e quindi scegliere Next (Avanti).
3. Nella schermata successiva eseguire le operazioni seguenti:

   a. Per SCSI address of the library robotic (Indirizzo SCSI per la robotica della libreria), selezionare l'indirizzo specifico.

b. Per Select what action Data Protector should take if the drive is busy (Selezionare l'operazione per Data Protector se l'unità è occupata), scegliere "Abort" (Interrompi) oppure l'operazione desiderata.

c. Scegli di attivare queste opzioni:

- Barcode reader support (Supporto lettore codice a barre)
- Automatically discover changed SCSI address (Individuazione automatica indirizzo SCSI modificato)
- SCSI Reserve/Release (robotic control) (Rilascio/Riserva SCSI - Controllo robotico)

d. Lasciare deselezionata l'opzione Use barcode as medium label on initialization (Usa codice a barre come etichetta supporto all'inizializzazione), a meno che l'opzione non sia richiesta dal sistema.

e. Seleziona Successivo per continuare.

4. Nella schermata successiva specificare gli slot da usare con HP Data Protector. Usare un trattino ("-") tra i numeri per indicare un intervallo di slot, ad esempio 1-6. Dopo aver specificato gli slot da usare, scegliere Next (Avanti).
5. Per il tipo di supporto standard usato dal dispositivo fisico, scegliere LTO_Ultrium e quindi scegliere Finish (Fine) per completare la configurazione.

La libreria di nastri è ora pronta per l'uso. Per caricare i nastri, consulta la sezione successiva.

Preparazione dei nastri virtuali per l'uso con HPE Data Protector

Prima di eseguire il Backup dei dati su nastro virtuale, è necessario preparare il nastro per l'uso. A tale scopo, sono necessarie le operazioni seguenti:

- Caricamento di un nastro virtuale in una libreria di nastri
- Caricamento del nastro virtuale in uno slot
- Creazione di un pool di supporti
- Caricamento del nastro virtuale nel pool di supporti

Nelle sezioni seguenti sono illustrate le fasi di questo processo.

Caricamento di nastri virtuali in una libreria di nastri

La libreria di nastri dovrebbe essere elencata in Devices (Dispositivi). Se non è presente, premi F5 per aggiornare la schermata. Quando la libreria viene visualizzata, puoi caricare i nastri virtuali.

Per caricare i nastri virtuali nella libreria di nastri

1. Scegliere il segno più accanto alla libreria di nastri per visualizzare i nodi per slot, unità e percorsi robotici.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per Drives (Unità), scegliere Add Drive (Aggiungi unità), digitare un nome per il nastro e quindi scegliere Next (Avanti) per continuare.
3. Scegliere l'unità nastro da aggiungere per SCSI address of data drive (Indirizzo SCSI dell'unità dati), scegliere Automatically discover changed SCSI address (Individuazione automatica indirizzo SCSI modificato) e quindi scegliere Next (Avanti).
4. Nella schermata successiva scegliere Advanced (Avanzate). Verrà visualizzata la schermata popup Advanced Options (Opzioni avanzate).

   a. Nella scheda Settings (Impostazioni) considerare le opzioni seguenti:

      - CRC Check (Controllo CRC) (per rilevare modifiche dei dati accidentali)
      - Detect dirty drive (Rileva unità dirty) (per fare in modo che venga eseguita la pulizia dell'unità prima del backup)
      - SCSI Reserve/Release (drive) (Rilascio/Riserva SCSI - Unità) (per evitare la contesa dei nastri)

      A scopo di test, è possibile lasciare queste opzioni disabilitate (deselezionate).

   b. Nella scheda Sizes (Dimensioni) impostare Block size (kB) (Dimensioni blocco - KB) su Default (256) (Predefinite - 256).
   c. Scegliere OK per chiudere la schermata di opzioni avanzate e quindi scegliere Next (Avanti) per continuare.
5. Nella schermata successiva scegliere queste opzioni in Device Policies (Policy dispositivi):

   - Device may be used for restore (Il dispositivo può essere usato per il ripristino)
   - Device may be used as source device for object copy (Il dispositivo può essere usato come origine per la copia di oggetti)

6. Scegliere Finish (Fine) per completare l'aggiunta dell'unità nastro alla libreria di nastri.

Caricamento dei nastri virtuali negli slot

Ora che è presente un'unità nastro nella libreria di nastri, puoi caricare nastri virtuali negli slot.

Per caricare un nastro virtuale in uno slot

1. Nel nodo dell'albero della libreria di nastri aprire il nodo Slots (Slot). Ogni slot ha unno stato rappresentato da un'icona:
   - Un nastro verde indica che è già caricato un nastro nello slot.
   - Uno slot grigio indica che lo slot è vuoto.
   - Un punto interrogativo ciano indica che il nastro nello slot non è formattato.
2. Per uno slot vuoto, aprire il menu contestuale (clic con il pulsante destro del mouse) e quindi scegliere Enter (Invio). Se ci sono nastri esistenti, sceglierne uno per caricarlo nello slot.

Creazione di un pool di supporti

Un pool di supporti è un gruppo logico usato per organizzare i nastri. Per configurare il backup su nastro, è necessario creare un pool di supporti.

Per creare un pool di supporti

1. In Devices & Media (Dispositivi e supporti) aprire il nodo dell'albero per Media (Supporti), aprire il menu contestuale (clic con il pulsante destro del mouse) per il nodo Pools (Pool) e quindi scegliere Add Media Pool (Aggiungi pool di supporti).
2. In Pool name (Nome pool) digitare un nome.
3. Per Media Type (Tipo di supporto), scegliere LTO_Ultrium e quindi Next (Avanti).
4. Nella schermata seguente accettare i valori predefiniti e quindi scegliere Next (Avanti).
5. Scegliere Finish (Fine) per completare la creazione del pool di supporti.

Caricamento di nastri in un pool di supporti

Prima di eseguire il backup dei dati sui nastri, è necessario caricare i nastri nel pool di supporti creato.

Per caricare un nastro virtuale in un pool di supporti

1. Nel nodo dell'albero della libreria di nastri scegliere il nodo Slots (Slot).
2. Scegliere un nastro caricato, ovvero uno contrassegnato da un'icona di nastro verde. Aprire il menu contestuale (clic con il pulsante destro del mouse), scegliere Format (Formato) e quindi scegliere Next (Avanti).
3. Scegliere il pool di supporti creato e quindi scegliere Next (Avanti).
4. Per Medium Description (Descrizione supporti), scegliere Use barcode (Usa codice a barre) e quindi scegliere Next (Avanti).
5. Per Options (Opzioni), scegliere Force Operation (Forza operazione) e quindi scegliere Finish (Fine).

Lo slot scelto dovrebbe passare da uno stato non assegnato (grigio) a uno stato di nastro inserito (verde). Vengono visualizzati alcuni messaggi per confermare che il supporto è inizializzato.

A questo punto, la configurazione è stata completata ed è possibile iniziare a usare la libreria di nastri virtuali con HPE Data Protector. Per verificare che sia tutto pronto, usa la procedura seguente.

Per verificare che la libreria di nastri sia configurata per l'uso

- Scegliere Drives (Unità), quindi aprire il menu contestuale (clic con il pulsante destro del mouse) per l'unità e scegliere Scan (Scansione).

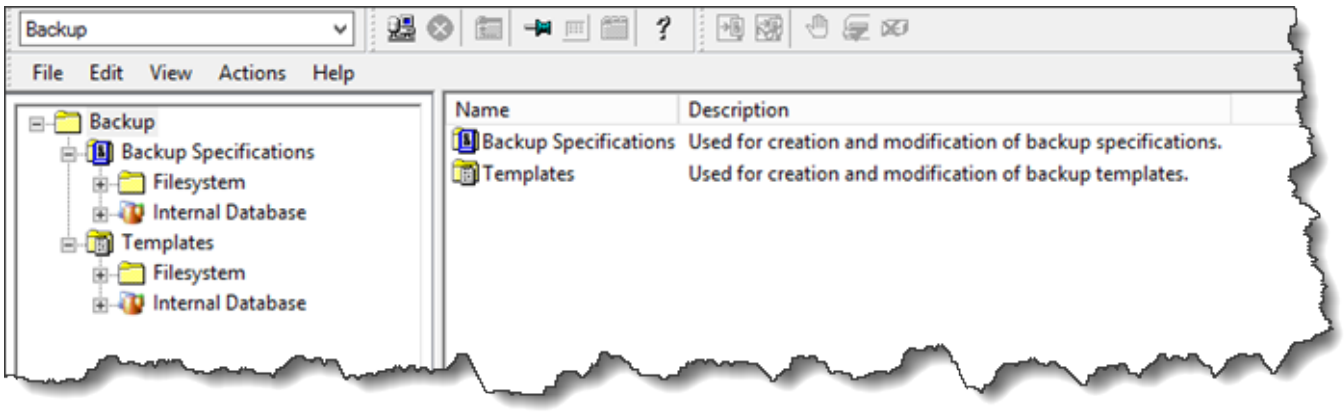
Se la configurazione è corretta, un messaggio conferma che la scansione dei supporti ha avuto esito positivo.

Backup dei dati su nastro

Quando i nastri sono stati caricati in un pool di supporti, è possibile eseguire il backup dei dati.

Per eseguire il backup dei dati su un nastro

1. Scegliere Backup in alto a sinistra nello schermo.



2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per Filesystem (File system) e scegliere Add Backup (Aggiungi backup).
3. Nella schermata Create New Backup (Crea nuovo backup), in Filesystem (File system) scegliere Blank File System Backup (Backup file system vuoto) e quindi scegliere OK.
4. Nel nodo dell'albero in cui è visualizzato il sistema host selezionare uno o più file system di cui eseguire il backup e scegliere Next (Avanti) per continuare.
5. Aprire il nodo dell'albero per la libreria di nastri da usare, aprire il menu contestuale (clic con il pulsante destro del mouse) per l'unità nastro da usare e quindi scegliere Properties (Proprietà).
6. Scegliere il pool di supporti, fare clic su OK e quindi su Next (Avanti).
7. Per le tre schermate seguenti accettare le impostazioni predefinite e scegliere Next (Avanti).
8. Nella schermata Perform finishing steps in your backup/template design (Esegui fasi finali nel progetto di backup/modello) scegliere Save as (Salva con nome) per salvare la sessione. Nella finestra popup assegnare un nome al backup e assegnare il backup al gruppo in cui si desidera salvare la nuova specifica di backup.
9. Scegliere Start Interactive Backup (Avvia backup interattivo).

Se il sistema host contiene un sistema di database, è possibile sceglierlo come sistema di backup di destinazione. Le schermate e le selezioni sono simili a quelle per il backup del file system appena descritto.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire e l'unità nastro in Data Protector viene contrassegnata come Dirty. Data Protector contrassegna inoltre la qualità del nastro come scadente e impedisce la scrittura sul nastro. Per continuare a leggere i dati dal nastro, è

necessario pulire l'unità e rimontare il nastro. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente su un nuovo nastro.

Archiviazione di un nastro

Quando archivi un nastro, il gateway di nastri virtuali sposta il nastro dalla libreria di nastri allo storage offline. Prima di espellere e archiviare un nastro, controlla i relativi contenuti.

Per controllare il contenuto di un nastro prima dell'archiviazione

1. Scegliere Slots (Slot) e quindi scegliere il nastro da controllare.
2. Scegliere Objects (Oggetti) e controllare il contenuto sul nastro.

Dopo aver scelto un nastro da archiviare, usa la procedura seguente.

Per espellere e archiviare un nastro

1. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro e scegliere Eject (Espelli).
2. Nella console Storage Gateway selezionare il gateway, quindi scegliere VTL Tape Cartridges (Cartucce nastro VTL) e verificare lo stato del nastro virtuale che si sta archiviando.

Dopo che il nastro viene espulso, viene automaticamente archiviato nello storage offline (S3 Glacier Flexible Retrieval oppure S3 Glacier Deep Archive). Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro è IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro non è più elencato nella VTL ma è archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Ripristino dei dati da un nastro

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

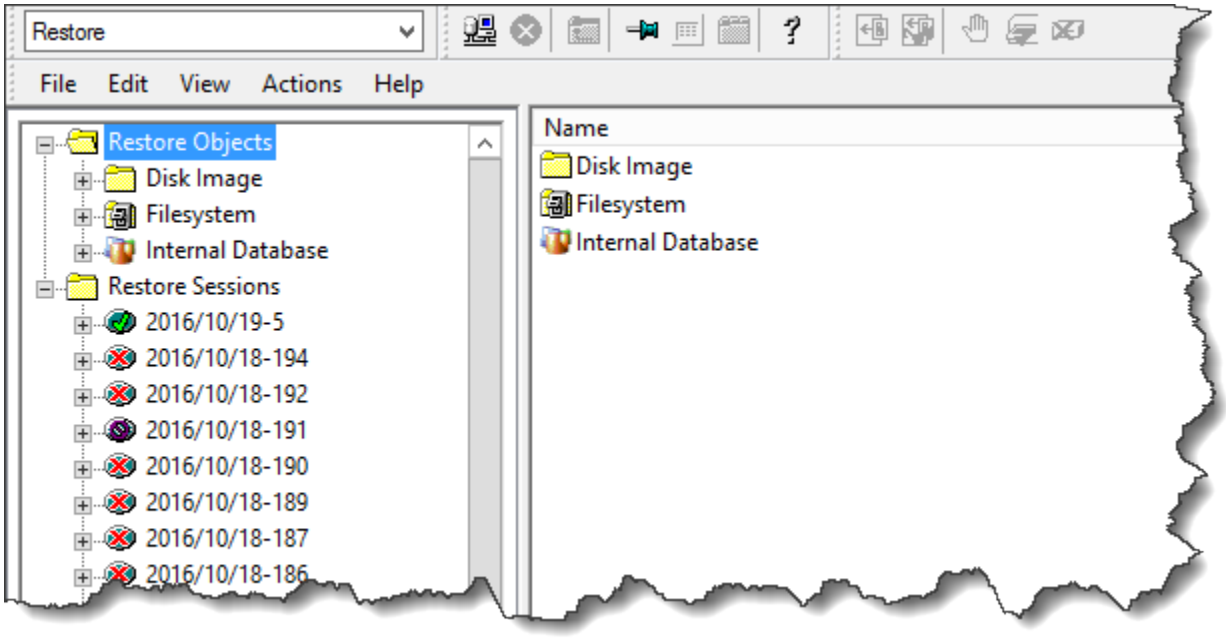
1. Recuperare il nastro archiviato su un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.

2. Usa HPE Data Protector per ripristinare i dati. Questo processo equivale a quello di ripristino dei dati da nastri fisici.

Per ripristinare i dati da un nastro, usa la procedura seguente.

Per ripristinare i dati da un nastro

1. Scegliere Restore (Ripristina) in alto a sinistra nello schermo.



2. Scegliere il file system o il sistema di database da ripristinare. Verificare che la casella relativa al backup da ripristinare sia selezionata. Scegli Restore (Ripristina).
3. Nella finestra Start Restore Session (Avvia sessione di ripristino) scegliere Needed Media (Supporti richiesti). Scegliere All media (Tutti i supporti). Dovrebbe venire visualizzato il nastro originariamente usato per il backup. Selezionare il nastro e quindi scegliere Close (Chiudi).
4. Nella finestra Start Restore Session (Avvia sessione di ripristino) accettare le impostazioni predefinite, scegliere Next (Avanti) e quindi scegliere Finish (Fine).

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione utilizzando Microsoft System Center Data Protection Manager

Puoi eseguire il backup dei dati su nastri virtuali, archiviare nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Microsoft System Center 2012 R2 o 2016 Data Protection Manager (DPM). In questo argomento viene illustrata la documentazione di base su come configurare l'applicazione di backup DPM per un gateway di nastri virtuali ed eseguire un'operazione di backup e ripristino.

Per informazioni dettagliate su come utilizzare DPM, consulta la documentazione di DPM sul sito web di Microsoft System Center. Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

Configurazione di DPM per il riconoscimento di dispositivi VTL

Dopo aver connesso i dispositivi della libreria di nastri virtuali al client Windows, puoi configurare DPM in modo che riconosca i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

Per impostazione predefinita, il server DPM non riconosce dispositivi gateway di nastri virtuali. Per configurare il server per l'utilizzo con i dispositivi gateway di nastri virtuali attieniti alla seguente procedura:

1. Aggiorna i driver dei dispositivi VTL in modo da esporli al server DPM.
2. Esegui manualmente la mappatura dei dispositivi VTL alla libreria di nastri DPM.

Per aggiornare i driver dei dispositivi VTL

- In Device Manager, aggiornare il driver per l'unità di sostituzione dei supporti. Per istruzioni, consulta Aggiornamento del driver del dispositivo per l'unità di sostituzione dei supporti.

Il DPM viene utilizzato DriveMappingTool per mappare le unità nastro alla libreria di nastri DPM.

Per mappare unità nastro alla libreria di nastri del server DPM

1. Creare almeno un nastro per il gateway. Per ulteriori informazioni su come effettuare tale operazione sulla console, consulta Creating Tapes (Creazione dei nastri).
2. Importare il nastro nella libreria DPM. Per informazioni su come fare, consulta Importazione di un nastro in DPM.
3. Se il servizio DPMLA è in esecuzione, arrestarlo aprendo un terminale comandi e digitando quanto segue nella riga di comando.

   ```
   net stop DPMLA
   ```

4. Individuare il seguente file nel server DPM: `%ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml`.

   > **Note**
   >
   > Se questo file esiste, il DPM lo sovrascriveDriveMappingTool . Se si desidera conservare il file originale, crearne una copia di backup.

5. Aprire un terminale comandi, modificare la directory in `%ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin` ed eseguire il comando riportato di seguito.

   ```
   C:\Microsoft System Center 2016 R2\DPM\DPM\bin>DPMDriveMappingTool.exe
   ```

   L'output del comando è simile al seguente.

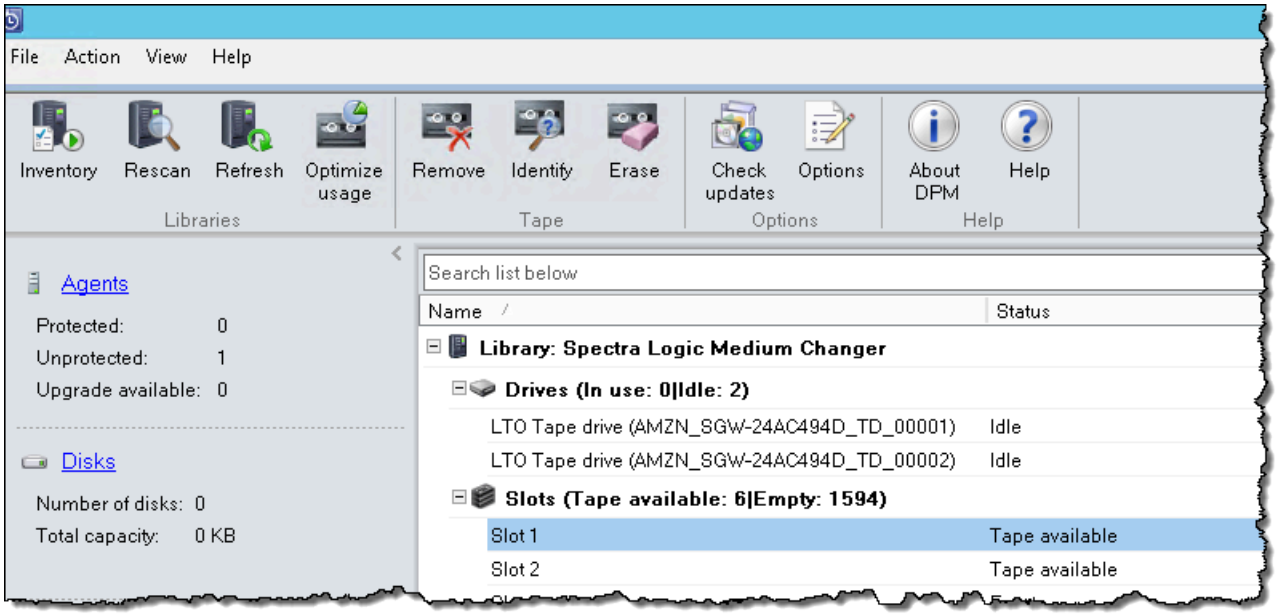
   ```
   Performing Device Inventory ...
   Mapping Drives to Library ...
   Adding Standalone Drives ...
   Writing the Map File ...
   Drive Mapping Completed Successfully.
   ```

Importazione di un nastro in DPM

È ora possibile importare i nastri dal gateway di nastri virtuali nella libreria di applicazioni di backup DPM.

Per importare nastri nella libreria di applicazioni di backup DPM

1. Sul server DPM, aprire la Console di gestione, scegliere Rescan (Ripeti analisi), quindi selezionare Refresh (Aggiorna). In questo modo vengono visualizzate le unità di sostituzione dei supporti e a nastro.



2. Aprire il menu contestuale (clic con il pulsante destro del mouse) dell'unità di sostituzione dei supporti nella sezione Library (Libreria), quindi scegliere Add tape (I/E port) (Aggiungi nastro - porta di importazione/esportazione) per aggiungere un nastro all'elenco Slots (Slot).

> **Note**
>
> Il processo di aggiunta di nastri può richiedere alcuni minuti.

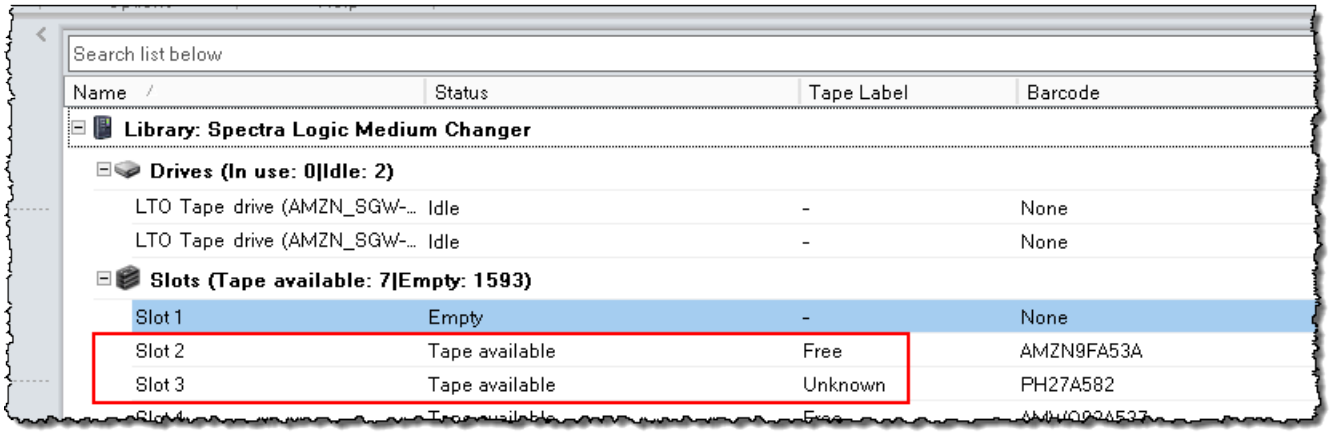
   Il nastro risulta contrassegnato con l'etichetta Unknown (Sconosciuto) e non può essere utilizzato. Affinché un nastro sia utilizzabile, deve essere identificato.

3. Aprire il menu contestuale (facendo clic con il pulsante destro del mouse) del nastro da identificare, quindi selezionare Identify unknown tape (Identifica nastro sconosciuto).

> **Note**
>
> Il processo di identificazione di nastri può richiedere alcuni secondi o minuti.
> Se i nastri non visualizzano correttamente i codici a barre, è necessario modificare il driver Media Changer in Sun/ Library. StorageTek Per ulteriori informazioni, consulta Visualizzazione di codici a barre per nastri in Microsoft System Center DPM.

Quando il processo di identificazione è stato completato, l'etichetta del nastro cambia in Free (Disponibile), a indicare che il nastro è disponibile per la scrittura dei dati.

Nel seguente screenshot, il nastro nello slot 2 è stato identificato ed è utilizzabile, mentre il nastro nello slot 3 non lo è.



Scrittura di dati su un nastro in DPM

Puoi scrivere i dati su un nastro virtuale del gateway di nastri virtuali utilizzando le stesse procedure e le stesse policy di protezione che si applicano ai nastri fisici. Puoi creare un gruppo di protezione e aggiungere i dati di cui desideri eseguire il backup, dopodiché puoi eseguire il backup dei dati creando un punto di ripristino. Per informazioni dettagliate su come utilizzare DPM, consulta la documentazione di DPM sul sito web di Microsoft System Center.

Per impostazione predefinita, la capacità di un nastro è di 30 GB. Quando esegui il backup di dati di dimensioni superiori alla capacità di un nastro, si verifica un errore di I/O del dispositivo. Se la posizione in cui si è verificato l'errore è di dimensioni superiori a quelle del nastro, Microsoft DPM tratta l'errore come un'indicazione di fine nastro. Se la posizione in cui si è verificato l'errore è di dimensioni inferiori a quelle del nastro, il processo di backup ha esito negativo. Per risolvere il

problema, modifica il valore `TapeSize` nella voce di registro in modo che corrisponda alle dimensioni del nastro. Per informazioni su come eseguire questa operazione, consulta ID errore: 30101 in Microsoft System Center.

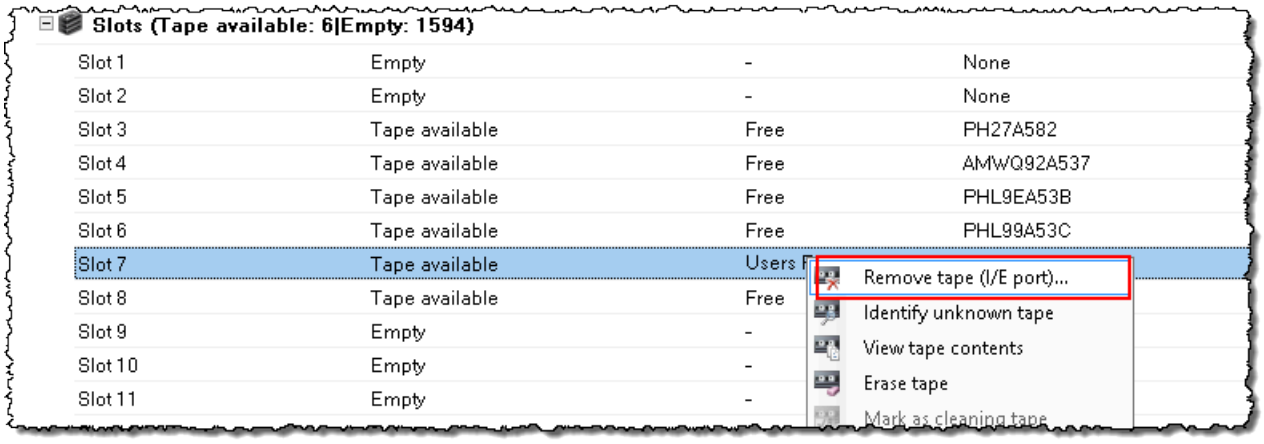
> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente.

Archiviazione di un nastro utilizzando DPM

Quando archivi un nastro, il gateway di nastri virtuali lo sposta dalla libreria di nastri DPM allo storage offline. Per iniziare il processo di archiviazione devi rimuovere il nastro dallo slot utilizzando la tua applicazione di backup - ossia DPM.

Per archiviare un nastro in DPM

1. Aprire il menu contestuale (facendo clic con il pulsante destro del mouse) del nastro da archiviare, quindi selezionare Remove tape (I/E port) (Rimuovi nastro - porta di importazione/esportazione).



2. Nella finestra di dialogo che viene visualizzata, scegliere Yes (Sì). L'operazione espelle il nastro dallo slot di storage dell'unità di sostituzione dei supporti e sposta il nastro in uno degli slot di importazione/esportazione del gateway. Quando un nastro viene spostato nello slot di importazione/esportazione del gateway, la procedura di archiviazione che lo riguarda ha subito inizio.

3. Nella console Storage Gateway selezionare il gateway, quindi scegliere VTL Tape Cartridges (Cartucce nastro VTL) e verificare lo stato del nastro virtuale che si sta archiviando.

   Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro è IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro esportato non è più elencato nella libreria di nastri virtuali.

Ripristino di dati da un nastro archiviato in DPM

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizzare l'applicazione di backup DPM per ripristinare i dati. L'operazione viene effettuata creando un punto di ripristino, come nel caso del ripristino di dati da nastri fisici. Per le istruzioni, consulta la sezione relativa al recupero di dati di un computer client nel sito web di DPM.

Fase successiva

Eliminazione delle risorse non necessarie

Verifica della configurazione utilizzando NovaStor DataCenter /Network

È possibile eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi VTL (Virtual Tape Library) utilizzando NovaStor DataCenter /Network versione 6.4 o 7.1. In questo argomento è disponibile la documentazione di base su come configurare l'applicazione di backup NovaStor DataCenter /Network versione 7.1 per un Tape Gateway ed eseguire operazioni di backup e ripristino. Per informazioni dettagliate su come utilizzare NovaStor DataCenter /Network versione 7.1, vedere Documentation /Network. NovaStor DataCenter

Configurazione di /Network NovaStor DataCenter

Dopo aver collegato i dispositivi VTL (Virtual Tape Library) al client Microsoft Windows, configuri il NovaStor software per riconoscere i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

NovaStor DataCenter/Network richiede driver forniti dai produttori dei driver. Puoi utilizzare i driver di Windows, ma devi prima disattivare altre applicazioni di backup.

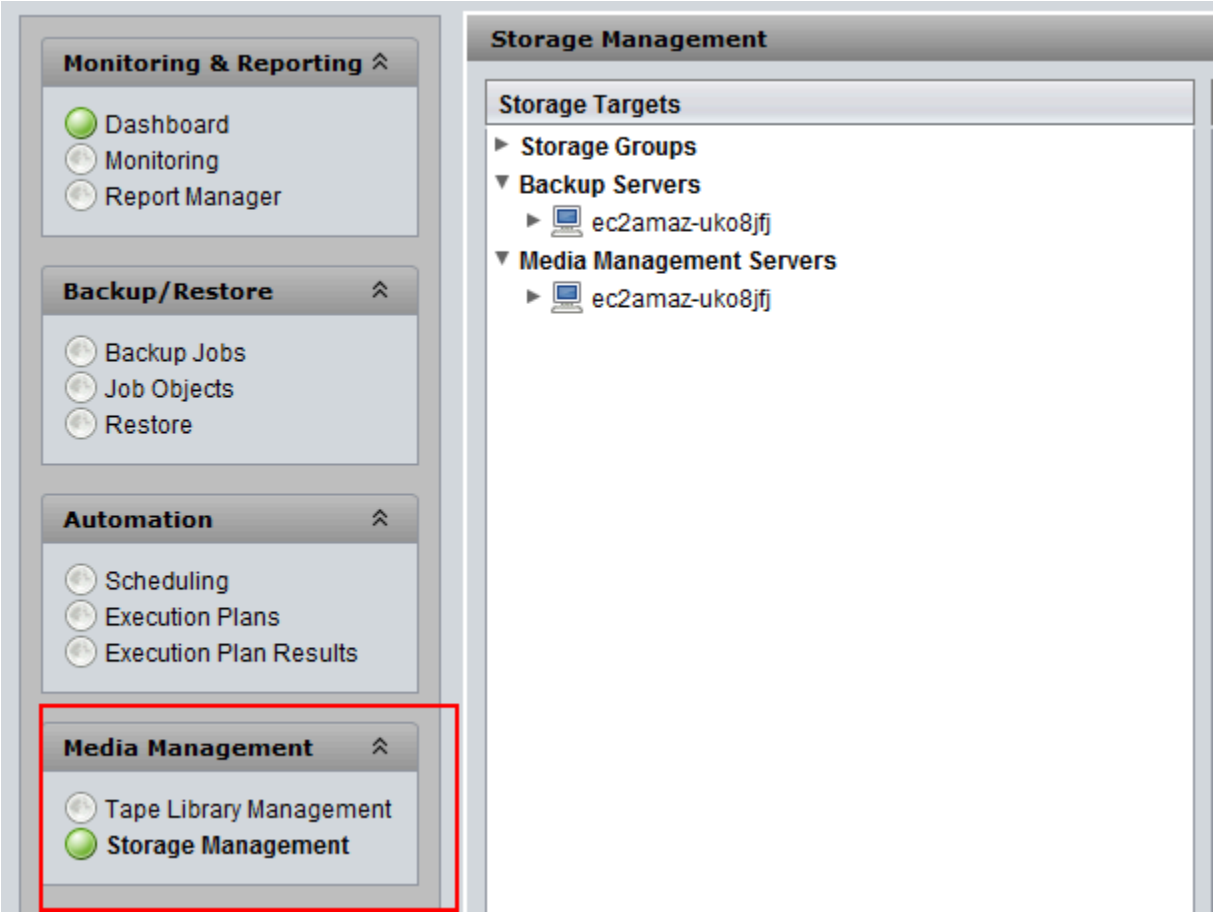
Configurazione di NovaStor DataCenter /Network per l'utilizzo con i dispositivi VTL

Durante la configurazione dei dispositivi VTL per l'utilizzo con NovaStor DataCenter /Network versione 6.4 o 7.1, è possibile che venga visualizzato un messaggio di errore che recita: `External Program did not exit correctly` Prima di poter continuare, deve risolvere questo problema.

Puoi prevenire il verificarsi del problema creando la soluzione alternativa prima di iniziare a configurare i dispositivi VTL. Per informazioni su come creare la soluzione alternativa, consulta Risoluzione di un errore "External Program Did Not Exit Correctly" (Chiusura programma esterno non corretta).

Per configurare /Network in modo che funzioni con i dispositivi NovaStor DataCenter VTL

1. Nella console NovaStor DataCenter /Network Admin, scegli Media Management, quindi scegli Storage Management.

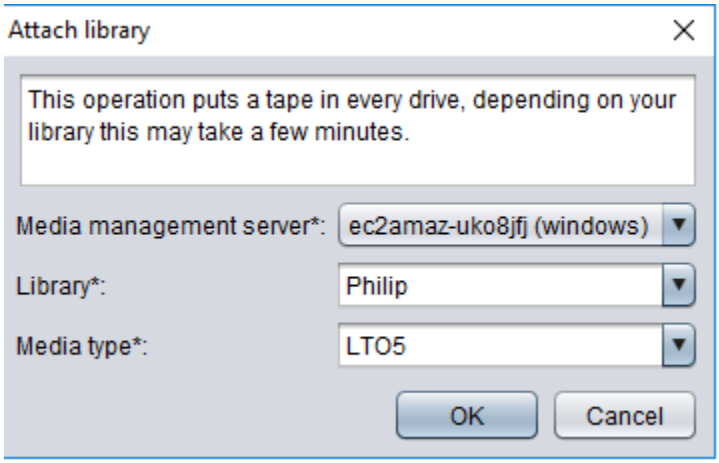


2. Nel menu Storage Targets (Target di storage), aprire il menu contestuale (clic con il pulsante destro del mouse) di Media Management Servers (Server di gestione supporti), scegliere New (Nuovo) e selezionare OK per creare e prepopolare un nodo di storage.

   Se viene visualizzato il messaggio di errore `External Program did not exit correctly`, risolvere il problema prima di continuare. Questo problema richiede una soluzione alternativa. Per informazioni su come risolvere il problema, consulta Risoluzione di un errore "External Program Did Not Exit Correctly" (Chiusura programma esterno non corretta).

   > **Important**
   >
   > Questo errore si verifica perché l'intervallo di assegnazione degli elementi tra le unità AWS Storage Gateway di archiviazione e le unità a nastro supera il numero consentito da /Network. NovaStor DataCenter

3. Aprire il menu contestuale (clic con il pulsante destro del mouse) del nodo storage che è stato creato e scegliere New library (Nuova libreria).
4. Scegliere il server della libreria dall'elenco. L'elenco della libreria viene popolato automaticamente.
5. Assegnare un nome alla libreria e scegliere OK.
6. Scegliere la libreria per visualizzare tutte le proprietà della libreria di nastri virtuali in Storage Gateway.
7. Nel menu Storage Targets (Destinazioni di storage), espandere Backup Servers (Server di backup), aprire il menu contestuale (clic con il pulsante destro del mouse) e scegliere Attach Library (Collega libreria).
8. Nella finestra di dialogo Attach Library (Collega libreria) visualizzata, scegliere il tipo di supporto LTO5 e selezionare OK.



9. Espandere Backup Servers (Server di backup) per visualizzare la libreria di nastri virtuali di Storage Gateway e la partizione della libreria che mostra tutte le unità nastro installate.

Creazione di un pool di nastri

Un pool di nastri viene creato dinamicamente nel software NovaStor DataCenter /Network e quindi non contiene un numero fisso di supporti. Un pool di nastri che richiede un nastro lo ottiene dal relativo pool di lavoro. Un pool di lavoro è un contenitore di nastri che possono essere utilizzati liberamente da uno o più pool di nastri. Un pool di nastri restituisce al pool di lavoro i supporti che hanno superato il periodo di conservazione e che non sono più necessari.

La creazione di un pool di nastri avviene in tre fasi:

1. Creazione di un pool di lavoro.
2. Assegnazione di nastri al pool di lavoro.
3. Creazione di un pool di nastri.

Per creare un pool di lavoro

1. Nel menu di navigazione a sinistra, scegliere la scheda Scratch Pools (Pool di lavoro).
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) di Scratch Pools (Pool di lavoro), quindi scegliere Create Scratch Pool (Crea pool di lavoro).
3. Nella finestra di dialogo Scratch Pools (Pool di lavoro), assegnare un nome al pool di lavoro, quindi selezionare il tipo di supporto.
4. Scegliere Label Volume (Volume etichetta) e creare un limite minimo per il pool di lavoro. Quando il pool di lavoro raggiunge il limite minimo, viene visualizzato un avviso.

5. Nella finestra di dialogo di avviso visualizzata scegliere OK per creare il pool di lavoro.

Per assegnare nastri a un pool di lavoro.

1. Nel menu di navigazione a sinistra, scegliere Tape Library Managements (Gestione libreria di nastri).
2. Selezionare la scheda Library (Libreria) per visualizzare l'inventario della libreria.
3. Scegli i nastri che si desidera assegnare al pool di lavoro. Assicurarsi che i nastri siano configurati per il tipo di supporto corretto.
4. Aprire il menu contestuale (clic con il pulsante destro del mouse) della libreria e scegliere Add to Scratch Pool (Aggiungi al pool di lavoro).

Ora il contenuto del pool di lavoro può essere utilizzato per i pool di nastri.

Per creare un pool di nastri

1. Dal menu di navigazione a sinistra, scegliere Tape Library Managements (Gestione libreria di nastri).
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) di Media Pools (Pool di supporti), quindi scegliere Create Media Pool (Crea pool di supporti).
3. Assegnare un nome al pool di supporti e scegliere Backup Server (Server di backup).
4. Scegliere una partizione della libreria per il pool di supporti.
5. Scegliere il pool di lavoro da cui si desidera ottenere i nastri.
6. Per Schedule (Pianificazione), selezionare Not Scheduled (Non pianificato).

Configurazione dell'importazione e dell'esportazione di supporti per l'archiviazione di nastri

NovaStor DataCenter/Network può utilizzare gli slot di importazione/esportazione se fanno parte del media changer.

Per un'esportazione, NovaStor DataCenter /Network deve sapere quali nastri verranno fisicamente rimossi dalla libreria.

Per l'importazione, NovaStor DataCenter /Network riconosce i supporti a nastro esportati nella libreria a nastro e offre la possibilità di importarli tutti, da uno slot di dati o da uno slot di esportazione. Il

gateway di nastri virtuali archivia i nastri nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive).

Per configurare l'importazione e l'esportazione di supporti

1. Accedere a Tape Library Management (Gestione libreria di nastri), scegliere un server per Media Management Server (Server di gestione supporti), quindi selezionare Library (Libreria).
2. Selezionare la scheda Off-site Locations (Posizioni esterne).
3. Aprire il menu contestuale (clic con il pulsante destro del mouse) dell'area bianca e scegliere Add (Aggiungi) per aprire un nuovo pannello.
4. Nel pannello, digitare **`S3 Glacier Flexible Retrieval`** o **`S3 Glacier Deep Archive`** e aggiungere una descrizione facoltativa nella casella di testo.

Backup dei dati su nastro

Puoi creare un processo di backup e scrivere i dati su un nastro virtuale utilizzando le stesse procedure valide per i nastri fisici. Per informazioni dettagliate su come eseguire il backup dei dati utilizzando il NovaStor software, vedere Documentation NovaStor DataCenter /Network.

> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup fallirà e il nastro diventerà non scrivibile. È possibile archiviare il nastro o continuare a leggere i dati da esso. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente su un nuovo nastro.

Archiviazione di un nastro

Quando archivi un nastro, il gateway di nastri virtuali lo trasferisce dall'unità a nastro allo slot di storage. Quindi esporta il nastro dallo slot all'archivio utilizzando l'applicazione di backup, ovvero / Network. NovaStor DataCenter

Per archiviare un nastro

1. Nel menu di navigazione a sinistra, scegliere Tape Library Managements (Gestione libreria di nastri).
2. Selezionare la scheda Library (Libreria) per visualizzare l'inventario della libreria.

3. Evidenziare i nastri da archiviare, aprire il menu contestuale (facendo clic con il pulsante destro del mouse) dei nastri e scegliere la posizione di archiviazione esterna.

Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro esportato non è più elencato nella libreria di nastri virtuali.

In NovaStor DataCenter /Network, verifica che il nastro non si trovi più nello slot di archiviazione.

Nel riquadro di navigazione della console Storage Gateway selezionare Tapes (Nastri). Verificare che lo stato del nastro archiviato sia ARCHIVED (ARCHIVIATO).

Ripristino di dati da un nastro archiviato e recuperato

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizzare il software NovaStor DataCenter /Network per ripristinare i dati. A questo scopo, aggiornare lo slot di inserimento/espulsione e trasferire ciascun nastro da recuperare in uno slot vuoto, in modo analogo a quanto avviene durante il ripristino dei dati da nastri fisici. Per informazioni sul ripristino dei dati, vedere Documentation NovaStor DataCenter /Network.

Scrittura di più processi di backup su un'unità nastro contemporaneamente

Nel NovaStor software, è possibile scrivere più lavori su un'unità nastro contemporaneamente utilizzando la funzione di multiplexing. Questa funzione è attiva quando è disponibile un multiplexer per un pool di supporti. Per informazioni su come utilizzare il multiplexing, vedere Documentation / Network. NovaStor DataCenter

Risoluzione di un errore "External Program Did Not Exit Correctly" (Chiusura programma esterno non corretta)

Durante la configurazione dei dispositivi VTL per l'utilizzo con NovaStor DataCenter /Network versione 6.4 o 7.1, è possibile che venga visualizzato un messaggio di errore che recita: `External`

`Program did not exit correctly` Questo errore si verifica perché l'intervallo di assegnazione degli elementi da Storage Gateway alle unità di archiviazione e alle unità a nastro supera il numero consentito da NovaStor DataCenter /Network.

Storage Gateway restituisce 3200 slot di archiviazione e importazione/esportazione, ovvero più del limite di 2400 consentito da /Network. NovaStor DataCenter Per risolvere questo problema, si aggiunge un file di configurazione che attiva il NovaStor software per limitare il numero di slot di archiviazione e di importazione/esportazione e preconfigura l'intervallo di assegnazione degli elementi.

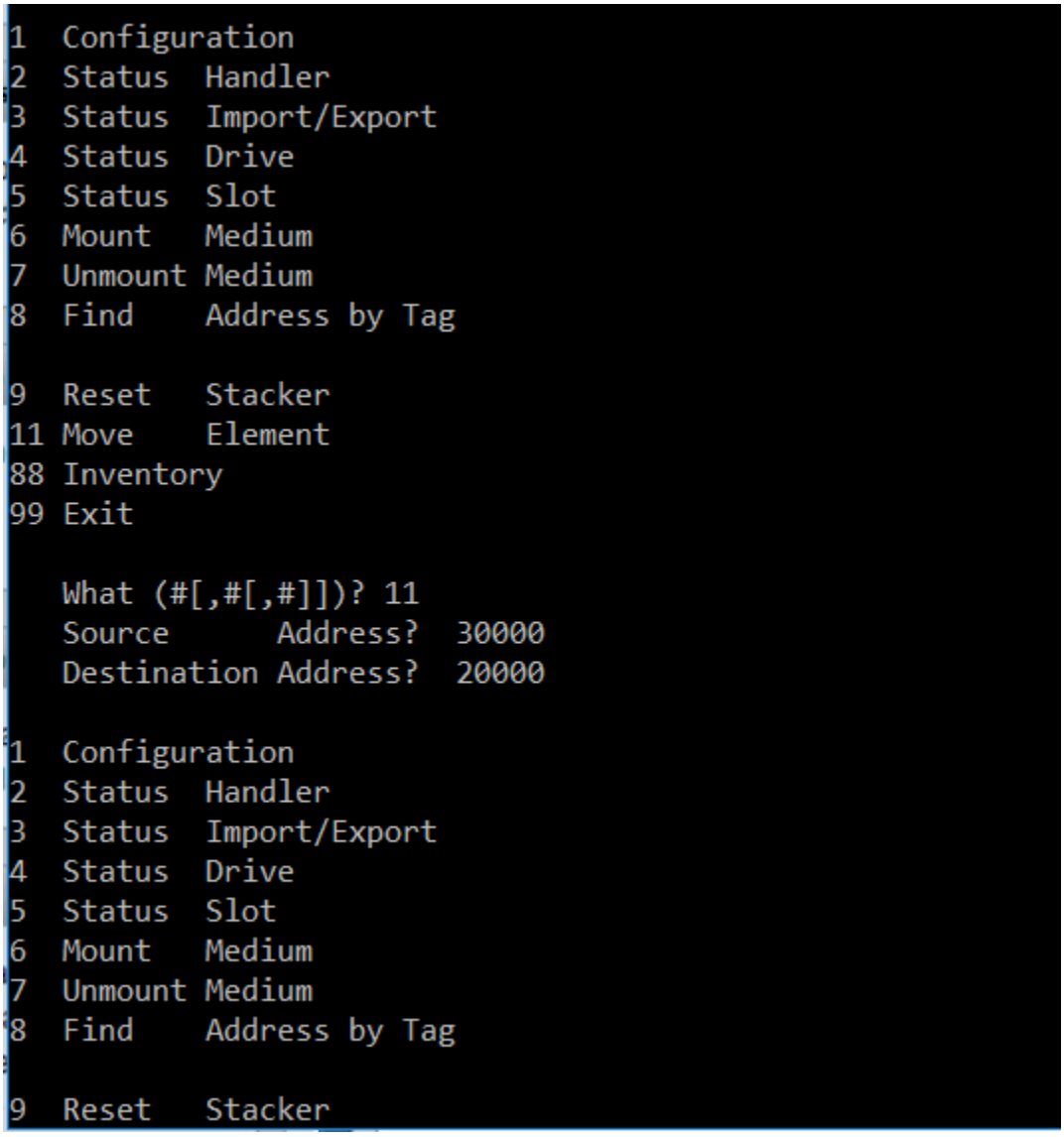
Per applicare la soluzione alternativa per un errore "External program did not exit correctly" (Chiusura programma esterno non corretta)

1. Accedete alla cartella Tape sul computer in cui avete installato il software. NovaStor
2. Nella cartella Tape (Nastri), creare un file di testo con il nome `hijacc.ini`.
3. Copiare il seguente contenuto, incollarlo nel file `hijacc.ini` e salvare il file.

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Aggiungere e collegare la libreria al server di gestione dei supporti.
5. Spostare un nastro dallo slot di importazione/esportazione nella libreria utilizzando il comando seguente, come illustrato nello screenshot qui sotto. Nel comando, sostituire VTL con il nome della propria libreria.

```
C:\Program Files\NovaStor\DataCenter\Hiback\tape>ophijacc.exe -c VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg

1  Configuration
2  Status  Handler
3  Status  Import/Export
4  Status  Drive
5  Status  Slot
6  Mount   Medium
7  Unmount Medium
8  Find    Address by Tag

9  Reset   Stacker
11 Move    Element
88 Inventory
99 Exit

   What (#[,#[,#]])? 1
Handlers     :   1   Address: 0
Import/Export:  30   Address: 30000
Drives       :  10   Address: 10000
Slots        :  200   Address: 20000
```



6. Collegare la libreria al server di backup.
7. Nel NovaStor software, importate tutti i nastri dagli slot di importazione/esportazione nella libreria.

Test della configurazione utilizzando Quest NetVault Backup

È possibile eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi VTL (Virtual Tape Library) utilizzando le seguenti versioni di backup di Quest (precedentemente Dell): NetVault

- NetVault Backup Quest 12.4
- NetVault Backup Quest 13.x

In questo argomento, è possibile trovare la documentazione di base su come configurare l'applicazione Quest NetVault Backup per un Tape Gateway ed eseguire un'operazione di backup e ripristino.

Per informazioni dettagliate su come utilizzare l'applicazione Quest NetVault Backup, consulta la Quest NetVault Backup — Administration Guide. Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

- Configurazione di Quest NetVault Backup per funzionare con i dispositivi VTL
- Backup dei dati su nastro in Quest NetVault Backup
- Archiviazione di un nastro utilizzando Quest Backup NetVault
- Ripristino dei dati da un nastro archiviato in Quest Backup NetVault

Configurazione di Quest NetVault Backup per funzionare con i dispositivi VTL

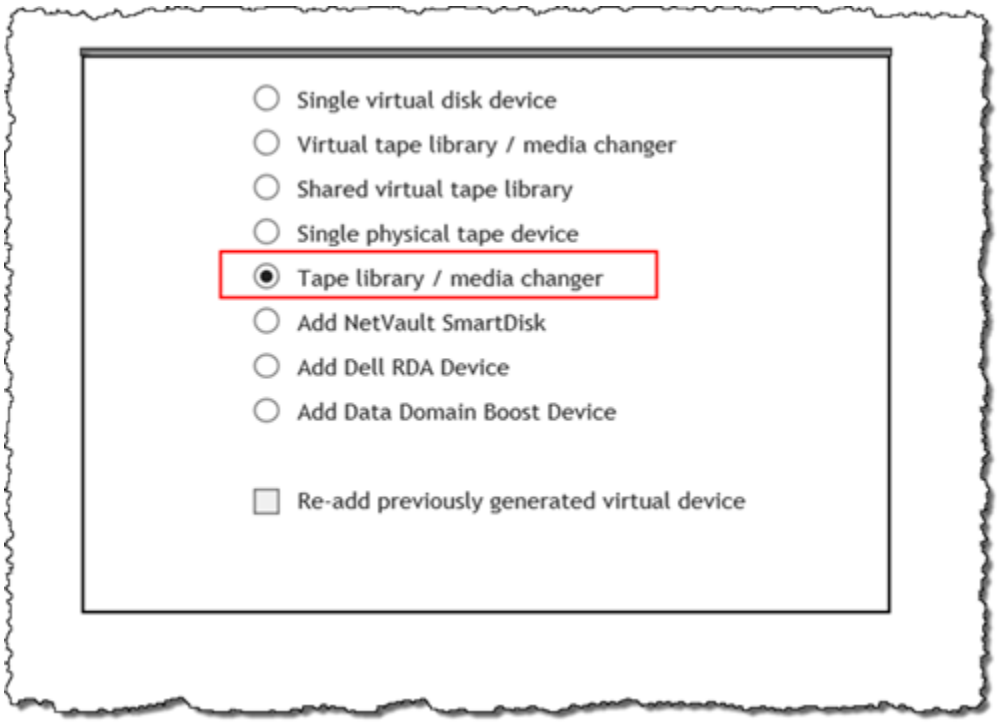
Dopo aver collegato i dispositivi Virtual Tape Library (VTL) al client Windows, configuri Quest NetVault Backup per riconoscere i tuoi dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

L'applicazione Quest NetVault Backup non riconosce automaticamente i dispositivi Tape Gateway. È necessario aggiungere manualmente i dispositivi per esporli all'applicazione Quest NetVault Backup e quindi scoprire i dispositivi VTL.

Aggiunta di dispositivi VTL

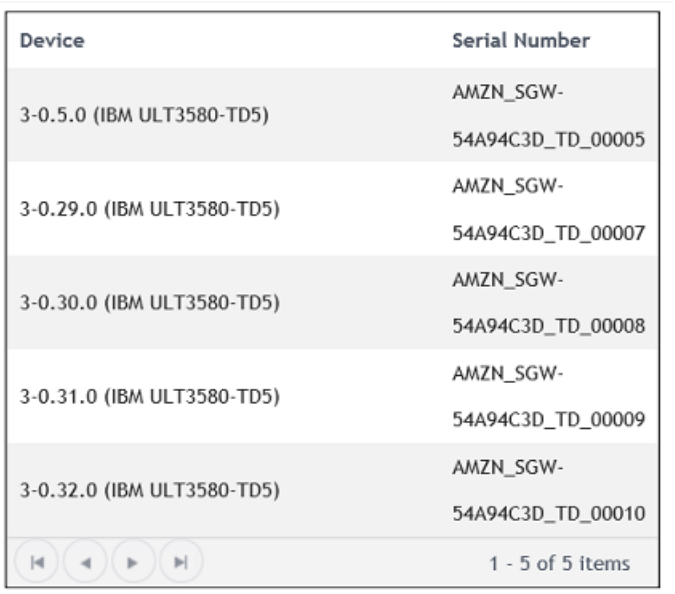
Per aggiungere i dispositivi VTL

1. In Quest NetVault Backup, scegli Gestisci dispositivi nella scheda Configurazione.
2. Nella pagina Manage Devices (Gestisci dispositivi) scegliere Add Devices (Aggiungi dispositivi).
3. Nella procedura guidata di aggiunta di storage scegliere Tape library / media changer (Libreria di nastri/Unità di sostituzione dei supporti) e quindi scegliere Next (Avanti).



4. Nella pagina successiva scegliere il computer client fisicamente collegato alla libreria e fare clic su Next (Avanti) per eseguire la scansione per la ricerca dei dispositivi.
5. Se i dispositivi vengono trovati, vengono visualizzati. In questo caso, l'unità di sostituzione dei supporti viene visualizzata nella casella del dispositivo.
6. Scegliere l'unità di sostituzione dei supporti e quindi Next (Avanti). Nella procedura guidata vengono visualizzate informazioni dettagliate sul dispositivo.
7. Nella pagina Add Tapes to Bays (Aggiungi nastri ad alloggiamenti) scegliere Scan For Devices (Cerca dispositivi), scegliere il computer client e quindi fare clic su Next (Avanti).

   Nella pagina vengono visualizzate tutte le unità. Quest NetVault Backup mostra i 10 alloggiamenti a cui è possibile aggiungere le unità. Gli alloggiamenti vengono visualizzati uno alla volta.



Device	Serial Number
3-0.5.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00005
3-0.29.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00007
3-0.30.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00008
3-0.31.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00009
3-0.32.0 (IBM ULT3580-TD5)	AMZN_SGW-54A94C3D_TD_00010

1 - 5 of 5 items

8. Scegliere l'unità da aggiungere all'alloggiamento visualizzato e quindi scegliere Next (Avanti).

> **Important**
>
> Quando si aggiunge un'unità a un alloggiamento, i numeri dell'unità e dell'alloggiamento devono corrispondere. Se, ad esempio, viene visualizzato l'alloggiamento 1, è necessario aggiungere l'unità 1. Se un'unità non è connessa, lasciare vuoto l'alloggiamento corrispondente.

9. Quando il computer client viene visualizzato, selezionarlo e quindi scegliere Next (Avanti). Il computer client può venire visualizzato più volte.
10. Quando le unità vengono visualizzate, ripetere le fasi da 7 a 9 per aggiungere tutte le unità agli alloggiamenti.
11. Nella scheda Configuration (Configurazione) scegliere Manage devices (Gestisci dispositivi) e nella pagina Manage devices (Gestisci dispositivi) espandere l'unità di sostituzione dei supporti per visualizzare i dispositivi aggiunti.

Backup dei dati su nastro in Quest NetVault Backup

È possibile creare un processo di backup e scrivere i dati su un nastro virtuale usando le stesse procedure usate con nastri fisici. Per informazioni dettagliate su come eseguire il backup dei dati, consulta la Quest NetVault Backup - Administration Guide.

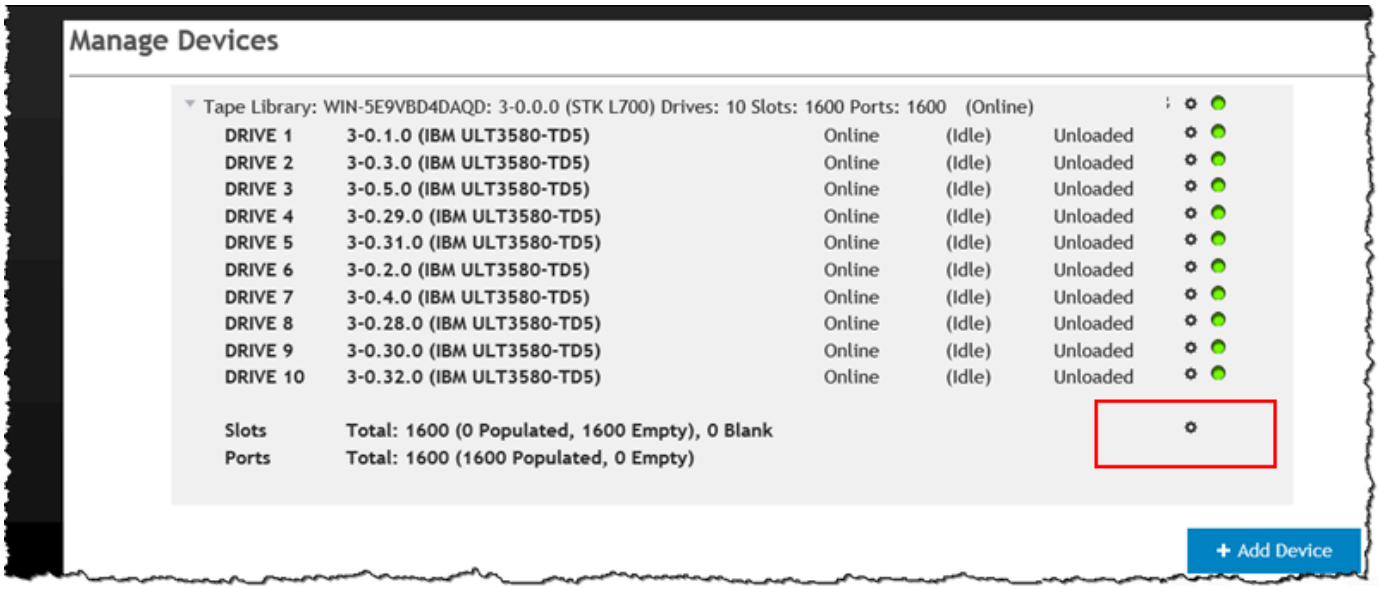
> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente.

Archiviazione di un nastro utilizzando Quest Backup NetVault

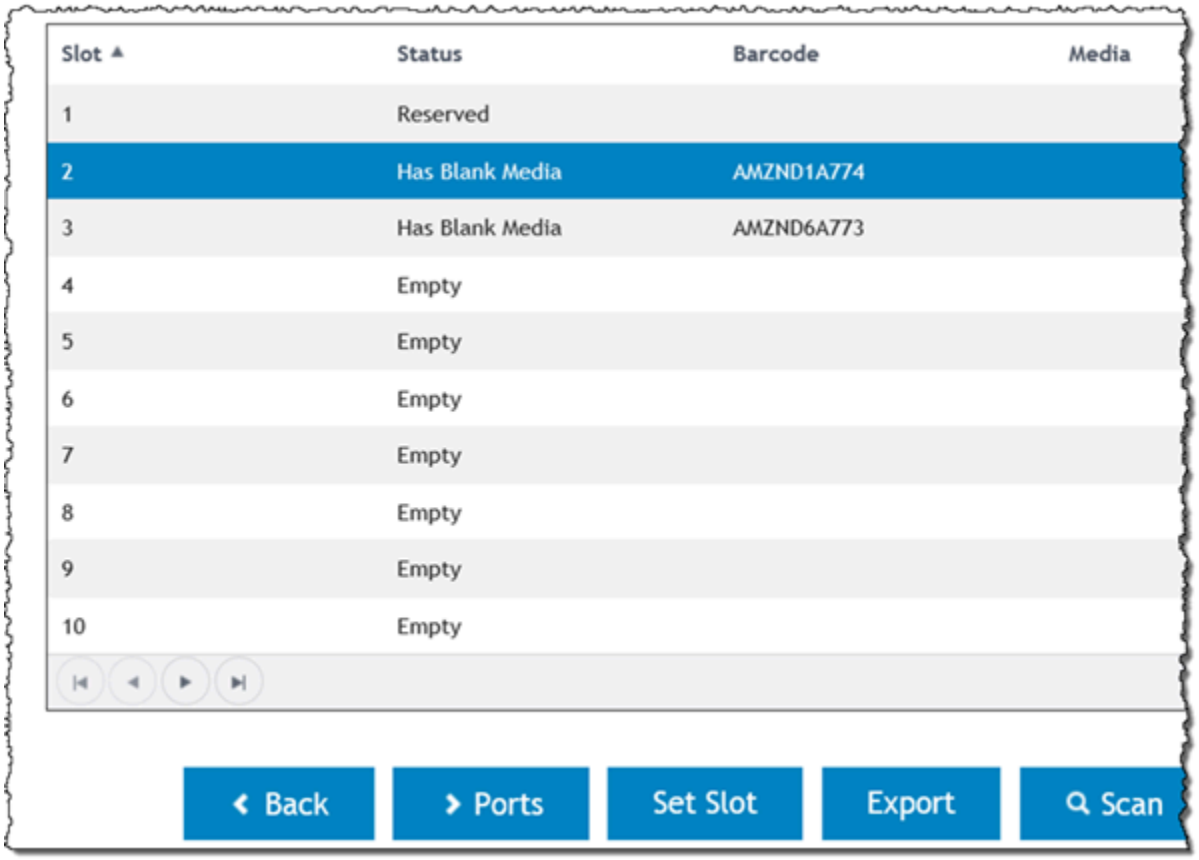
Quando archivi un nastro, il gateway di nastri virtuali lo trasferisce dall'unità a nastro allo slot di storage. Quindi esporta il nastro dallo slot all'archivio utilizzando l'applicazione di backup, ovvero Quest Backup. NetVault

Per archiviare un nastro in Quest NetVault Backup

1. Nella scheda Configurazione NetVault di Quest Backup, scegli ed espandi il tuo media changer per vedere i tuoi nastri.
2. Nella riga Slots (Slot) scegliere l'icona delle impostazioni per aprire Slots Browser (Esplora slot) per l'unità di sostituzione dei supporti.



3. Negli slot individuare il nastro da archiviare, selezionarlo e quindi scegliere Export (Esporta).



Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro esportato non è più elencato nella libreria di nastri virtuali.

Nel software Quest NetVault Backup, verifica che il nastro non sia più nello slot di archiviazione.

Nel riquadro di navigazione della console Storage Gateway selezionare Tapes (Nastri). Verificare che lo stato del nastro archiviato sia ARCHIVED (ARCHIVIATO).

Ripristino dei dati da un nastro archiviato in Quest Backup NetVault

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.

2. Usa l'applicazione Quest NetVault Backup per ripristinare i dati. A questo scopo, devi ripristinare una cartella, come fai per il ripristino dei dati da nastri fisici. Per istruzioni sulla creazione di un processo di ripristino, vedere Quest NetVault Backup - Administration Guide.

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione tramite Veeam Backup & Replication

Puoi eseguire il backup dei dati su nastri virtuali, archiviare nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Veritas Backup & Replication 11A. In questo argomento, puoi trovare la documentazione di base su come configurare il software Veeam Backup & Replication per un gateway di nastri virtuali ed eseguire un'operazione di backup e ripristino. Per informazioni dettagliate su come usare il software Veeam, consulta la documentazione backup e replica di Veeam in Veeam Help Center. Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

- Configurazione di Veeam per gestire i dispositivi VTL
- Importazione di un nastro in Veeam
- Backup dei dati su nastro in Veeam
- Archiviazione di un nastro mediante Veeam
- Ripristino dei dati da un nastro archiviato in Veeam

Configurazione di Veeam per gestire i dispositivi VTL

Dopo aver connesso i dispositivi della libreria di nastri virtuali al client Windows, puoi configurare Veeam Backup & Replication affinché riconosca i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

Aggiornamento dei driver dei dispositivi VTL

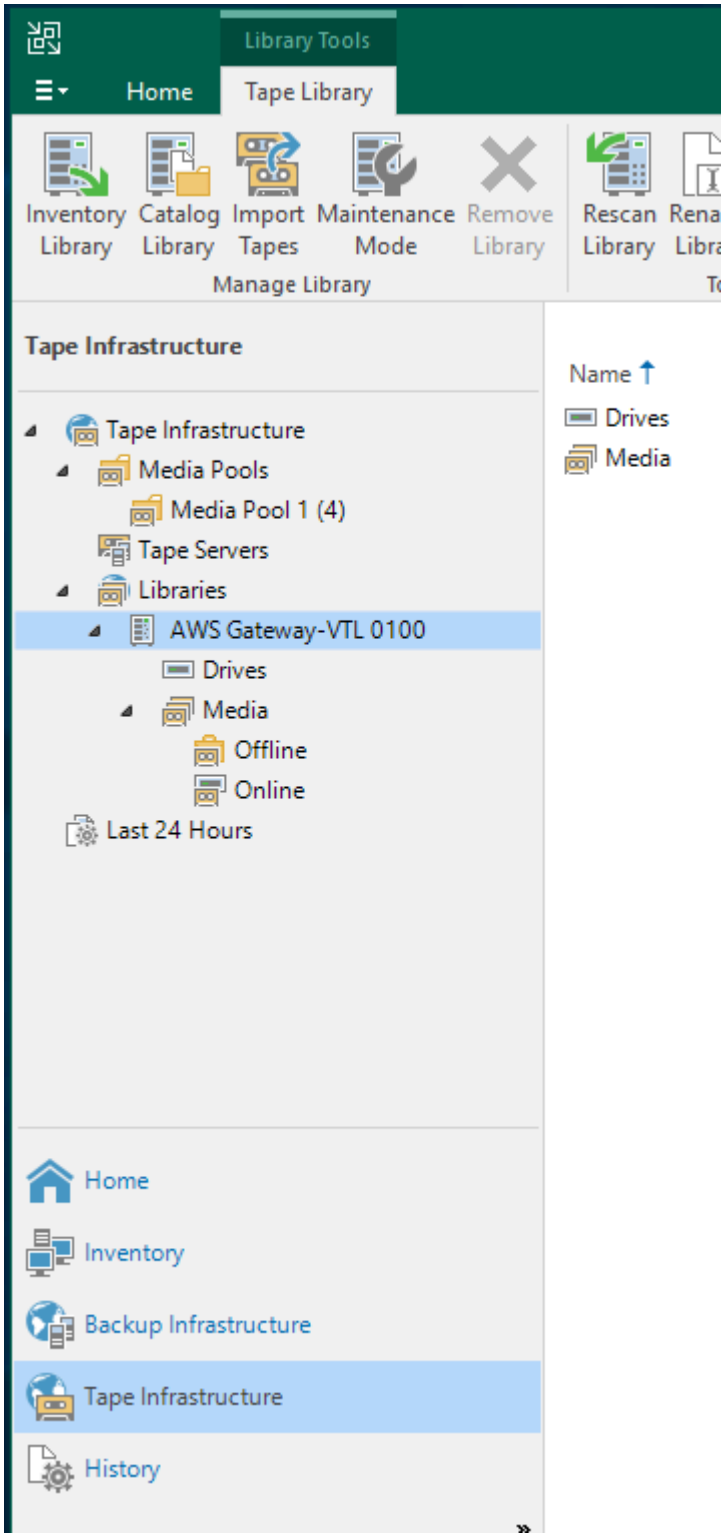
Per configurare il software in modo che funzioni con dispositivi gateway di nastri virtuali, aggiorna i driver di dispositivo per i dispositivi VTL per esporli al software Veeam e quindi individuare i dispositivi VTL. In Device Manager, aggiornare il driver per l'unità di sostituzione dei supporti. Per istruzioni, consulta Aggiornamento del driver del dispositivo per l'unità di sostituzione dei supporti.

Rilevamento di dispositivi VTL

È necessario utilizzare comandi SCSI nativi piuttosto che un driver Windows per scoprire la libreria di nastri se l'unità di sostituzione è sconosciuta. Per istruzioni dettagliate, consulta Librerie di nastri.

Per rilevare dispositivi VTL

1. Nel software Veeam, selezionare Tape infrastructure (Infrastruttura del nastro). Quando il gateway di nastri virtuali è connesso, i nastri virtuali sono elencati nella scheda Tape Infrastructure (Infrastruttura del nastro).



2. Espandere la struttura ad albero Tape (Nastro) per vedere le unità nastro e l'unità di sostituzione dei supporti.

3. Espandere la struttura ad albero delle unità di sostituzione dei supporti. Se le unità nastro sono mappate all'unità di sostituzione dei supporti, le unità verranno visualizzate in Drives (Unità). In caso contrario, la tua libreria di nastri e unità nastro appaiono come separare i dispositivi.

   Se le unità non sono mappate automaticamente, segui le istruzioni sul sito web Veeam per mappare le unità.

Importazione di un nastro in Veeam

È ora possibile importare i nastri dal gateway di nastri virtuali nella libreria di applicazioni per il backup Veaam.

Per importare un nastro nella libreria Veeam

1. Aprire il menu contestuale (clic con il pulsante destro del mouse) per una unità di sostituzione dei supporti e quindi scegliere Import (Importa) per importare i nastri sugli slot di importazione/esportazione.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) per una unità di sostituzione dei supporti e scegliere Inventory Library (Libreria inventario) per identificare nastri non riconosciuti. Quando si carica un nuovo nastro virtuale in una unità nastro per la prima volta, il nastro non è riconosciuto dall'applicazione per il backup Veeam. Per identificare i nastri non riconosciuti, fare l'inventario dei nastri nella libreria di nastri.

Backup dei dati su nastro in Veeam

Il backup dei dati su nastro è un processo in due fasi:

1. Creare un pool di supporti e aggiungervi il nastro.
2. Scrivere i dati sul nastro.

Puoi creare un pool di supporti e scrivere i dati su un nastro virtuale seguendo le stesse procedure che utilizzi con nastri fisici. Per informazioni dettagliate su come eseguire il backup dei dati, consulta Iniziare con i nastri in Veeam Help Center.

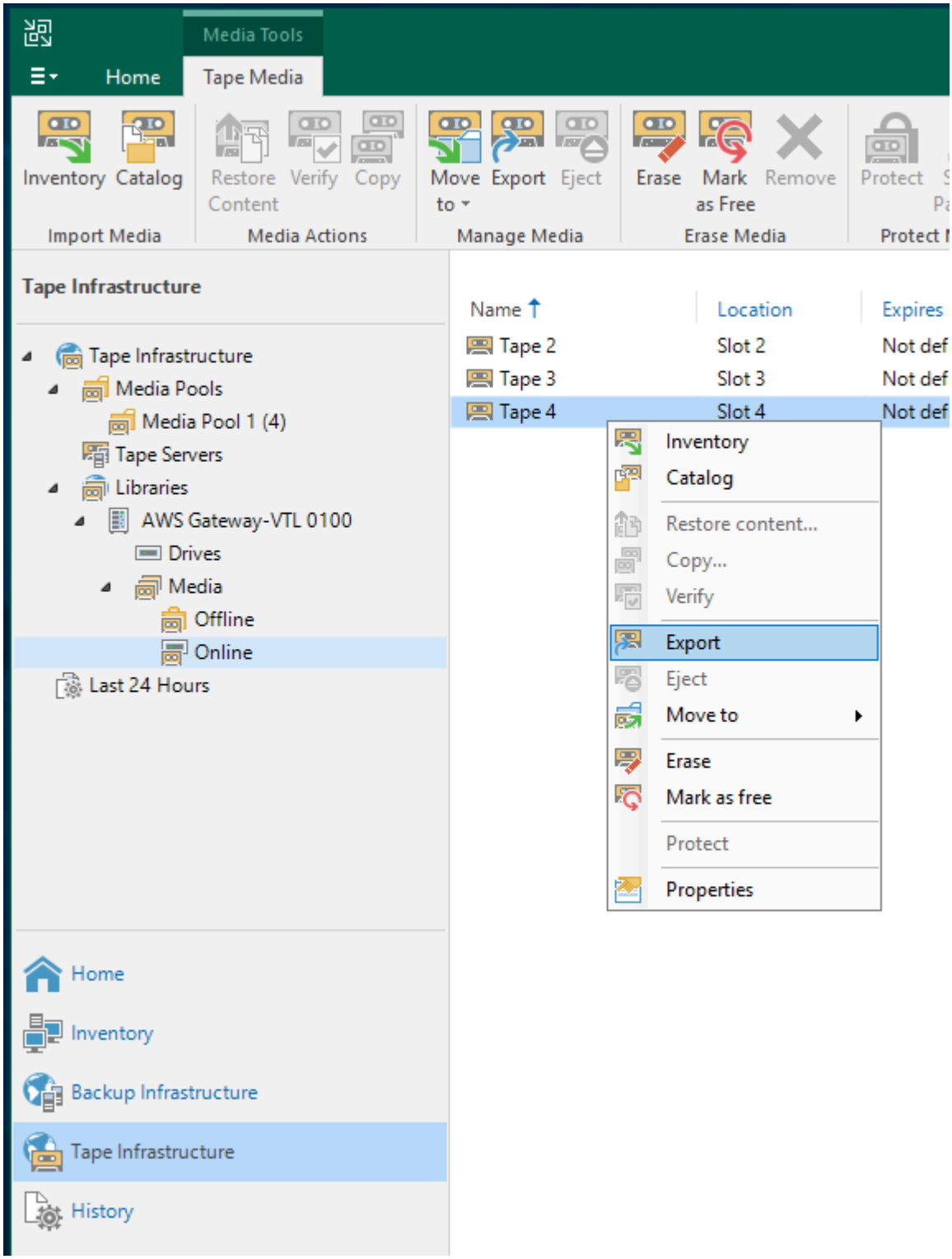
> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente.

Archiviazione di un nastro mediante Veeam

Quando archivi un nastro, il gateway di nastri virtuali sposta il nastro dalla libreria di nastri Veeam allo storage offline. Puoi iniziare l'archiviazione di nastri da espellere dalle unità a nastro allo slot di storage, quindi esportare il nastro dallo slot all'archivio utilizzando l'applicazione di backup - ovvero il software Veeam.

Per archiviare un nastro nella libreria Veeam

1. Selezionare Tape Infrastructure (Infrastruttura del nastro), quindi il pool di supporti contenente il nastro da archiviare.



2. Aprire il menu contestuale (facendo clic con il pulsante destro del mouse) per il nastro da archiviare, quindi selezionare Eject Tape (Espelli nastro).
3. Per Ejecting tape (Espulsione nastro), selezionare Close (Chiudi). La posizione del nastro cambia da un'unità nastro a uno slot.

4. Aprire nuovamente il menu contestuale (clic con il pulsante destro del mouse) per il nastro, quindi seleziona Export (Esporta). Lo stato del nastro passa da Tape drive (Unità nastro) a Offline.
5. Per Exporting tape (Esportazione nastro), selezionare Close (Chiudi). L'ubicazione del nastro passa da Slot a Offline.
6. Nella console Storage Gateway, selezionare il gateway, quindi scegliere VTL Tape Cartridges (Cartucce nastro VTL) e verificare lo stato del nastro virtuale che si sta archiviando.

   Il processo di archiviazione potrebbe richiedere del tempo. Lo stato iniziale del nastro appare come IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato diventa ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione viene completata, il nastro non è più elencato nella VTL ma è archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

Ripristino dei dati da un nastro archiviato in Veeam

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato dall'archivio in un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizzare il software Veeam per ripristinare i dati. A questo scopo, devi ripristinare una cartella, come fai per il ripristino dei dati da nastri fisici. Per istruzioni, consulta ripristino di dati da un nastro in Veeam Help Center.

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione tramite Veritas Backup Exec

Puoi eseguire il backup dei dati su nastri virtuali, archiviare nastri e gestire dispositivi della libreria di nastri virtuali (VTL) utilizzando Veritas Backup Exec. In questo argomento viene illustrata la documentazione di base necessaria per eseguire operazioni di backup e ripristino utilizzando le seguenti versioni di Backup Exec:

- Veritas Backup Exec 2014

- Veritas Backup Exec 15
- Veritas Backup Exec 16
- Veritas Backup Exec 20.x
- Veritas Backup Exec 22.x

La procedura per l'utilizzo di queste versioni di Backup Exec con un gateway di nastri virtuali è la stessa. Vedere il sito Web del supporto Veritas per informazioni dettagliate sull'utilizzo di Backup Exec, incluse informazioni su come creare backup sicuri con Backup Exec, elenchi di compatibilità software e hardware e guide per gli amministratori di Backup Exec.

Per ulteriori informazioni sulle applicazioni di backup supportate, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

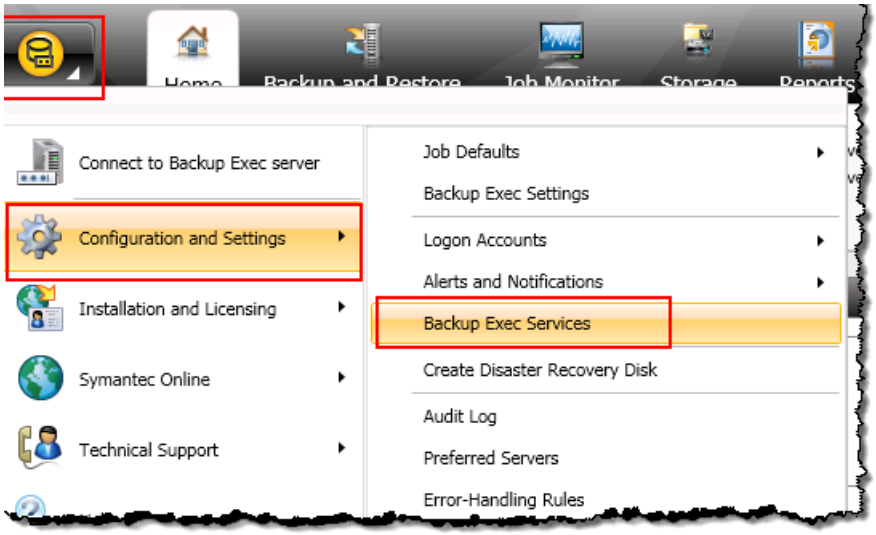
- Configurazione dello storage in Backup Exec
- Importazione di un nastro in Backup Exec
- Scrittura di dati su un nastro in Backup Exec
- Archiviazione di un nastro utilizzando Backup Exec
- Ripristino dei dati da un nastro archiviato in Backup Exec
- Disattivazione di un'unità nastro in Backup Exec

Configurazione dello storage in Backup Exec

Dopo aver connesso i dispositivi della libreria di nastri virtuali al client Windows, puoi configurare lo storage in Backup Exec in modo che riconosca i dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

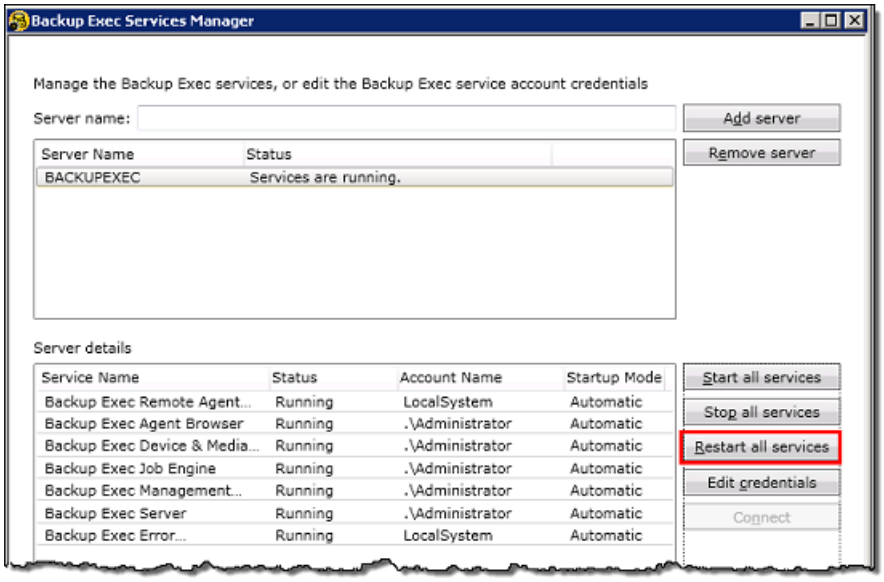
Per configurare lo storage

1. Avviare il software Backup Exec, quindi scegliere l'icona gialla nell'angolo in alto a sinistra nella barra degli strumenti.
2. Scegliere Configuration and Settings (Configurazione e impostazioni), quindi selezionare Backup Exec Services (Servizi di Backup Exec) per aprire Backup Exec Service Manager.



3. Selezionare Restart All Services (Riavvia tutti i servizi). A questo punto, Backup Exec riconosce i dispositivi VTL (ovvero l'unità di sostituzione dei supporti e l'unità nastro). Il processo di riavvio potrebbe richiedere alcuni minuti.

> **Note**
>
> Un gateway di nastri virtuali fornisce 10 unità a nastro. Tuttavia, l'accordo di licenza di Backup Exec potrebbe prevedere per l'applicazione di backup un numero di unità nastro inferiore a 10. In questo caso, è necessario disabilitare le unità nastro nella libreria robotica di Backup Exec in modo da lasciare solo il numero di unità nastro consentito dall'accordo di licenza attivo. Per istruzioni, consulta Disattivazione di un'unità nastro in Backup Exec .



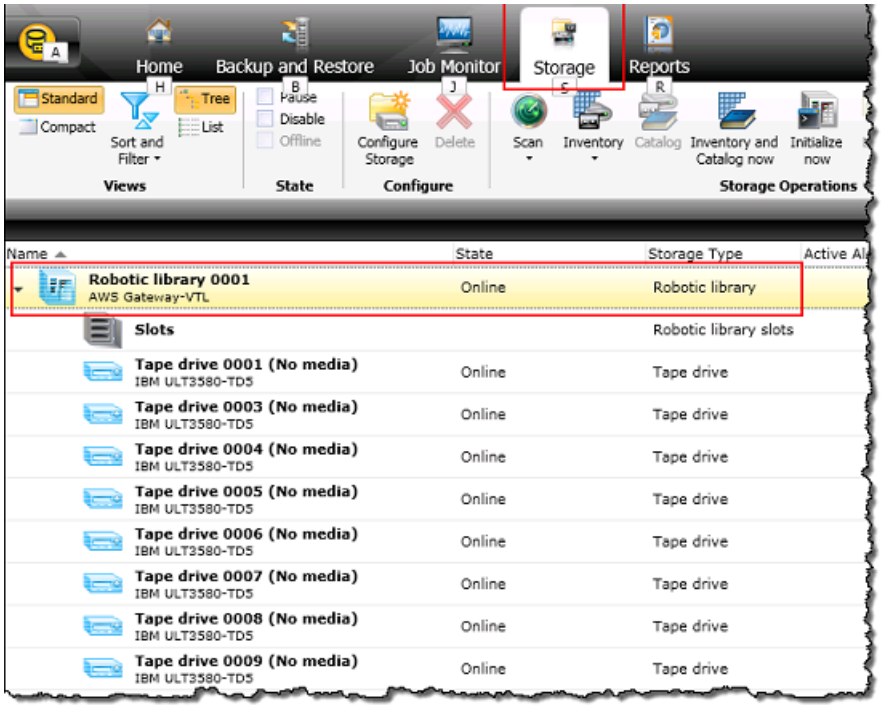
4. Dopo il riavvio, chiudere Backup Exec Service Manager.

Importazione di un nastro in Backup Exec

Ora puoi importare un nastro dal gateway in uno slot.

1. Scegliere la scheda Storage, quindi espandere la struttura ad albero Robotic library (Libreria robotica) per visualizzare i dispositivi VTL.

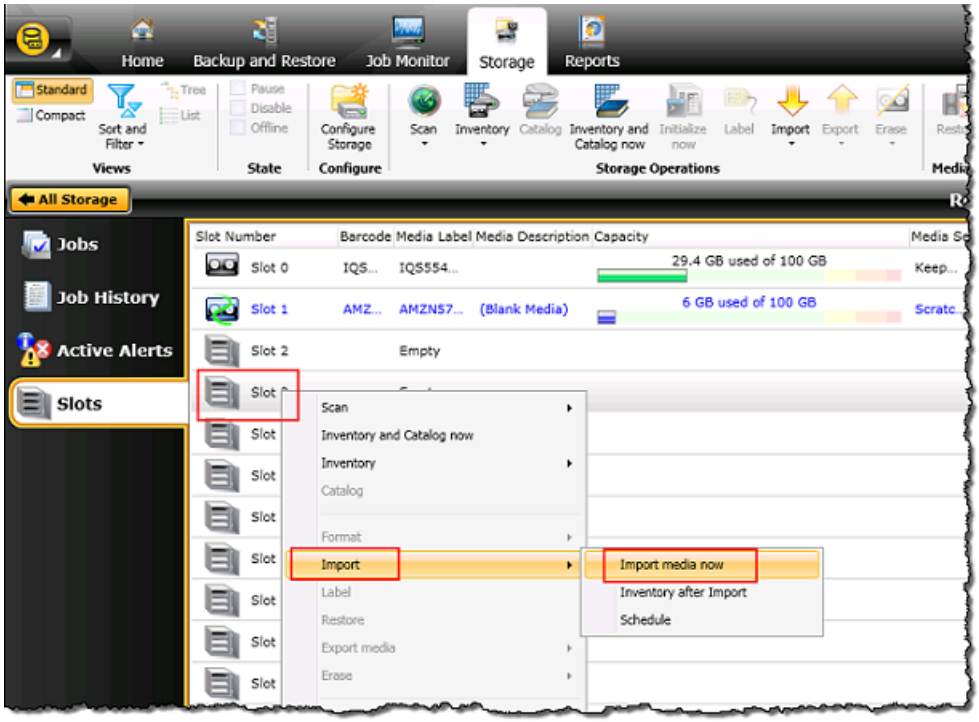
> **Important**
>
> Il software Veritas Backup Exec richiede un tipo di unità di sostituzione dei supporti Gateway di nastri virtuali. Se il tipo di unità di sostituzione dei supporti elencato in Robotic library (Libreria robotica) non è Gateway di nastri virtuali, è necessario modificarlo prima di configurare lo storage nell'applicazione di backup. Per informazioni su come selezionare un tipo di unità di sostituzione dei supporti diverso, consulta Selezione di un'unità di sostituzione dei supporti dopo l'attivazione del gateway.



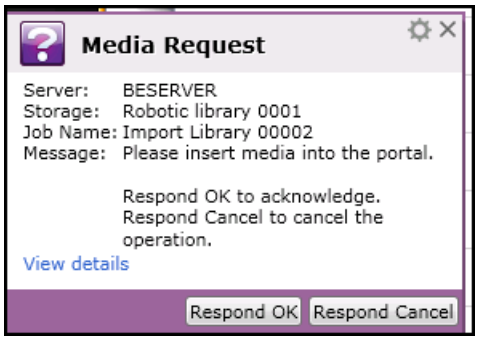
2. Scegliere l'icona Slots (Slot) per visualizzare tutti gli slot.

> **Note**
>
> Quando si importano nastri nella libreria robotica, essi vengono archiviati in slot invece di unità nastro. Pertanto, le unità nastro potrebbero mostrare un messaggio che indica che non è presente alcun supporto nelle unità (No media). Quando si avvia un processo di backup o di ripristino, i nastri vengono spostati nelle unità nastro.
>
> È necessario disporre di nastri disponibili nella libreria di nastri del gateway per importare un nastro in uno slot di storage. Per istruzioni su come creare nastri, consulta Aggiunta di nastri virtuali.

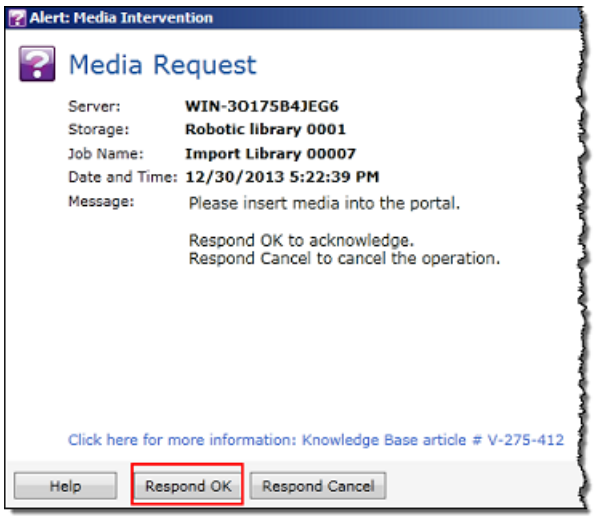
3. Aprire il menu contestuale (clic con il pulsante destro del mouse) di uno slot vuoto, quindi scegliere Import (Importa) e selezionare Import media now (Importa supporti ora). Nel seguente screenshot, lo slot numero 3 è vuoto. È possibile selezionare più di uno slot e importare diversi nastri con un'unica operazione di importazione.



4. Nella finestra Media Request (Richiesta supporti) mostrata, scegliere View details (Visualizza dettagli).



5. Nella finestra Action Alert: Media Intervention (Avviso operazione: intervento supporti), scegliere Respond OK (Rispondi OK) per inserire i supporti nello slot.



Il nastro viene visualizzato nello slot selezionato.

> **Note**
>
> I nastri importati includono nastri vuoti e nastri recuperati dall'archivio nel gateway.

Scrittura di dati su un nastro in Backup Exec

Puoi scrivere i dati su un nastro virtuale del gateway di nastri virtuali utilizzando la stessa procedura e le stesse policy di backup che si applicano ai nastri fisici. Per informazioni dettagliate, consulta la guida amministrativa di Backup Exec nella sezione della documentazione del software Backup Exec.

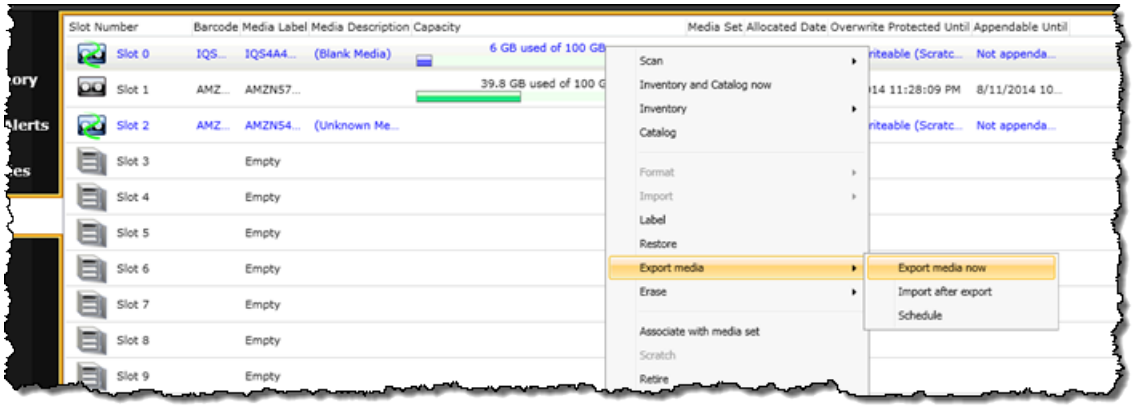
> **Note**
>
> Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Se il processo di backup fallisce, lo stato del nastro in Veritas Backup Exec cambia in Not Appendable. È possibile archiviare il nastro o continuare a leggere i dati da esso. Per completare il processo di backup non riuscito, è necessario inviarlo nuovamente su un nuovo nastro.

Archiviazione di un nastro utilizzando Backup Exec

Quando archivi un nastro, il gateway di nastri virtuali lo sposta dalla libreria di nastri virtuali (VTL) del gateway allo storage offline. Puoi avviare l'archiviazione del nastro esportandolo con il software Backup Exec.

Per archiviare un nastro

1. Scegliere il menu Storage, selezionare Slots (Slot), aprire il menu contestuale (clic con il pulsante destro del mouse) dello slot da cui esportare il nastro, scegliere Export media (Esporta supporti) e selezionare Export media now (Esporta supporti ora). È possibile selezionare più di uno slot e esportare diversi nastri con un'unica operazione di esportazione.



2. Nella finestra popup Media Request (Richiesta supporti), scegliere View details (Visualizza dettagli), quindi selezionare Respond OK (Rispondi OK) nella finestra Alert: Media Intervention (Avviso: intervento supporti).

   Nella console Storage Gateway è possibile verificare lo stato del nastro che si sta archiviando. Il caricamento dei dati in AWS potrebbe richiedere tempo. Durante tale periodo, il nastro esportato viene elencato nella libreria di nastri virtuali del gateway di nastri virtuali con lo stato IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando il caricamento è terminato e inizia il processo di archiviazione, lo stato passa a ARCHIVING (ARCHIVIAZIONE). Quando l'archiviazione dei dati viene completata, il nastro esportato non è più elencato nella VTL ma è archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

3. Scegliere il gateway, quindi selezionare VTL Tape Cartridges (Cartucce nastro VTL) e verificare che il nastro virtuale non sia più elencato nel gateway.

4. Nel riquadro di navigazione della console Storage Gateway, scegliere Tapes (Nastri). Verificare che lo stato del nastro sia ARCHIVED (ARCHIVIATO).

Ripristino dei dati da un nastro archiviato in Backup Exec

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato su un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizzare Backup Exec per ripristinare i dati. Questo processo equivale a quello di ripristino dei dati da nastri fisici. Per le istruzioni, consulta la guida amministrativa di Backup Exec nella sezione della documentazione del software Backup Exec.

Disattivazione di un'unità nastro in Backup Exec

Un gateway di nastri virtuali fornisce 10 unità a nastro, ma potresti decidere di utilizzarne un numero inferiore. In questo caso, puoi disabilitare le unità nastro che non utilizzi.

1. Aprire Backup Exec e scegliere la scheda Storage.
2. Nella struttura ad albero Robotic library (Libreria robotica), aprire il menu contestuale (clic con il pulsante destro del mouse) dell'unità nastro da disabilitare, quindi scegliere Disable (Disabilita).

Fase successiva

Eliminazione delle risorse non necessarie

Test della configurazione utilizzando Veritas NetBackup

È possibile eseguire il backup dei dati su nastri virtuali, archiviare i nastri e gestire i dispositivi VTL (Virtual Tape Library) utilizzando Veritas. NetBackup In questo argomento, è possibile trovare la documentazione di base su come configurare l' NetBackup applicazione per un Tape Gateway ed eseguire un'operazione di backup e ripristino. A tale scopo, è possibile utilizzare le seguenti versioni di NetBackup:

- Veritas 7.x NetBackup
- Veritas 8.x NetBackup

La procedura per l'utilizzo di queste versioni di Backup Exec con un gateway di nastri virtuali è simile. Per informazioni dettagliate sull'utilizzo NetBackup, consulta Veritas Services and Operations Readiness Tools (SORT) sul sito Web di Veritas. Per informazioni sull'assistenza di Veritas sulla

compatibilità hardware, consulta l'elenco di compatibilità hardware NetBackup 7.0 - 7.6.x, l'elenco di compatibilità hardware NetBackup 8.0 - 8.1.x o NetBackup l'elencodi compatibilità hardware 8.2 - 8.x.x sul sito Web di Veritas.

Per ulteriori informazioni sulle applicazioni di backup compatibili, consulta Applicazioni di backup di terze parti supportate per un gateway di nastri virtuali.

Argomenti

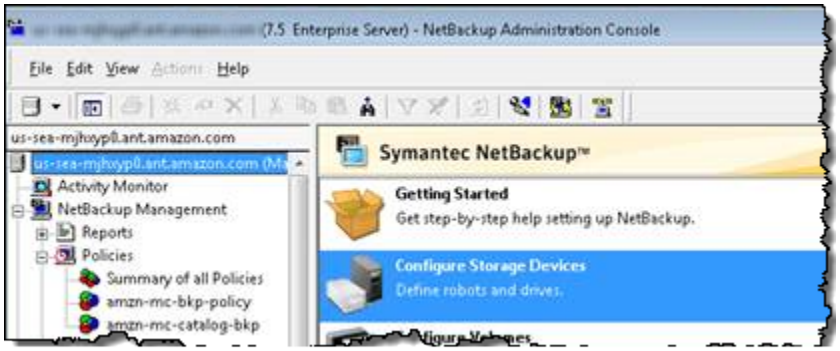
- Configurazione dei dispositivi di storage NetBackup
- Backup dei dati su nastro
- Archiviazione del nastro
- Ripristino dei dati dal nastro

Configurazione dei dispositivi di storage NetBackup

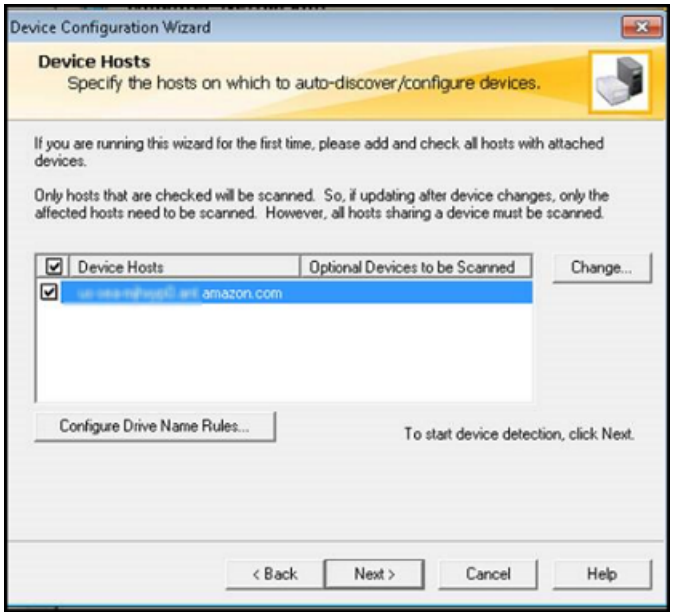
Dopo aver collegato i dispositivi VTL (Virtual Tape Library) al client Windows, configuri NetBackup lo storage Veritas per riconoscere i tuoi dispositivi. Per ulteriori informazioni su come connettere i dispositivi VTL al client Windows, consulta Connessione dei dispositivi VTL.

NetBackup Per configurare l'utilizzo dei dispositivi di archiviazione sul Tape Gateway

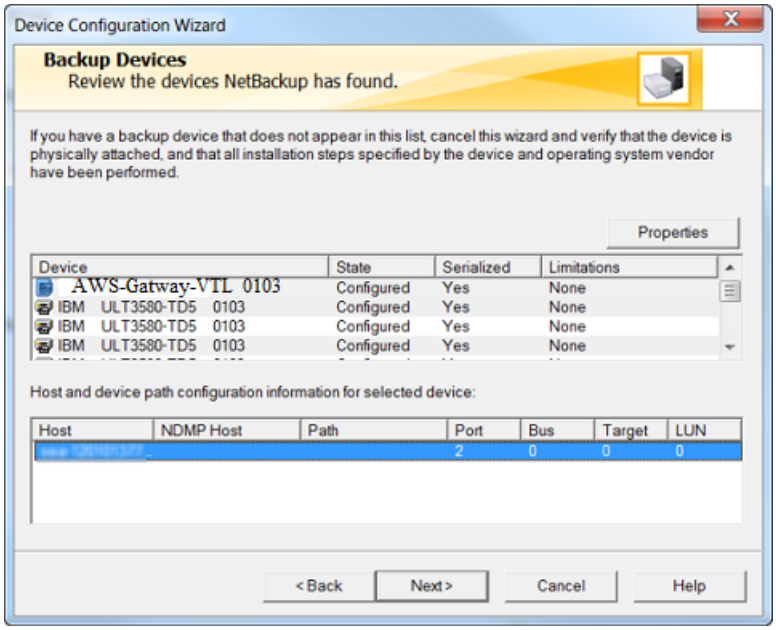
1. Apri la console di NetBackup amministrazione ed eseguila come amministratore.



2. Scegliere Configure Storage Devices (Configura dispositivi di storage) per aprire la procedura guidata di configurazione dei dispositivi.
3. Seleziona Avanti. L' NetBackup applicazione rileva il computer come host del dispositivo.
4. Nella colonna Device Hosts (Host dispositivi) selezionare il computer e quindi scegliere Next (Avanti). L' NetBackup applicazione esegue la scansione del computer alla ricerca di dispositivi e rileva tutti i dispositivi.



5. Nella pagina Scanning Hosts (Scansione host) scegliere Next (Avanti) e quindi Next (Avanti). L' NetBackup applicazione trova tutte le 10 unità nastro e il caricatore di supporti sul computer.

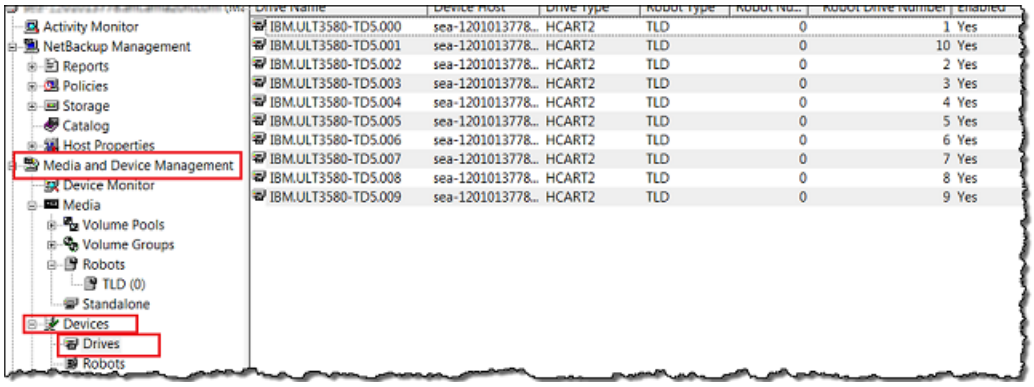


6. Nella finestra Backup Devices (Dispositivi di backup) scegliere Next (Avanti).
7. Nella finestra Drag and Drop Configuration (Configurazione trascinamento della selezione) verificare che sia selezionata l'unità di sostituzione dei supporti e quindi scegliere Next (Avanti).
8. Nella finestra di dialogo visualizzata scegliere Yes (Sì) per salvare la configurazione nel computer. L' NetBackup applicazione aggiorna la configurazione del dispositivo.

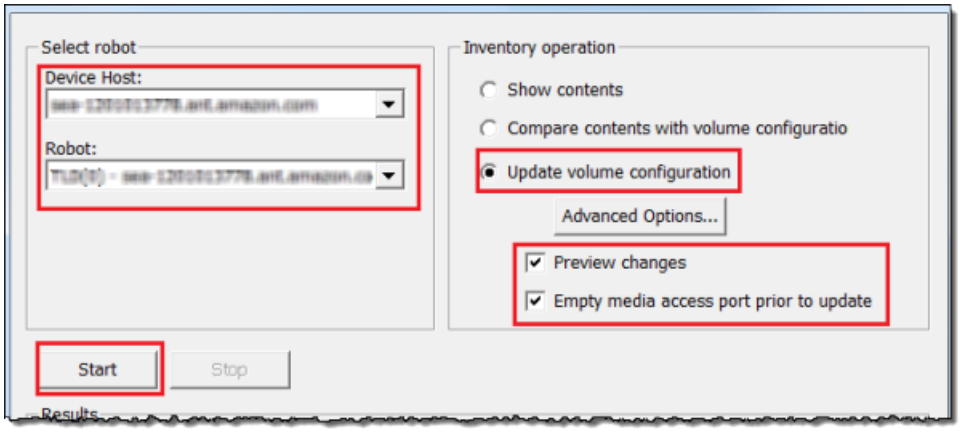
9. Una volta completato l'aggiornamento, scegliete Avanti per rendere i dispositivi disponibili all' NetBackup applicazione.
10. Nella finestra Finished! (Completato), scegliere Finish (Fine).

Per verificare i dispositivi nell' NetBackup applicazione

1. In NetBackup Administration Console, espandi il nodo Gestione di supporti e dispositivi, quindi espandi il nodo Dispositivi. Scegliere Drives (Unità) per visualizzare tutte le unità nastro.

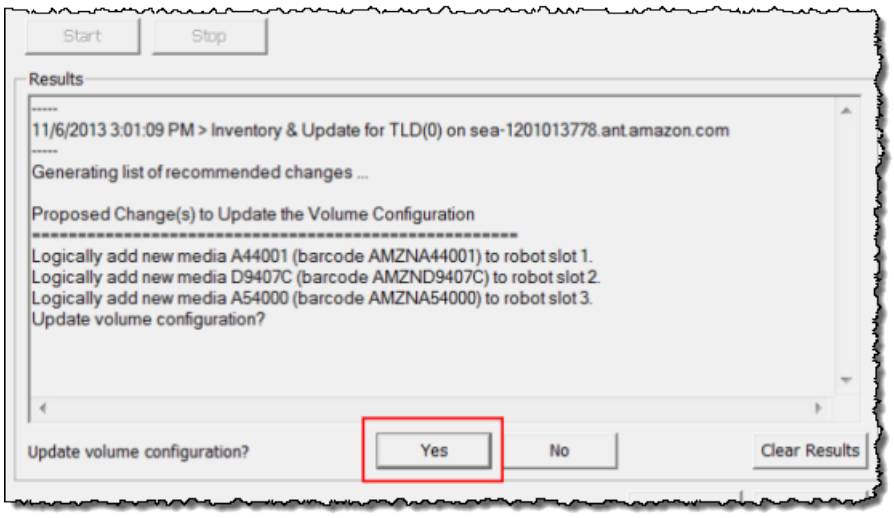


2. Nel nodo Devices (Dispositivi) scegliere Robots (Robot) per visualizzare tutte le unità di sostituzione dei supporti. Nell' NetBackup applicazione, il medium changer è chiamato robot.
3. Nel riquadro All Robots (Tutti i robot) aprire il menu contestuale (clic con il pulsante destro del mouse) per TLD(0) (ovvero il robot in uso) e quindi scegliere Inventory Robot (Robot inventario).
4. Nella finestra Robot Inventory (Inventario robot) verificare che l'host sia selezionato nell'elenco Device-Host (Host dispositivi) nella categoria Select robot (Seleziona robot).
5. Verificare che il robot sia selezionato nell'elenco Robot.
6. Nella finestra Robot Inventory (Inventario robot) selezionare Update volume configuration (Aggiorna configurazione volume), selezionare Preview changes (Anteprima modifiche), selezionare Empty media access port prior to update (Libera porta di accesso supporti prima dell'aggiornamento) e quindi scegliere Start (Avvia).

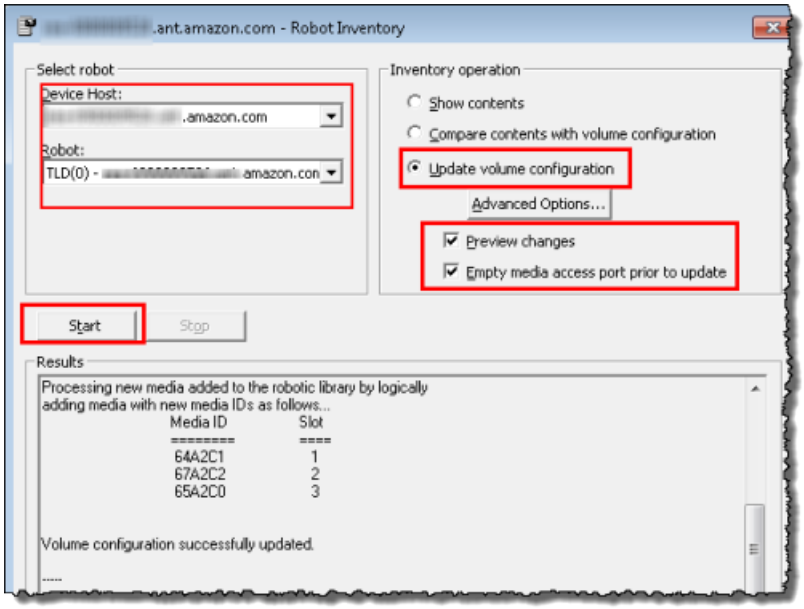


Il processo esegue quindi l'inventario del caricatore di supporti e dei nastri virtuali nel database NetBackup Enterprise Media Management (EMM). NetBackup archivia le informazioni multimediali, la configurazione del dispositivo e lo stato del nastro nell'EMM.

7. Nella finestra Robot Inventory (Inventario robot) scegliere Yes (Sì) una volta completato l'inventario. Scegliendo Yes (Sì) la configurazione viene aggiornata e i nastri virtuali trovati negli slot di importazione/esportazione vengono spostati nella libreria di nastri virtuali.

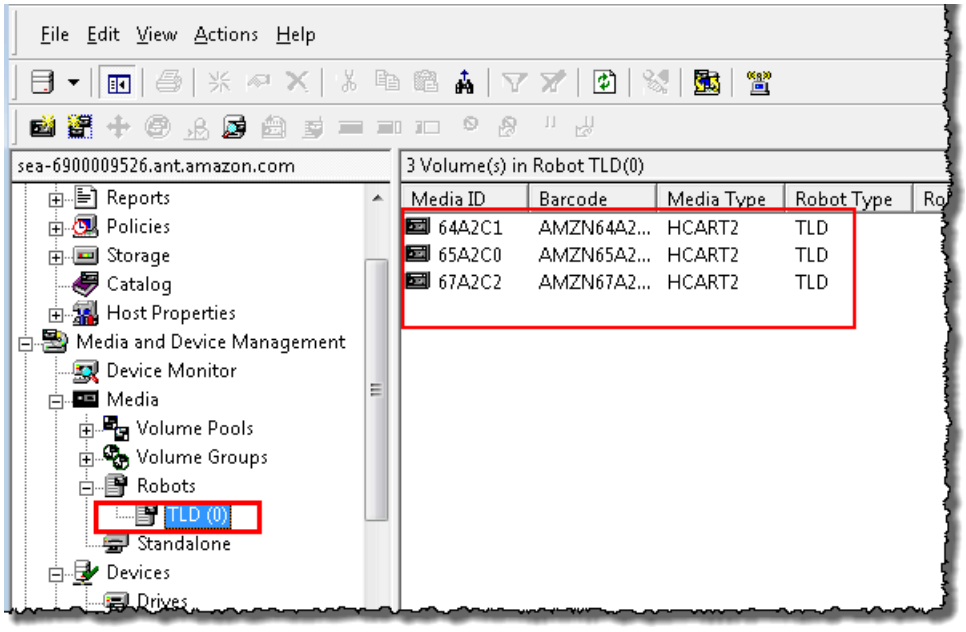


Lo screenshot seguente mostra ad esempio tre nastri virtuali trovati negli slot di importazione/esportazione.



8. Chiudere la finestra Robot Inventory (Inventario robot).
9. Nel nodo Media (Supporti) espandere il nodo Robots (Robot) e scegliere TLD(0) per visualizzare tutti i nastri virtuali disponibili per il robot (unità di sostituzione dei supporti).

> **Note**
>
> Se in precedenza avete collegato altri dispositivi all' NetBackupapplicazione, potreste avere più robot. Assicurarsi di selezionare il robot appropriato.



Dopo aver connesso i dispositivi e averli resi disponibili per l'applicazione di backup, è possibile testare il gateway. Per testare il gateway, è necessario eseguire il backup dei dati sui nastri virtuali creati e archiviare i nastri.

Backup dei dati su nastro

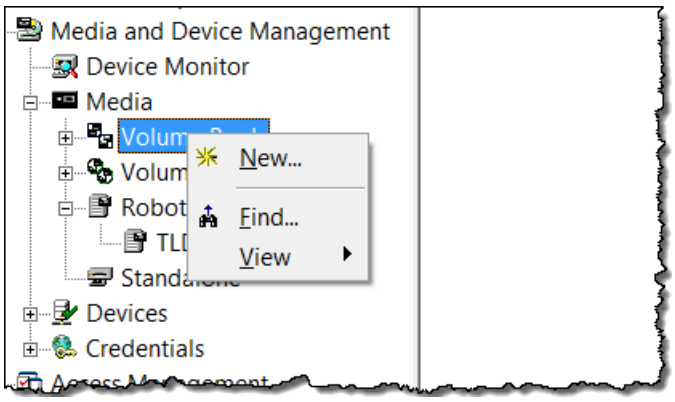
Per testare la configurazione del gateway di nastri virtuali, devi eseguire il backup dei dati sui nastri virtuali.

> **Note**
>
> - Per questo esercizio sulle nozioni di base, esegui il backup solo di una piccola quantità di dati, perché per la memorizzazione, l'archiviazione e il recupero dei dati vengono addebitati costi. Per informazioni dettagliate sui prezzi, consulta Pricing (Prezzi) sulla pagina dello Storage Gateway.
> - Se il gateway di nastri virtuali si riavvia per qualsiasi motivo durante un processo di backup in corso, il processo di backup potrebbe fallire. Il processo di backup sospeso riprenderà automaticamente al termine del riavvio del gateway.

Per creare un pool di volumi

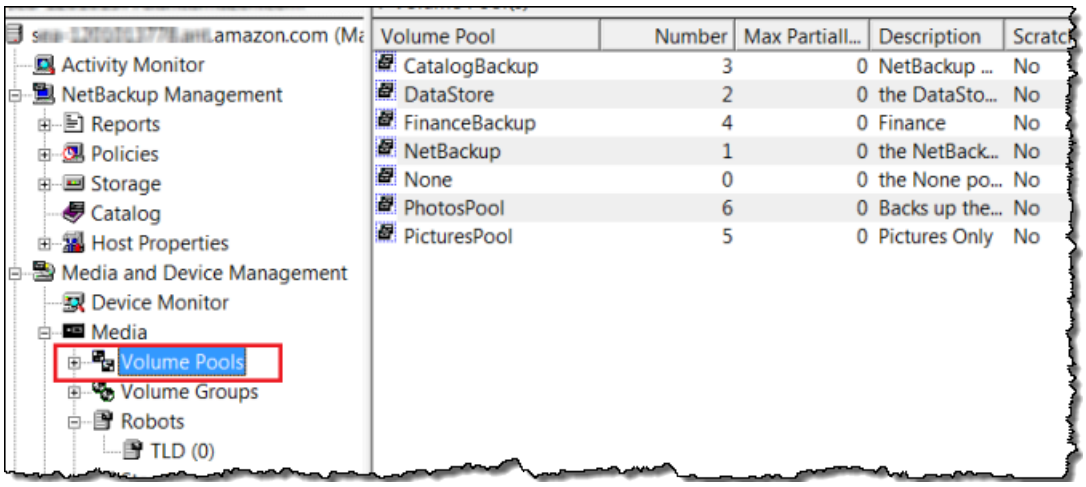
Un pool di volumi è una raccolta di nastri virtuali da usare per un backup.

1. Avvia la console di NetBackup amministrazione.
2. Espandere il nodo Media (Supporti), aprire il menu contestuale (clic con il pulsante destro del mouse) per Volume Pool (Pool di volumi) e quindi scegliere New (Nuovo). Verrà visualizzata la finestra di dialogo New Volume Pool (Nuovo pool di volumi).



3. Per Name (Nome) digitare un nome per il pool di volumi.
4. Per Description (Descrizione) digitare una descrizione per il pool di volumi e quindi scegliere OK. Il pool di volumi appena creato verrà aggiunto all'elenco di pool di volumi.

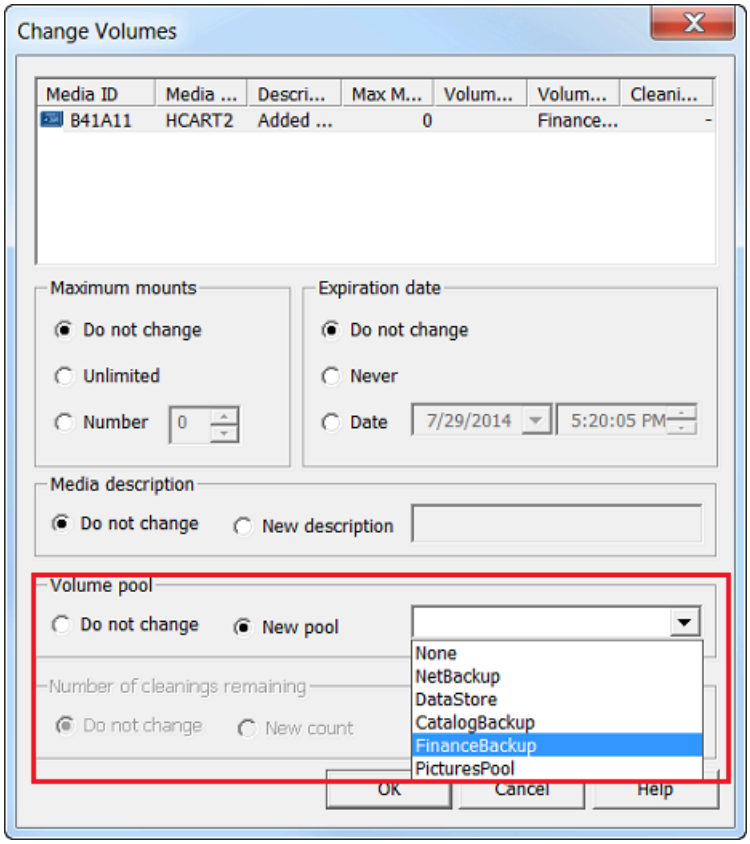
   Lo screenshot seguente mostra un elenco di pool di volumi.



Per aggiungere nastri virtuali a un pool di volumi

1. Espandere il nodo Robots (Robot) e selezionare il robot TLD(0) per visualizzare i nastri virtuali riconosciuti dal robot.

   Se in precedenza è già stato connesso un robot, il robot del gateway di nastri virtuali potrebbe avere un nome diverso.
2. Nell'elenco di nastri virtuali aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro che si desidera aggiungere al pool di volumi e scegliere Change (Modifica) per aprire la finestra di dialogo Change Volumes (Modifica volumi). Lo screenshot seguente mostra la finestra di dialogo Change Volumes (Modifica volumi).



3. Per Volume Pool (Pool di volumi), scegliere New pool (Nuovo pool).
4. Per New pool (Nuovo pool), selezionare il pool appena creato e quindi scegliere OK.

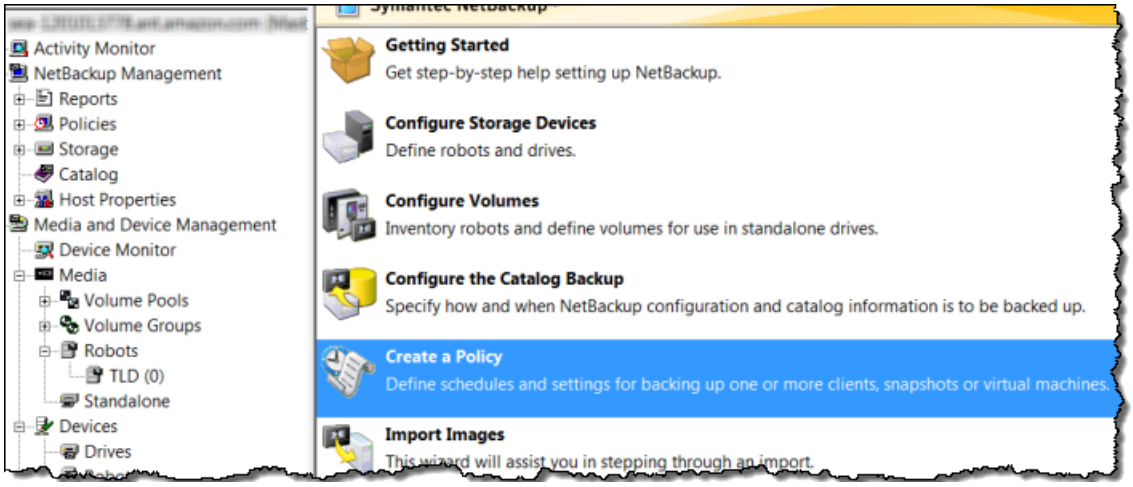
   È possibile verificare che il pool di volumi contenga il nastro virtuale appena aggiunto espandendo il nodo Media (Supporti) e scegliendo il pool di volumi.

Per creare una policy di backup

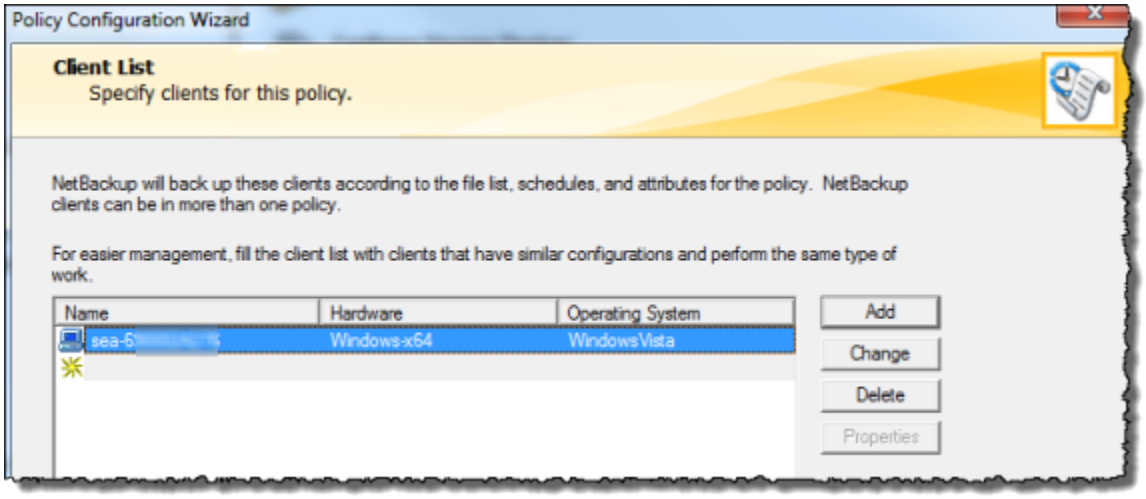
La policy di backup specifica i dati di cui eseguire il backup, quando eseguire il backup e il pool di volumi da usare.

1. Scegli il tuo Master Server per tornare alla NetBackup console Veritas.

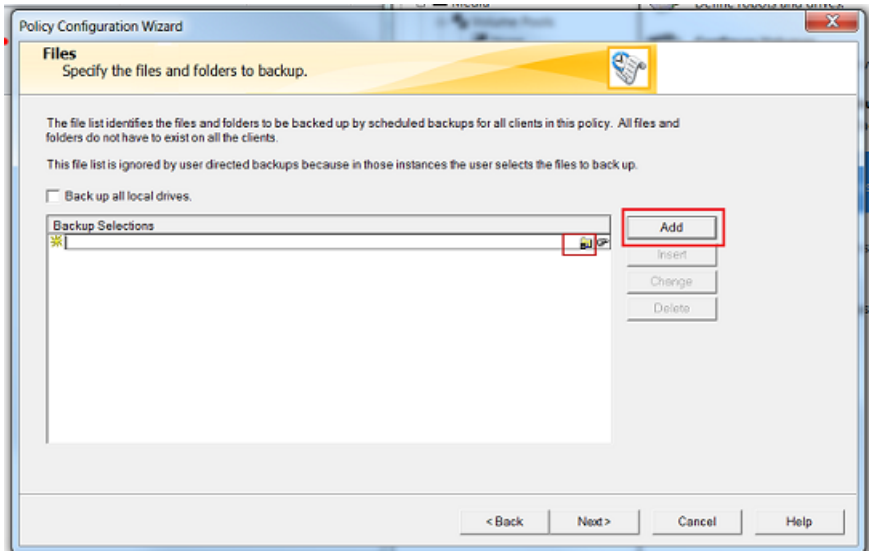
   La schermata seguente mostra la NetBackup console con l'opzione Create a Policy selezionata.



2. Scegliere Create a Policy (Crea una policy) per aprire la finestra Policy Configuration Wizard (Procedura guidata di configurazione policy).
3. Selezionare File systems, databases, applications (File system, database, applicazioni) e scegliere Next (Avanti).
4. Per Policy Name (Nome policy) digitare un nome per la policy e verificare che sia selezionata l'opzione MS-Windows nell'elenco Select the policy type (Seleziona tipo di policy), quindi scegliere Next (Avanti).
5. Nella finestra Client List (Elenco client) scegliere Add (Aggiungi), digitare il nome host del computer nella colonna Name (Nome) e quindi scegliere Next (Avanti). Questa fase permette di applicare la policy che si sta definendo a `localhost` (computer client).



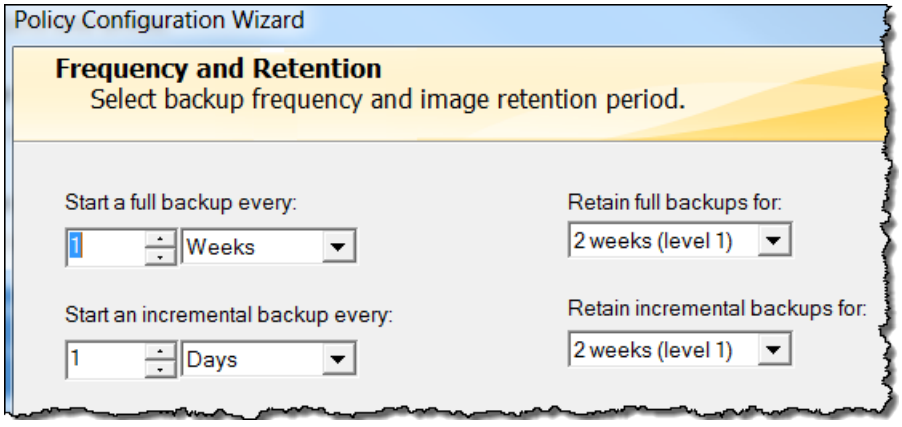
6. Nella finestra Files (File) scegliere Add (Aggiungi) e quindi scegliere l'icona della cartella.



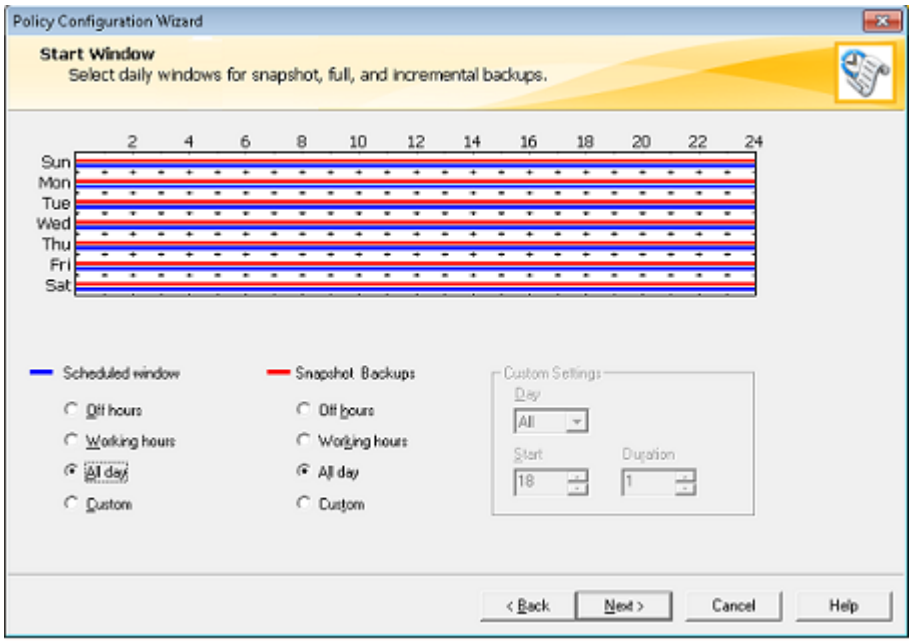
7. Nella finestra Browse (Sfoglia) passare alla cartella o ai file di cui si desidera eseguire il backup, scegliere OK e quindi scegliere Next (Avanti).
8. Nella finestra Backup Types (Tipi di backup) accettare le impostazioni predefinite e quindi scegliere Next (Avanti).

> **Note**
>
> Se si desidera avviare personalmente il backup, selezionare User Backup (Backup utente).

9. Nella finestra Frequency and Retention (Frequenza e conservazione) selezionare la policy relativa a frequenza e conservazione da applicare al backup. Per questo esercizio, è possibile accettare tutte le impostazioni predefinite e scegliere Next (Avanti).



10. Nella finestra Start (Avvia) selezionare Off hours (Ore non di picco) e quindi scegliere Next (Avanti). Questa selezione specifica che il backup della cartella deve venire eseguito solo durante le ore non di picco.

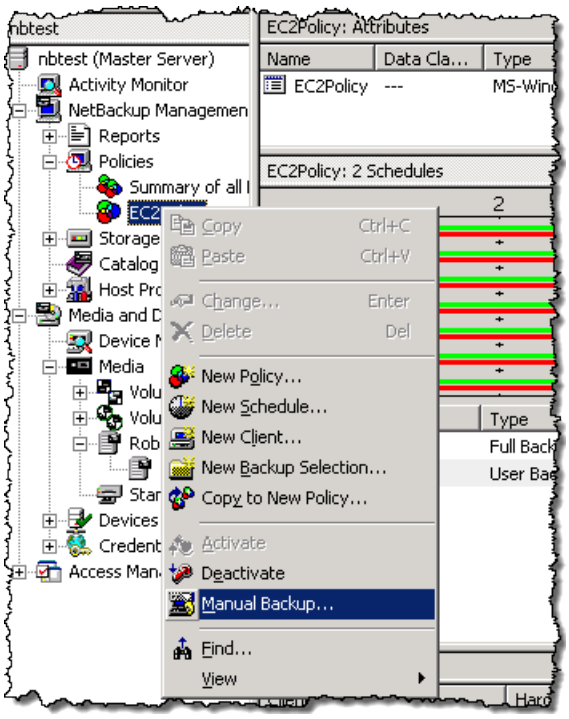


11. Nella procedura guidata Policy Configuration (Configurazione policy) scegliere Finish (Fine).

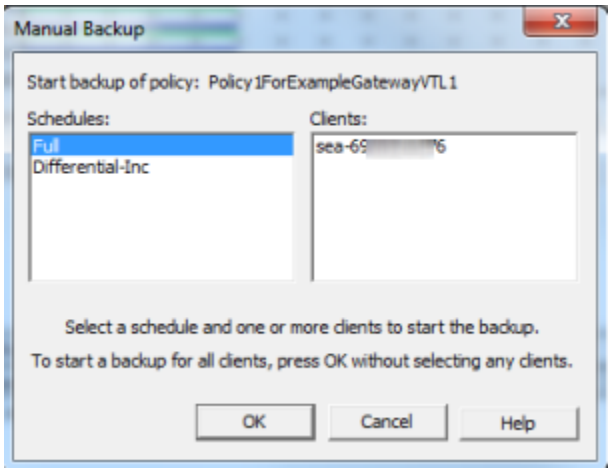
La policy esegue i backup in base alla pianificazione. È anche possibile eseguire un backup manuale in qualsiasi momento, come illustrato nella fase successiva.

Per eseguire un backup manuale

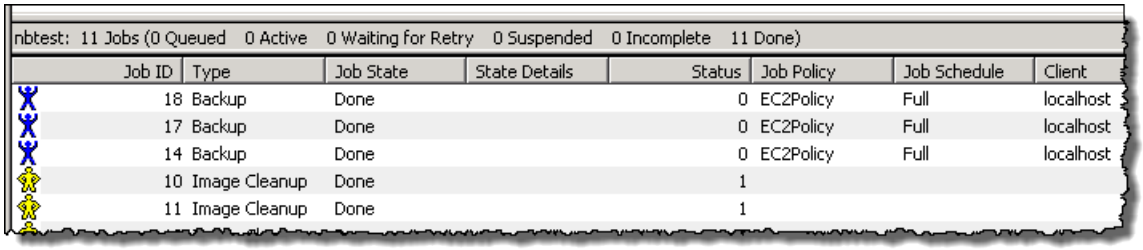
1. Nel riquadro di navigazione della NetBackup console, espandere il NetBackup nodo Gestione.
2. Espandere il nodo Policies (Policy).
3. Aprire il menu contestuale (clic con il pulsante destro del mouse) per la policy e scegliere Manual Backup (Backup manuale).



4. Nella finestra Manual Backup (Backup manuale) selezionare una pianificazione, selezionare un client e quindi scegliere OK.



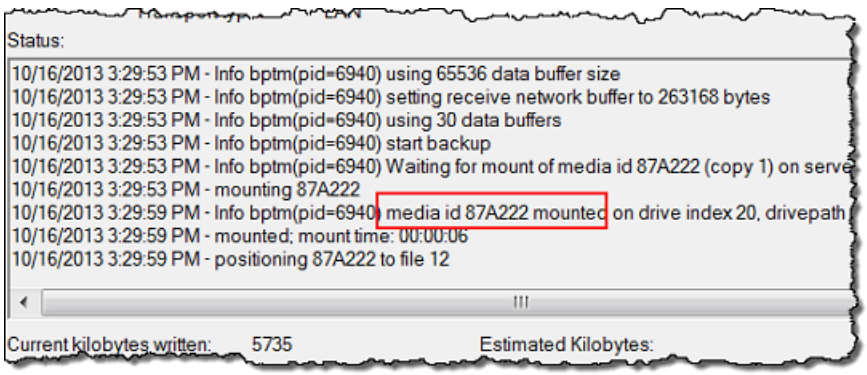
5. Nella finestra di dialogo Manual Backup Started (Backup manuale avviato) visualizzata scegliere OK.
6. Nel riquadro di navigazione scegliere Activity Monitor (Monitoraggio attività) per visualizzare lo stato del backup nella colonna Job ID (ID processo).



Per trovare il codice a barre del nastro virtuale su cui sono NetBackup stati scritti i dati del file durante il backup, guarda nella finestra Job Details come descritto nella procedura seguente. Questo codice a barre è necessario per la procedura nella sezione successiva, quando si archivia il nastro.

Per trovare il codice a barre di un nastro

1. In Activity Monitor (Monitoraggio attività) aprire il menu contestuale (clic con il pulsante destro del mouse) per l'identificatore del processo di backup nella colonna Job ID (ID processo) e quindi scegliere Details (Dettagli).
2. Nella finestra Job Details (Dettagli processo) scegliere la scheda Detailed Status (Stato dettagliato).
3. Nella casella Status (Stato) individuare l'ID del supporto. Nello screenshot seguente, ad esempio, l'ID del supporto è 87A222. Questo ID permette di determinare il nastro su cui sono stati scritti i dati.



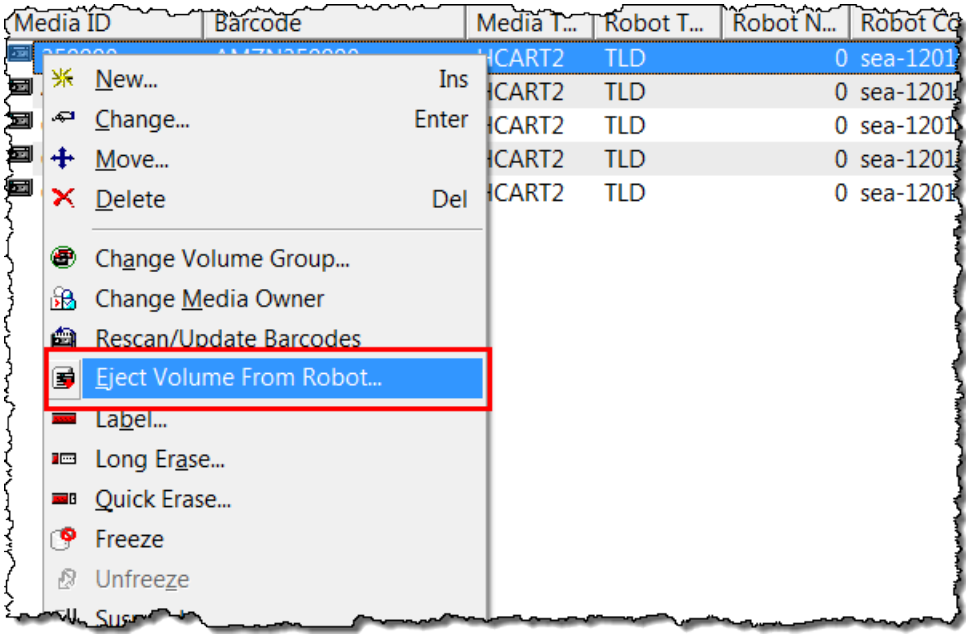
A questo punto, è stato distribuito un gateway di nastri virtuali, sono stati creati i nastri virtuali ed è stato eseguito il backup dei dati. È quindi possibile archiviare i nastri virtuali e recuperarli dall'archivio.

Archiviazione del nastro

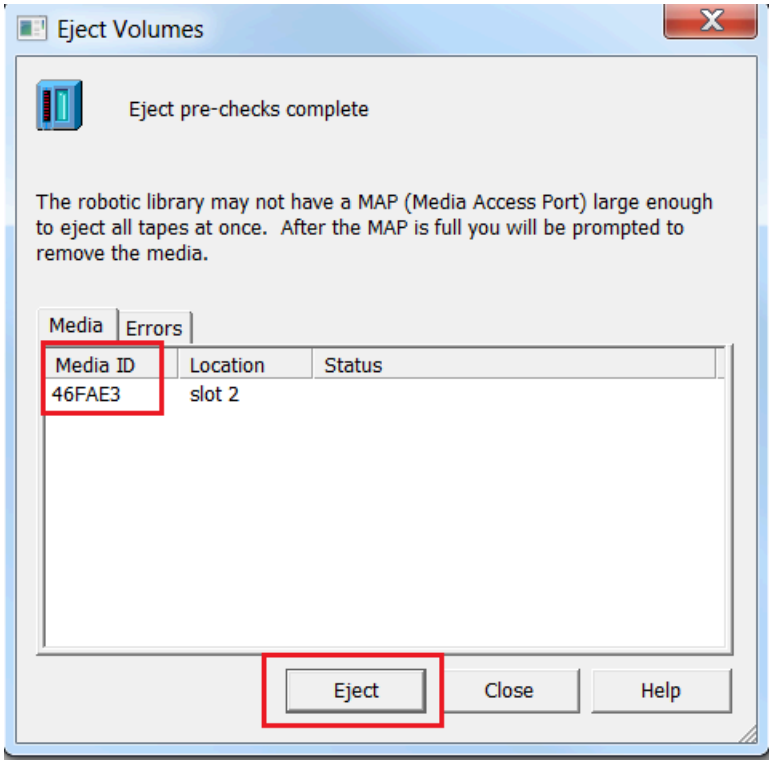
Quando archivi un nastro, il gateway di nastri virtuali sposta il nastro dalla libreria di nastri virtuali (VTL) del gateway all'archivio, che offre storage offline. Puoi avviare l'archiviazione del nastro espellendo il nastro tramite l'applicazione di backup.

Per archiviare un nastro virtuale

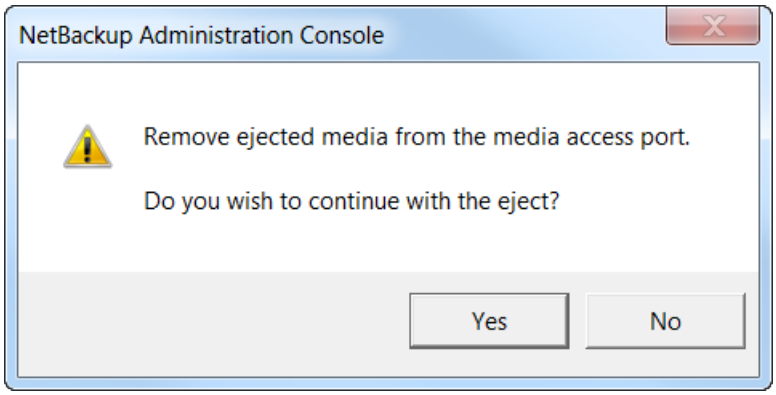
1. Nella console di NetBackup amministrazione, espandi il nodo Gestione dei contenuti multimediali e dei dispositivi ed espandi il nodo Media.
2. Espandere Robots (Robot) e scegliere TLD(0).
3. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il nastro virtuale da archiviare e scegliere Eject Volume From Robot (Espelli volume da robot).



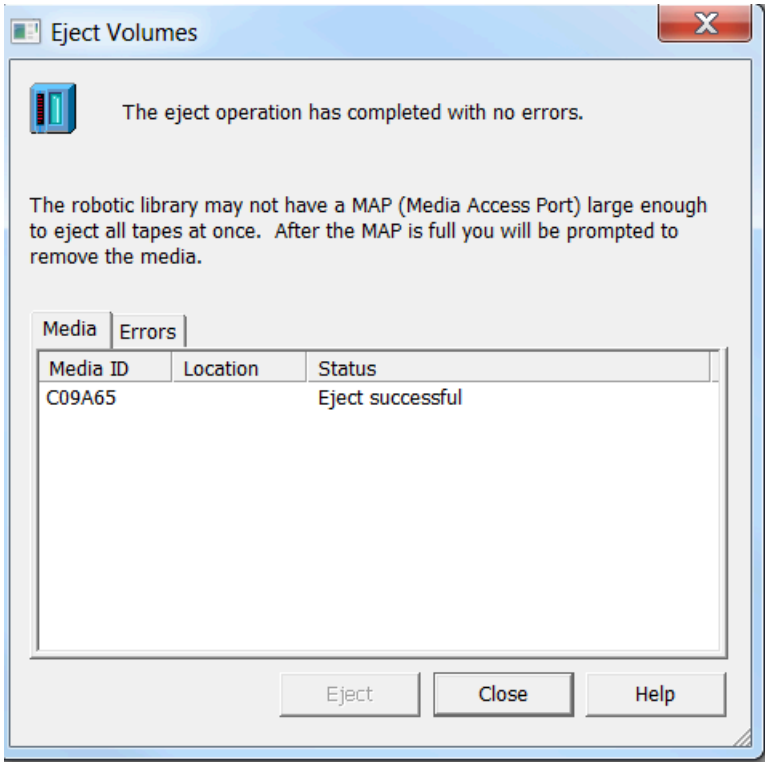
4. Nella finestra Eject Volumes (Espelli volumi) verificare che Media ID (ID supporto) corrisponda al nastro virtuale da espellere e quindi scegliere Eject (Espelli).



5. Nella finestra di dialogo scegliere Yes (Sì). La finestra di dialogo è visualizzata di seguito.



Quando il processo di espulsione viene completato, lo stato del nastro nella finestra di dialogo Eject Volumes (Espelli volumi) indica che l'operazione è stata completata.



6. Scegliere Close (Chiudi) per chiudere la finestra Eject Volumes (Espelli volumi).
7. Nella console Storage Gateway verificare lo stato del nastro che si sta archiviando nella libreria di nastri virtuali del gateway. Il caricamento dei dati in AWS potrebbe richiedere tempo. Durante tale periodo, il nastro espulso viene elencato nella libreria di nastri virtuali del gateway con lo stato IN TRANSIT TO VTS (IN TRANSITO VERSO VTS). Quando l'archiviazione viene avviata, lo stato è ARCHIVING (ARCHIVIAZIONE). Quando il caricamento dei dati viene completato, il nastro espulso non è più elencato nella VTL ma è archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
8. Per verificare che il nastro virtuale non sia più elencato nel gateway, scegliere il gateway e quindi scegliere VTL Tape Cartridges (Cartucce nastro VTL).
9. Nel riquadro di navigazione della console Storage Gateway selezionare Tapes (Nastri). Verificare che lo stato del nastro archiviato sia ARCHIVED (ARCHIVIATO).

Ripristino dei dati dal nastro

Il ripristino dei dati archiviati è un processo in due fasi.

Per ripristinare i dati da un nastro archiviato

1. Recuperare il nastro archiviato su un gateway di nastri virtuali. Per istruzioni, consulta Recupero di nastri archiviati.
2. Utilizza il software di Backup, Archiviazione e Ripristino installato con l' NetBackup applicazione Veritas. Questo processo equivale a quello di ripristino dei dati da nastri fisici. Per istruzioni, consulta la pagina relativa a Veritas Services e Operations Readiness Tools (SORT) nel sito web di Veritas.

Fase successiva

Eliminazione delle risorse non necessarie

Cosa fare in seguito?

Dopo aver messo in produzione il gateway di nastri virtuali, puoi eseguire diverse attività di manutenzione, ad esempio aggiungere e rimuovere nastri, monitorare e ottimizzare le prestazioni del gateway e risolvere i problemi. Per informazioni generali su queste attività di gestione, consulta Gestione del gateway.

È possibile eseguire alcune attività di manutenzione del Tape Gateway su AWS Management Console, come la configurazione dei limiti di velocità della larghezza di banda del gateway e la gestione degli aggiornamenti software del gateway. Se il gateway di nastri virtuali viene distribuito on-premise, puoi eseguire alcune operazioni di manutenzione sulla console locale del gateway. Queste includono il routing del gateway di nastri virtuali tramite un proxy e la configurazione del gateway per l'utilizzo di un indirizzo IP statico. Se il gateway è in esecuzione come istanza Amazon EC2, è possibile eseguire attività di manutenzione specifiche sulla console Amazon EC2, ad esempio aggiungere o rimuovere volumi Amazon EBS. Per ulteriori informazioni sulla gestione del gateway di nastri virtuali, consulta Gestione del gateway di nastri virtuali.

Se prevedi di distribuire il gateway in produzione, devi prendere in considerazione il carico di lavoro reale per determinare le dimensioni del disco. Per informazioni su come determinare le dimensioni reali del disco, consulta Gestione dei dischi locali per Storage Gateway. Inoltre, considera di pulire il disco se non prevedi di continuare a utilizzare il gateway di nastri virtuali. Il processo di pulizia consente di evitare costi aggiuntivi. Per informazioni sulla pulizia, consulta Eliminazione delle risorse non necessarie.

Eliminazione delle risorse non necessarie

Se hai creato il gateway per esercitarti o per prova, considera di eliminarlo per evitare di incorrere in spese superflue o impreviste.

Se prevedi di continuare a utilizzare il gateway di nastri virtuali, consulta ulteriori informazioni in Cosa fare in seguito?

Per eliminare risorse non necessarie

1. Eliminare i nastri dall'archivio e dalla libreria di nastri virtuali del gateway. Per ulteriori informazioni, consulta Eliminazione del gateway tramite la console AWS Storage Gateway e rimozione delle risorse associate.
    a. Archiviare qualsiasi nastro che abbia lo stato RETRIEVED (RICHIAMATO) nella libreria di nastri virtuali (VTL) del gateway. Per istruzioni, consulta Archiviazione di nastri.
    b. Eliminare ogni nastro rimanente dalla libreria di nastri virtuali del gateway. Per istruzioni, consulta Eliminazione di nastri.
    c. Eliminare ogni nastro dall'archivio. Per istruzioni, consulta Eliminazione di nastri.
2. A meno che non si preveda di continuare a utilizzare il gateway di nastri virtuali, eliminarlo. Per istruzioni, consulta Eliminazione del gateway tramite la console AWS Storage Gateway e rimozione delle risorse associate.
3. Eliminare la macchina virtuale Storage Gateway dall'host on-premise. Se è stato creato un proprio gateway su un'istanza Amazon EC2, terminare l'istanza.

Attivazione di un gateway in un cloud privato virtuale

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

Per attivare il gateway in un VPC, usa la console Amazon VPC per creare un endpoint VPC per Storage Gateway e ottieni l'ID dell'endpoint VPC, quindi specifica questo ID endpoint VPC quando crei e attivi il gateway. Per ulteriori informazioni, consulta Connect your Tape Gateway to AWS .

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

Argomenti

Creazione di un endpoint VPC per Storage Gateway

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

Per creare un endpoint VPC per Storage Gateway

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Endpoint e scegliere Create Endpoint (Crea endpoint).
3. Nella pagina Crea endpoint, scegliere Servizi AWS per Categoria del servizio.
4. Per Service Name (Nome del servizio), selezionare `com.amazonaws.region.storagegateway`. Ad esempio `com.amazonaws.us-east-2.storagegateway`.
5. Per VPC, scegliere il VPC e annotare le zone di disponibilità e le sottoreti.
6. 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. Seleziona Crea endpoint. Lo stato iniziale dell'endpoint è pending (in sospeso). Quando l'endpoint viene creato, prendere nota dell'ID dell'endpoint VPC appena creato.
9. Quando l'endpoint viene creato, scegliere Endpoint quindi il nuovo endpoint VPC.
10. Nella scheda Dettagli dell'endpoint del gateway di archiviazione selezionato, in Nomi DNS, utilizza il primo nome DNS che non specifica una zona di disponibilità. Il 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. Per ulteriori informazioni, consulta Creazione di un gateway.

Gestione del gateway

La gestione del gateway include attività come la configurazione dello storage della cache e dello spazio del buffer di caricamento, l'uso di volumi o nastri virtuali e l'esecuzione di attività di manutenzione generale. Se non è stato creato un gateway, consulta Nozioni di base.

Le versioni del software del gateway includeranno periodicamente aggiornamenti del sistema operativo e patch di sicurezza che sono state convalidate. Questi aggiornamenti vengono applicati come parte del normale processo di aggiornamento del gateway durante una finestra di manutenzione pianificata e in genere vengono rilasciati ogni sei mesi. Nota: gli utenti devono trattare l'appliance Storage Gateway come una macchina virtuale gestita e non devono tentare di accedere o modificare l'istanza dell'appliance Storage Gateway. Il tentativo di installare o aggiornare qualsiasi pacchetto software utilizzando metodi diversi (ad esempio: strumenti SSM o Hypervisor) rispetto al normale meccanismo di aggiornamento del gateway può compromettere il corretto funzionamento del gateway.

Argomenti

Gestione del gateway di nastri virtuali

Di seguito sono disponibili informazioni su come gestire le risorse del gateway di nastri virtuali in AWS Storage Gateway.

Argomenti

- Eliminazione di nastri
- Eliminazione di pool di nastri personalizzati
- Disattivazione del gateway di nastri virtuali
- Comprendere lo stato del nastro

Modifica delle informazioni di base sul gateway

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

Per modificare le informazioni di base per un gateway esistente

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le informazioni di base.
3. Dal menu a discesa Operazioni, scegli Modifica le informazioni sul gateway.
4. Modificare l'impostazione desiderata, quindi selezionare Salva.

> **Note**
>
> La modifica del nome di un gateway disconnetterà tutti gli CloudWatch allarmi configurati per monitorare il gateway. Per ricollegare gli allarmi, aggiorna il file GatewayNameper ogni allarme nella console. CloudWatch

Aggiunta di nastri virtuali

È possibile aggiungere nastri al gateway di nastri virtuali quando è necessario. Per informazioni su come creare i nastri virtuali, consulta Creazione di nastri virtuali.

Dopo aver creato il nastro, puoi trovare informazioni al riguardo nella pagina Panoramica del nastro. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà. Per informazioni sulle quote del gateway di nastri virtuali, consulta AWS Storage Gateway quote.

Gestione della creazione automatica di nastri

Il gateway di nastri virtuali crea automaticamente nuovi nastri virtuali per mantenere il numero minimo di nastri disponibili configurati. Quindi rende questi nuovi nastri disponibili per l'importazione dall'applicazione di backup in modo che i processi di backup possano essere eseguiti senza interruzioni. La creazione automatica di nastri elimina la necessità di script personalizzati oltre al processo manuale per la creazione di nuovi nastri virtuali.

Per eliminare una policy di creazione automatica del nastro

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere la scheda Gateways (Gateway).
3. Scegliere il gateway per il quale è necessario gestire la creazione automatica del nastro.
4. Nel menu Operazioni, scegli Configura la creazione automatica del nastro.
5. Per eliminare un criterio di creazione automatica del nastro in un gateway, scegliere Rimuovi a destra della policy che si desidera eliminare.

   Per arrestare la creazione automatica del nastro in un gateway, eliminare tutte le policy di creazione automatica del nastro per tale gateway.

   Scegliere Salva modifiche per confermare l'eliminazione dei criteri di creazione automatica del nastro per il gateway di nastri virtuali selezionato.

   > **Note**
   >
   > L'eliminazione di un criterio di creazione automatica del nastro da un gateway non può essere annullata.

Per modificare le policy di creazione automatica dei nastri per un gateway di nastri virtuali

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere la scheda Gateways (Gateway).
3. Scegliere il gateway per il quale è necessario gestire la creazione automatica del nastro.

4. Nel menu Operazioni, scegli Configura la creazione automatica del nastro e modifica le impostazioni nella pagina visualizzata.
5. In Numero minimo di nastri, immettere il numero minimo di nastri virtuali che devono essere sempre disponibili sul gateway di nastri virtuali. L'intervallo valido per questo valore è un minimo di 1 e un massimo di 10.
6. Per Capacità, immettere le dimensioni in byte della capacità del nastro virtuale. L'intervallo valido per questo valore è un minimo di 100 GiB e un massimo di 15 TiB.
7. In Barcode prefix (Prefisso codice a barre), digitare il prefisso che si vuole aggiungere al codice a barre dei nastri virtuali.

   > **Note**
   >
   > I nastri virtuali sono identificati in modo univoco da un codice a barre ed è possibile aggiungere un prefisso al codice a barre. Il prefisso è facoltativo, ma può essere usato per identificare meglio i nastri virtuali. Il prefisso deve contenere lettere maiuscole (A–Z) e deve essere costituito da uno a quattro caratteri.

8. Per Pool, scegliere Glacier Pool o Deep Archive Pool. Questo pool rappresenta la classe di storage in cui il nastro sarà archiviato quando viene espulso dal software di backup.

   - Scegli Glacier Pool se desideri archiviare i nastri nella classe di archiviazione S3 Glacier Flexible Retrieval. Quando il software di backup espelle i nastri, vengono automaticamente archiviati in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per più archivi attivi in cui è possibile recuperare un nastro, generalmente entro 3-5 ore. Per informazioni dettagliate, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.
   - Scegliere Deep Archive Pool se si desidera archiviare i nastri in S3 Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore. Per informazioni dettagliate, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.

Se si archivia i nastri in S3 Glacier Flexible Retrieval, è possibile spostarli in S3 Glacier Deep Archive in un secondo momento. Per ulteriori informazioni, consulta Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive.

9. Puoi trovare informazioni riguardo i nastri nella pagina Panoramica dei nastri virtuali. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.

   Lo stato dei nastri virtuali è inizialmente impostato su CREATING (CREAZIONE IN CORSO) quando i nastri virtuali sono in fase di creazione. Al termine della creazione, lo stato dei nastri passa a AVAILABLE (DISPONIBILE). Per ulteriori informazioni, consulta Gestione del gateway di nastri virtuali.

   Per ulteriori informazioni sull'abilitazione della creazione automatica del nastro, consulta Creazione automatica di nastri.

Archiviazione di nastri virtuali

Puoi archiviare i nastri in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Quando si crea un nastro, si sceglie il pool di archivio che si desidera utilizzare.

Scegli Glacier Pool se desideri archiviare il nastro in S3 Glacier Flexible Retrieval. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per archivi più attivi in cui i dati vengono regolarmente recuperati e sono necessari entro pochi minuti. Per ulteriori informazioni, consulta Storage Classes for Archiving Objects.

Scegliere Deep Archive Pool se si desidera archiviare il nastro in S3 Glacier Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale a costi estremamente contenuti. I dati in S3 Glacier Deep Archive non vengono recuperati spesso o vengono recuperati raramente. Per informazioni dettagliate, consulta Classi di storage per l'archiviazione degli oggetti (storage Classes for Archiving Objects).

> **Note**
>
> I nastri creati prima del 27 marzo 2019 sono archiviati direttamente in S3 Glacier Flexible Retrieval quando il software di backup li espelle.

Quando il software di backup espelle un nastro, viene automaticamente archiviato nel pool scelto quando è stato creato il nastro. Il processo di espulsione di un nastro varia a seconda del software di backup. Alcuni software di backup richiedono l'esportazione dei nastri dopo l'espulsione prima di iniziare l'archiviazione. Per ulteriori informazioni in merito al software di backup supportato, consulta Utilizzo del software di backup per testare la configurazione del gateway.

Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive

Spostare i nastri da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione di dati digitali ad un costo molto basso. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. Per informazioni dettagliate, consulta Classi di storage per l'archiviazione degli oggetti (storage Classes for Archiving Objects).

Per spostare un nastro da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive

1. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.
2. Seleziona le caselle di controllo per i nastri che desideri spostare in S3 Glacier Deep Archive. È possibile visualizzare il pool al quale ogni nastro è associato nella colonna Pool.
3. Scegli Assegna al pool.
4. Nella finestra di dialogo Assegna nastro al pool, verificare i codici a barre che si sta spostando e scegliere Assegna.

> **Note**
>
> Se un nastro è stato espulso dall'applicazione di backup e archiviato in S3 Glacier Deep Archive, non sarà possibile rispostarlo in S3 Glacier Flexible Retrieval. Lo spostamento dei nastri da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive comporta un addebito. Inoltre, se si spostano nastri da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive prima di 90 giorni, c'è una tariffa di eliminazione anticipata per S3 Glacier Flexible Retrieval.

5. Dopo lo spostamento del nastro, è possibile vedere lo stato aggiornato nella colonna Pool della pagina Panoramica dei nastri virtuali.

Recupero di nastri archiviati

Per accedere ai dati archiviati in un nastro virtuale archiviato, è prima necessario recuperare il nastro desiderato e spostarlo nel gateway di nastri virtuali. Il gateway di nastri virtuali fornisce una libreria di nastri virtuali (VTL) per ogni gateway.

Se si dispone di più di un Tape Gateway in un unico gateway Regione AWS, è possibile recuperare un nastro su un solo gateway.

Il nastro recuperato è protetto da scrittura ed è possibile solo leggere i dati presenti.

> **Important**
>
> È possibile recuperare un nastro archiviato in S3 Glacier Flexible Retrieval, generalmente entro 3-5 ore. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore.

> **Note**
>
> Il recupero di nastri dall'archivio prevede l'addebito di costi. Per informazioni dettagliate sui prezzi, consulta Prezzi di Storage Gateway.

Per recuperare un nastro archiviato e spostarlo nel gateway

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.
3. Scegli il nastro virtuale che desideri recuperare dalla scheda Scaffali di nastri virtuali e scegli Recupera nastro.

   > **Note**
   >
   > Lo stato del nastro virtuale da recuperare deve essere ARCHIVED (ARCHIVIATO).

4. Nella finestra di dialogo Retrieve tape (Recupera nastro), per Barcode (Codice a barre) verificare che il codice a barre identifichi il nastro virtuale che si desidera recuperare.
5. Per Gateway, scegliere il gateway in cui inserire il nastro archiviato recuperato e quindi scegliere Retrieve tape (Recupera nastro).

Lo stato del nastro cambia da ARCHIVED (ARCHIVIATO) a RETRIEVING (RECUPERO IN CORSO). A questo punto, i dati vengono spostati dallo scaffale di nastri virtuali (supportato da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) alla libreria di nastri virtuali (supportata da Amazon S3). Dopo che tutti i dati sono stati spostati, lo stato del nastro virtuale nell'archivio cambia in RETRIEVED (RECUPERATO).

> **Note**
>
> I nastri virtuali recuperati sono di sola lettura.

Visualizzazione dell'utilizzo dei nastri

Quando scrivi dati in un nastro, puoi visualizzare la quantità di dati archiviati nel nastro nella console Storage Gateway. La scheda Details (Dettagli) per ogni nastro mostra le informazioni sull'utilizzo del nastro.

Per visualizzare la quantità di dati archiviati su un nastro

1. Aprire la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.
3. Scegliete il nastro che vi interessa.
4. La pagina visualizzata fornisce vari dettagli e informazioni sul nastro, tra cui:
   - Size (Dimensioni): capacità totale del nastro selezionato.
   - Used (Spazio usato): dimensioni dei dati scritti sul nastro dall'applicazione di backup.

     > **Note**
     >
     > Questo valore non è disponibile per i nastri creati prima del 13 maggio 2015.

Eliminazione di nastri

È possibile eliminare i nastri virtuali dal gateway di nastri virtuali usando la console Storage Gateway.

> **Note**
>
> Se il nastro da eliminare dal gateway di nastri virtuali ha lo stato RECUPERATO, prima di eliminarlo è necessario espellerlo usando l'applicazione di backup. Per istruzioni su come espellere un nastro utilizzando il NetBackup software Symantec, vedere Archiviazione del

nastro. Dopo che il nastro è stato espulso, il suo stata cambia in ARCHIVED (ARCHIVIATO). A questo punto, è possibile eliminare il nastro.

Crea copie dei dati prima di eliminare i nastri. Dopo aver eliminato un nastro, non potrai più recuperarlo.

Per eliminare un nastro virtuale

> **Warning**
>
> Questa procedura elimina il nastro virtuale selezionato in modo permanente.

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.
3. Selezionare uno o più nastri da eliminare.
4. In Operazioni, scegliere Elimina nastro. Viene visualizzata la finestra di dialogo di conferma.
5. Verifica di voler eliminare i nastri specificati, quindi digita la parola delete nella casella di conferma e scegli Elimina.

Dopo l'eliminazione, il nastro non è più presente nel gateway di nastri virtuali.

Eliminazione di pool di nastri personalizzati

È possibile eliminare un pool di nastri personalizzato solo se nel pool non sono presenti nastri archiviati e al pool non sono associate politiche di creazione automatica dei nastri.

Per eliminare il pool di nastri personalizzato

1. Aprire la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.

2. Nel riquadro di navigazione, scegliere Pools per vedere i pool disponibili.
3. Selezionare uno o più pool di nastri da eliminare.

   Se il numero di nastri per i pool di nastri che si desidera eliminare è 0 e se non esistono politiche di creazione automatica di nastri che facciano riferimento al pool di nastri personalizzato, è possibile eliminare i pool.
4. Scegli Elimina. Viene visualizzata una finestra di dialogo di conferma.
5. Verifica di voler eliminare i pool di nastri specificati, quindi digita la parola delete nella casella di conferma e scegli Elimina.

   > ⚠ Warning
   >
   > Questa procedura elimina definitivamente i pool di nastri selezionati e non può essere annullata.

   Dopo l'eliminazione, i pool di nastri scompaiono dalla libreria di nastri.

Disattivazione del gateway di nastri virtuali

Puoi disabilitare un gateway di nastri virtuali se si è verificato un errore del gateway di nastri virtuali e desideri ripristinare i nastri in un altro gateway.

Per ripristinare i nastri devi prima disabilitare il gateway in cui si è verificato l'errore. La disabilitazione di un gateway di nastri virtuali blocca i nastri virtuali presenti nel gateway. Ciò significa che i dati scritti in questi nastri dopo la disabilitazione del gateway non vengono inviati ad AWS. È possibile disabilitare un gateway dalla console Storage gateway solo se il gateway non è più connesso ad AWS. Se il gateway è connesso a AWS, non è possibile disattivare il Tape Gateway.

Puoi disattivare un gateway di nastri virtuali come parte di un'operazione di ripristino dei dati. Per ulteriori informazioni sul ripristino di nastri, consulta È necessario recuperare un nastro virtuale da un gateway di nastri virtuali non funzionante.

Per disabilitare il gateway

1. Aprire la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.

2. Nel riquadro di navigazione scegliere Gateways (Gateway) e quindi selezionare il gateway in cui si è verificato l'errore.
3. Scegliere la scheda Details (Dettagli) per visualizzare il messaggio per la disabilitazione del gateway.
4. Scegliere Create recovery tapes (Crea nastri di ripristino).
5. Scegliere Disable gateway (Disabilita gateway).

Comprendere lo stato del nastro

Ogni nastro ha uno stato associato che indica chiaramente l'integrità del nastro. Nella maggior parte dei casi, lo stato indica che il nastro funziona correttamente e che non è richiesta nessuna operazione da parte tua. In alcuni casi, lo stato indica un problema con il nastro che potrebbe richiedere un'azione da parte tua. Puoi trovare le informazioni seguenti per aiutarti a decidere quando è necessario agire.

Argomenti

- Comprendere le informazioni sullo stato del nastro in una VTL
- Determinare lo stato del nastro in un archivio

Comprendere le informazioni sullo stato del nastro in una VTL

Affinché possa essere utilizzato in lettura e in scrittura, lo stato del nastro deve essere DISPONIBILE. La tabella seguente elenca e descrive i possibili valori dello stato.

Stato	Descrizione	Dati nastro archiviati
CREAZIONE IN CORSO	Il nastro virtuale è in fase di creazione. Il nastro non può essere caricato in un'unità nastro, perché il nastro è in fase di creazione.	—
DISPONIBILE	Il nastro virtuale viene creato ed è pronto per essere caricato in un'unità nastro.	Amazon S3
IN TRANSIT TO VTS (IN	Il nastro virtuale è stato espulso ed è in fase di caricamento per l'archiviazione. A questo punto, il Tape Gateway sta caricando i dati su. AWS Se la	Amazon S3

Stato	Descrizione	Dati nastro archiviati
TRANSITO VERSO VTS)	quantità di dati da caricare è piccola, questo stato potrebbero non essere visualizzato. Al termine del caricamento, lo stato diventa ARCHIVING (ARCHIVIA ZIONE).	
ARCHIVING (ARCHIVIA ZIONE)	Il nastro virtuale viene spostato dal gateway di nastri virtuali all'archivio, che è supportato da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Questo processo avviene dopo il completamento del caricamento dei dati su. AWS	I dati vengono trasferiti da Amazon S3 a S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
ELIMINAZI ONE IN CORSO	Il nastro virtuale è in fase di eliminazione.	I dati vengono eliminati da Amazon S3
ELIMINATO	Il nastro virtuale è stato eliminato.	—
RICHIAMO IN CORSO	Il nastro virtuale viene richiamato dall'archivio sul gateway di nastri virtuali. **Note** I nastri virtuali possono essere richiamati solo su un gateway di nastri virtuali.	I dati vengono trasferit i da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive ad Amazon S3
RICHIAMAT O	Il nastro virtuale è stato richiamato dall'archivio. Il nastro richiamato è protetto da scrittura.	Amazon S3
RECUPERAT O	Il nastro virtuale viene recuperato ed è di sola lettura. Quando il gateway di nastri virtuali non è accessibile per qualsiasi motivo, è possibile recuperare i nastri virtuali associati a tale gateway di nastri virtuali a un altro gateway di nastri virtuali. Per recuperare i nastri virtuali, disabilitare innanzitutto il gateway di nastri virtuali inaccessibile.	Amazon S3

Stato	Descrizione	Dati nastro archiviati
IRRECUPERABILE	Il nastro virtuale non può essere usato né in lettura né in scrittura. Questo stato indica un errore nel gateway di nastri virtuali.	Amazon S3

Determinare lo stato del nastro in un archivio

È possibile utilizzare la procedura seguente per determinare lo stato di un nastro virtuale in un archivio.

Per determinare lo stato di un nastro virtuale

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione selezionare Tapes (Nastri).
3. Nella colonna Status (Stato) della griglia della libreria di nastri, controllare lo stato del nastro.

   Lo stato del nastro viene visualizzato anche nella scheda Details (Dettagli) di ogni nastro virtuale.

In seguito, è possibile trovare una descrizione dei possibili valori di stato.

Stato	Descrizione
ARCHIVIATO	Il nastro virtuale è stato espulso ed è caricato nell'archivio.
RICHIAMO IN CORSO	Il nastro virtuale viene richiamato dall'archivio. **Note** I nastri virtuali possono essere richiamati solo su un gateway di nastri virtuali.
RICHIAMATO	Il nastro virtuale è stato richiamato dall'archivio. Il nastro richiamato è di sola lettura.

Per ulteriori informazioni su come gestire i nastri e i dispositivi VTL, consulta Utilizzo dei nastri.

Spostamento dei dati su un nuovo gateway

Puoi spostare i dati tra i gateway man mano che le tue esigenze di dati e prestazioni aumentano o se ricevi una AWS notifica per migrare il gateway. Di seguito sono riportati alcuni motivi per eseguire questa operazione:

- Sposta i dati su più piattaforme host o su nuove istanze Amazon EC2.
- Aggiorna l'hardware utilizzato per il tuo server.

I passaggi da seguire per spostare i dati su un nuovo gateway dipendono dal tipo di gateway in uso.

> **Note**
>
> I dati possono essere spostati solo tra gli stessi tipi di gateway.

Spostamento di nastri virtuali al nuovo gateway di nastri virtuali

Per spostare i nastri virtuali al nuovo gateway di nastri virtuali

1. Usa la tua applicazione di backup per eseguire il backup di tutti i tuoi dati su un nastro virtuale. Attendi che il backup venga completato correttamente.
2. Usa l'applicazione di backup per espellere il nastro. Il nastro verrà archiviato in una delle classi di archiviazione Amazon S3. I nastri espulsi vengono archiviati in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive e sono di sola lettura.

   Prima di procedere, verifica che i nastri espulsi siano stati archiviati:

   a. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.

   b. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di

1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.

c. Nella colonna Stato dell'elenco, controllare lo stato del nastro.

   Lo stato del nastro viene visualizzato anche nella scheda Details (Dettagli) di ogni nastro virtuale.

   Per ulteriori informazioni sulla determinazione dello stato dei nastri in un archivio, consulta Determinare lo stato del nastro in un archivio.

3. Utilizzando l'applicazione di backup, verifica che non vi siano processi di backup attivi sul gateway di nastri virtuali esistente prima di interromperlo. Se sono presenti processi di backup attivi, attendi che finiscano e vengano espulsi i nastri (vedi il passaggio precedente) prima di arrestare il gateway.
4. Utilizza la procedura seguente per interrompere il gateway di nastri virtuali:

   a. Nel riquadro di navigazione scegliere Gateway e quindi scegliere il vecchio gateway di nastri virtuali da interrompere. Lo stato del gateway è Running (In esecuzione).

   b. In Operazioni, scegli Arresta gateway. Verificare l'ID del gateway dalla finestra di dialogo, quindi scegliere Arresta gateway.

      Durante l'arresto del vecchio gateway di nastri virtuali, è possibile che venga visualizzato un messaggio che indica lo stato del gateway. Quando il gateway viene arrestato, sulla scheda Dettagli vengono visualizzati un messaggio e un pulsante Avvia gateway.

   Per informazioni su come arrestare un gateway, consulta Avvio e arresto di un gateway d nastri virtuali.
5. Crea un nuovo gateway di nastri virtuali. Per istruzioni dettagliate, consulta Creazione di un gateway.
6. Utilizzare la procedura seguente per creare nuovi nastri:

   a. Nel riquadro di navigazione scegliere la scheda Gateways (Gateway).

   b. Scegliere Crea nastri per aprire la finestra di dialogo Crea nastro.

   c. Per Gateway, scegliere un gateway. Il nastro viene creato per questo gateway.

   d. Per Number of tapes (Numero di nastri), scegliere il numero di nastri che si vuole creare. Per ulteriori informazioni sui limiti relativi ai nastri, consulta AWS Storage Gateway quote.

A questo punto è inoltre possibile impostare la creazione automatica dei nastri. Per ulteriori informazioni, consulta Creazione automatica di nastri.

e. In Capacità, immettere le dimensioni del nastro virtuale che si desidera creare. I nastri devono avere dimensioni maggiori di 100 GiB. Per informazioni sui limiti di capacità, consulta AWS Storage Gateway quote.

f. In Barcode prefix (Prefisso codice a barre), digitare il prefisso che si vuole aggiungere al codice a barre dei nastri virtuali.

> **Note**
>
> I nastri virtuali sono identificati in modo univoco da un codice a barre. È possibile aggiungere un prefisso al codice a barre. Il prefisso è facoltativo, ma può essere usato per identificare meglio i nastri virtuali. Il prefisso deve contenere lettere maiuscole (A–Z) e deve essere costituito da uno a quattro caratteri.

g. Per Pool, scegliere Glacier Pool o Deep Archive Pool. Questo pool rappresenta la classe di storage in cui il nastro sarà archiviato quando viene espulso dal software di backup.

   Scegli Glacier Pool se desideri archiviare il nastro in S3 Glacier Flexible Retrieval. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Flexible Retrieval. È possibile utilizzare S3 Glacier Flexible Retrieval per più archivi attivi in cui è possibile recuperare un nastro, generalmente entro 3-5 ore. Per ulteriori informazioni, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.

   Scegliere Deep Archive Pool se si desidera archiviare il nastro in S3 Deep Archive. Quando il software di backup espelle il nastro, viene automaticamente archiviato in S3 Glacier Deep Archive. È possibile utilizzare S3 Glacier Deep Archive per la conservazione dei dati a lungo termine e la conservazione digitale nel caso in cui l'accesso ai dati avvenga una o due volte all'anno. È possibile recuperare un nastro archiviato in S3 Glacier Deep Archive, generalmente entro 12 ore. Per ulteriori informazioni, consulta Classi di archiviazione per archiviare oggetti nella Guida per l'utente di Amazon Simple Storage Service.

   Se si archivia un nastro in S3 Glacier Flexible Retrieval, è possibile spostarlo in S3 Glacier Deep Archive in un secondo momento. Per ulteriori informazioni, consulta Spostamento del nastro da S3 Glacier Flexible Retrieval alla classe di archiviazione S3 Glacier Deep Archive.

> **Note**
>
> I nastri creati prima del 27 marzo 2019 sono archiviati direttamente in S3 Glacier Flexible Retrieval quando il software di backup li espelle.

h. (Facoltativo) In Tags (Tag), immettere una chiave e un valore per aggiungere tag al nastro. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare i nastri.

i. Scegliere Create tapes (Crea nastri).

7. Utilizza l'applicazione di backup per avviare un processo di backup ed eseguire il backup dei dati sul nuovo nastro.

8. (Facoltativo) Se il nastro è archiviato e devi ripristinare i dati da esso, recuperalo sul nuovo gateway di nastri virtuali. Il nastro sarà in modalità di sola lettura. Per ulteriori informazioni sul recupero dei nastri archiviati, consulta la sezione Recupero di nastri archiviati.

> **Note**
>
> Potrebbero venire applicati costi per la trasmissione di dati in uscita.

a. Nel riquadro di navigazione, scegliere Libreria di nastri>Nastri per visualizzare i propri nastri. Per impostazione predefinita, questo elenco visualizza fino a 1.000 nastri virtuali alla volta, ma le ricerche eseguite si applicano a tutti i nastri. È possibile utilizzare la barra di ricerca per trovare nastri virtuali che soddisfano criteri specifici o per ridurre l'elenco a meno di 1.000 nastri. Se l'elenco contiene al massimo 1.000 nastri, è possibile ordinarli in ordine crescente o decrescente in base a varie proprietà.

b. Scegliere il nastro virtuale da recuperare. Per Operazioni, scegli Recupera nastro.

> **Note**
>
> Lo stato del nastro virtuale da recuperare deve essere `ARCHIVED`.

c. Nella finestra di dialogo Retrieve tape (Recupera nastro), per Barcode (Codice a barre) verificare che il codice a barre identifichi il nastro virtuale che si desidera recuperare.

d. Per Gateway, scegliere il nuovo gateway di nastri virtuali in cui inserire il nastro archiviato recuperato e quindi scegliere Recupera nastro.

Dopo aver verificato che il nuovo gateway di nastri virtuali funziona correttamente, è possibile eliminare il vecchio gateway di nastri virtuali.

> **Important**
>
> Prima di eliminare un gateway, 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.

9. Utilizza i seguenti passaggi per eliminare il vecchio gateway di nastri virtuali:

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

   a. Nel riquadro di navigazione, scegliere Gateway e selezionare il gateway da eliminare.
   b. Per Actions (Operazioni), scegli Delete stack (Elimina stack).

      Nella finestra di dialogo di conferma che appare, assicurati che l'ID del gateway elencato specifichi il vecchio gateway di nastri virtuali che desideri eliminare, immetti **`delete`** nel campo di conferma, quindi scegli Elimina.
   c. Eliminare la macchina virtuale. Per ulteriori informazioni su come eliminare una macchina virtuale, consultare la documentazione del proprio hypervisor.

Monitoraggio di Storage Gateway

Questa sezione descrive come monitorare un gateway, incluso il monitoraggio delle risorse associate al gateway, utilizzando Amazon CloudWatch. È possibile monitorare il buffer di caricamento e lo storage della cache del gateway. È possibile utilizzare la console Storage Gateway per visualizzare i parametri e gli allarmi per il gateway. Ad esempio, puoi visualizzare il numero di byte utilizzati nelle operazioni di lettura e scrittura, il tempo impiegato per le operazioni di lettura e scrittura e il tempo impiegato per recuperare i dati dal Cloud Amazon Web Services. I parametri consentono di monitorare l'integrità del gateway e di impostare allarmi di notifica quando uno o più parametri sono al di fuori di una soglia definita.

Storage Gateway fornisce CloudWatch metriche senza costi aggiuntivi. I parametri Storage Gateway sono registrati per un periodo di due settimane. Utilizzando questi parametri, puoi accedere alle informazioni cronologiche e avere una migliore percezione delle performance di gateway e volumi. Storage Gateway fornisce anche CloudWatch allarmi, ad eccezione degli allarmi ad alta risoluzione, senza costi aggiuntivi. Per ulteriori informazioni sui CloudWatch prezzi, consulta la pagina CloudWatch dei prezzi di Amazon. Per ulteriori informazioni su CloudWatch, consulta Amazon CloudWatch User Guide.

Argomenti

Comprendere i parametri del gateway

Per la discutere di questo argomento, definiamo i parametri del gateway come parametri che rientrano nell'ambito del gateway ovvero misurano determinati aspetti del gateway. Poiché un gateway contiene uno o più volumi, un parametro specifico del gateway è rappresentativo di tutti i

volumi sul gateway. Ad esempio, il parametro `CloudBytesUploaded` rappresenta il numero totale di byte che il gateway invia al cloud durante il periodo di reporting. Questo parametro include l'attività di tutti i volumi nel gateway.

Quando si utilizzano i dati dei parametri gateway, è necessario specificare l'identificativo univoco del gateway di cui si desidera visualizzare i parametri. Per questo, specificare i valori `GatewayId` e `GatewayName`. Per utilizzare un parametro per il gateway, specificare la dimensione del gateway nello spazio dei nomi del parametro, che distingue un parametro specifico del gateway da un parametro specifico del volume. Per ulteriori informazioni, consulta Utilizzo di Amazon CloudWatch Metrics.

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

Parametro	Descrizione
`AvailabilityNotifications`	Numero di notifiche di stato relative alla disponibilità generate dal gateway. Utilizza questo parametro con la statistica `Sum` per verificare se il gateway sta riscontrando eventi correlati alla disponibilità. Per dettagli sugli eventi, controlla il gruppo di CloudWatch log configurato. Unità: numero
`CacheHitPercent`	Percentuale di letture delle applicazioni servite dalla cache. Il campione si riferisce al termine del periodo di reporting.

Parametro	Descrizione	
	Unità: percentuale	
`CacheUsed`	Numero totale di byte utilizzati nello storage della cache del gateway. Il campione si riferisce al termine del periodo di reporting. Unità: byte	
`IoWaitPercent`	Percentuale di tempo durante la quale il gateway è in attesa di una risposta dal disco locale. Unità: percentuale	
`MemTotalBytes`	Quantità di RAM assegnata alla macchina virtuale del gateway, in byte. Unità: byte	
`MemUsedBytes`	Quantità di RAM attualmente utilizzata dalla macchina virtuale del gateway, in byte. Unità: byte	
`QueuedWrites`	Il numero di byte in attesa di scrittura AWS, prelevato alla fine del periodo di riferimento per tutti i volumi del gateway. Questi byte sono conservati nello storage di lavoro del gateway. Unità: byte	

Parametro	Descrizione
`TotalCacheSize`	Dimensione totale della cache in byte. Il campione si riferisce al termine del periodo di reporting. Unità: byte
`UploadBufferPercentUsed`	Percentuale di utilizzo del buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting. Unità: percentuale
`UploadBufferUsed`	Numero totale di byte utilizzati nel buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting. Unità: byte
`UserCpuPercent`	Percentuale di tempo CPU impiegato per l'elaborazione del gateway, calcolata in media su tutti i core. Unità: percentuale

Dimensioni per i parametri di Storage Gateway

Lo spazio dei CloudWatch nomi per il servizio Storage Gateway è. `AWS/StorageGateway` I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.

Dimensione	Descrizione
`GatewayId` , `GatewayName`	Queste dimensioni filtrano i dati richiesti sui parametri specifici per il gateway. Puoi identificare un gateway mediante il valore `GatewayId` o `GatewayName` . Se il nome del gateway è cambiato per l'intervallo di tempo per cui vuoi visualizzare i parametri, utilizza `GatewayId` . I dati di throughput e latenza di un gateway si basano su tutti i volumi per il gateway. Per informazioni sull'utilizzo delle metriche del gateway, consulta Measuring Performance Between Your Gateway and. AWS

Monitoraggio del buffer di caricamento

Puoi trovare le informazioni seguenti su come monitorare un buffer di caricamento di un gateway e come creare un allarme in modo da ottenere una notifica quando il buffer supera una soglia specificata. Grazie a questo approccio, è possibile aggiungere lo storage del buffer a un gateway prima che si riempia completamente e prima che l'applicazione di storage interrompa l'esecuzione del backup su AWS.

Il monitoraggio del buffer di caricamento è identico sia nelle architetture nel volume memorizzato nella cache sia in quelle del gateway di nastri virtuali. Per ulteriori informazioni, consulta Come funziona il gateway di nastri virtuali (architettura).

> **Note**
>
> I parametri `WorkingStoragePercentUsed`, `WorkingStorageUsed` e `WorkingStorageFree` rappresentano il buffer di caricamento dei volumi archiviati solo prima del rilascio della funzionalità del volume nella cache in Storage Gateway. Utilizza i parametri del buffer di caricamento equivalenti `UploadBufferPercentUsed`, `UploadBufferUsed` e `UploadBufferFree`. Queste metriche si applicano a entrambe le architetture del gateway.

Articolo di interesse	Come misurare
Utilizzo del buffer di caricamento	Utilizzare i parametri `UploadBufferPercentUsed` , `UploadBufferUsed` e `UploadBufferFree` con la statistica `Average`. Ad esempio, utilizzare `UploadBufferUsed` con la statistica `Average` per analizzare l'impiego dello storage per un dato periodo di tempo.

Per misurare la percentuale del buffer di caricamento utilizzato

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli la dimensione StorageGateway: Gateway Metrics e trova il gateway con cui desideri lavorare.
3. Scegliere il parametro `UploadBufferPercentUsed`.
4. Scegliere un valore per Time Range (Intervallo di tempo).
5. Scegliere la statistica `Average`.
6. Per Period (Periodo), selezionare un valore di 5 minuti corrispondente a un tempo di reporting predefinito.

Il risultante set di punti di dati in ordine cronologico contiene la percentuale di utilizzo del buffer di caricamento.

Utilizzando la procedura seguente, è possibile creare un allarme utilizzando la CloudWatch console. Per ulteriori informazioni su allarmi e soglie, consulta Creating CloudWatch Alarms nella Amazon User Guide. CloudWatch

Per impostare un allarme soglia superiore allarme per un buffer di caricamento del gateway

1. Apri la console all'indirizzo https://console.aws.amazon.com/cloudwatch/ CloudWatch .
2. Scegliere Create Alarm (Crea allarme) per avviare la procedura guidata di creazione allarme.
3. Specificare un parametro per l'allarme.
    a. Nella pagina Seleziona metrica della procedura guidata Create Alarm, scegli la GatewayName dimensione AWS/StorageGateway:GatewayId, quindi trova il gateway con cui desideri lavorare.

b. Scegliere il parametro `UploadBufferPercentUsed`. Utilizzare la statistica `Average` e un periodo di 5 minuti.

c. Scegli Continua.

4. Definire il nome dell'allarme, la descrizione e la soglia:

a. Nella pagina Define Alarm (Definisci allarme) della procedura guidata di creazione allarme, identificare l'allarme assegnando a esso un nome e una descrizione nelle caselle Name (Nome) e Description (Descrizione).

b. Definire la soglia dell'allarme.

c. Scegli Continua.

5. Configurare un'operazione e-mail per l'allarme:

a. Nella pagina Configure Actions (Configura azioni) della procedura guidata di creazione allarme, selezionare Alarm (Allarme) per Alarm State (Stato allarme).

b. Selezionare Choose or create email topic (Seleziona o crea argomento e-mail) per Topic (Argomento).

Creare un argomento e-mail significa impostare un argomento Amazon SNS. Per ulteriori informazioni su Amazon SNS, consulta Configurare Amazon SNS nella Amazon User Guide. CloudWatch

c. In Topic (Argomento), immettere un nome descrittivo per l'argomento.

d. Selezionare Add action (Aggiungi operazione).

e. Scegli Continua.

6. Esaminare le impostazioni di allarme e quindi creare l'allarme.

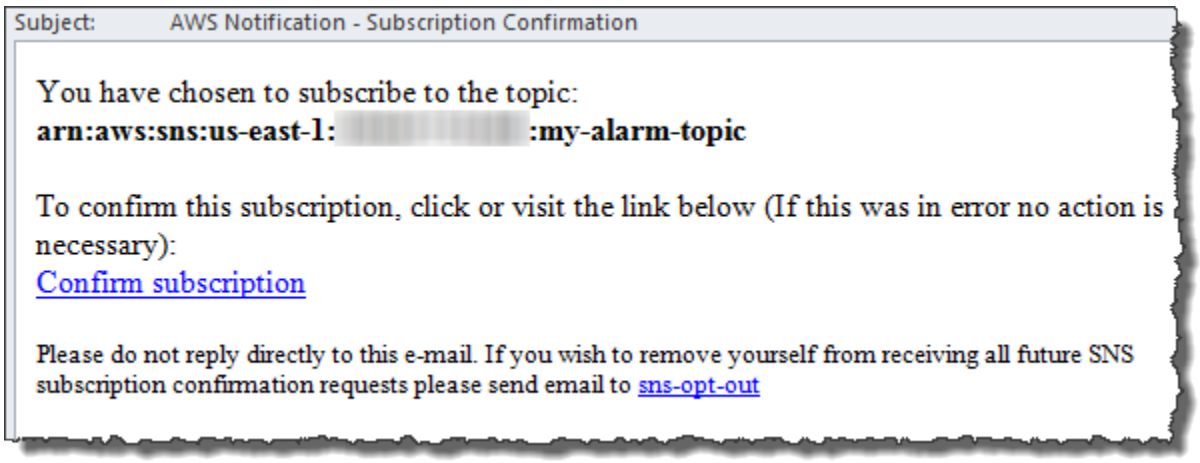
a. Nella pagina Review (Revisiona) della procedura guidata di creazione allarme, rivedere la definizione allarme, i parametri e le operazioni associate da intraprendere (ad esempio, l'invio di una notifica e-mail).

b. Dopo avere rivisto il riepilogo degli allarmi, selezionare Save Alarm (Salva allarme).

7. Confermare la sottoscrizione all'argomento allarmi.

a. Aprire il messaggio e-mail Amazon SNS inviato all'indirizzo e-mail che è stato specificato durante la creazione dell'argomento.

L'immagine seguente mostra una tipica notifica e-mail.



b. Confermare la sottoscrizione facendo clic sul link contenuto nel messaggio e-mail.

   Viene visualizzata una conferma di sottoscrizione.

Monitoraggio dello storage della cache

Puoi trovare le informazioni seguenti su come monitorare lo storage della cache del gateway e su come creare un allarme in modo da ottenere una notifica quando i parametri della cache superano le soglie specificate. Utilizzando questo allarme, capisci quando aggiungere lo storage della cache a un gateway.

Puoi monitorare solo lo storage della cache nell'architettura dei volumi della cache. Per ulteriori informazioni, consulta Come funziona il gateway di nastri virtuali (architettura).

Articolo di interesse	Come misurare
Utilizzo totale della cache	Utilizzare i parametri `CachePercentUsed` e `TotalCacheSize` con la statistica `Average`. Ad esempio, utilizzare `CachePercentUsed` con la statistica `Average` per analizzare l'impiego della cache per un dato periodo di tempo. Il parametro `TotalCacheSize` cambia solo quando aggiungi cache al gateway.
La percentuale di richieste di lettura gestite dalla cache.	Utilizzare il parametro `CacheHitPercent` con la statistica `Average`.

Articolo di interesse	Come misurare
	Generalmente, desideri che il valore `CacheHitPercent` rimanga elevato.
Percentuale di cache sporca, vale a dire che contiene contenuti su cui non è stato caricato AWS	Utilizzare i parametri `CachePercentDirty` con la statistica `Average`. Generalmente, desideri che il valore `CachePercentDirty` rimanga basso.

Per misurare la percentuale di una cache sporca per un gateway e tutti i suoi volumi

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli la dimensione StorageGateway: Gateway Metrics e trova il gateway con cui desideri lavorare.
3. Scegliere il parametro `CachePercentDirty`.
4. Scegliere un valore per Time Range (Intervallo di tempo).
5. Scegliere la statistica `Average`.
6. Per Period (Periodo), selezionare un valore di 5 minuti corrispondente a un tempo di reporting predefinito.

Il risultante set di punti di dati in ordine cronologico contiene la percentuale di cache sporca oltre i 5 minuti.

Per misurare la percentuale della cache sporca per un volume

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli la dimensione StorageGateway: Volume Metrics e trova il volume con cui desideri lavorare.
3. Scegliere il parametro `CachePercentDirty`.
4. Scegliere un valore per Time Range (Intervallo di tempo).
5. Scegliere la statistica `Average`.
6. Per Period (Periodo), selezionare un valore di 5 minuti corrispondente a un tempo di reporting predefinito.

Il risultante set di punti di dati in ordine cronologico contiene la percentuale di cache sporca oltre i 5 minuti.

Comprensione degli allarmi CloudWatch

CloudWatch gli allarmi monitorano le informazioni sul gateway in base a metriche ed espressioni. È possibile aggiungere CloudWatch allarmi per il gateway e visualizzarne lo stato nella console Storage Gateway. Per ulteriori informazioni sui parametri utilizzati per monitorare il gateway di nastri virtuali, consulta Comprensione dei parametri del gateway e Comprensione dei parametri dei nastri virtuali. Per ogni allarme, si specificano le condizioni che avvieranno lo stato ALLARME. Gli indicatori di stato degli allarmi nella console Storage Gateway diventano rossi quando si trova nello stato ALLARME, semplificando il monitoraggio dello stato in modo proattivo. È possibile configurare gli allarmi per richiamare automaticamente le azioni in base a cambiamenti di stato sostenuti. Per ulteriori informazioni sugli CloudWatch allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

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

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

- Attesa I/O elevata: `IoWaitpercent` >= 20 per 3 antidatato in 15 minuti
- Percentuale di cache dirty: `CachePercentDirty` > 80 per 4 datapoint entro 20 minuti
- Notifiche di stato: `HealthNotifications` >= 1 per 1 datapoint entro 5 minuti. Quando configuri questo allarme, imposta Trattamento dei dati mancanti su notBreaching.

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

Per i gateway su piattaforme host VMware con modalità HA attivata, consigliamo anche questo allarme aggiuntivo: CloudWatch

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

Nella tabella seguente viene descritto lo stato di un allarme.

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

Creazione di CloudWatch allarmi consigliati per il gateway

Quando si crea un nuovo gateway utilizzando la console Storage Gateway, è possibile scegliere di creare automaticamente tutti gli CloudWatch allarmi consigliati come parte del processo di configurazione iniziale. Per ulteriori informazioni, consulta Configurazione del gateway di nastri virtuali. Se si desidera aggiungere o aggiornare gli CloudWatch allarmi consigliati per un gateway esistente, utilizzare la procedura seguente.

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

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

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home/.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri creare gli allarmi consigliati. CloudWatch
3. Nella pagina dei dettagli del gateway, scegliere la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarmi consigliati. Gli allarmi consigliati vengono creati automaticamente.

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

Creazione di un CloudWatch allarme personalizzato per il gateway

CloudWatch utilizza Amazon Simple Notification Service (Amazon SNS) per inviare notifiche di allarme quando un allarme cambia stato. Un allarme controlla un singolo parametro in un periodo di tempo specificato ed esegue una o più operazioni in base al valore del parametro relativo a una determinata soglia in una serie di periodi di tempo. L'operazione corrisponde all'invio di una notifica a un argomento Amazon SNS. Puoi creare un argomento Amazon SNS quando crei un CloudWatch allarme. Per ulteriori informazioni su Amazon SNS, consulta Che cos'è Amazon SNS? nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Per creare un CloudWatch allarme nella console Storage Gateway

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home/.
2. Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera creare un allarme.
3. Nella pagina dei dettagli del gateway, scegliere la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarme per aprire la CloudWatch console.
5. Usa la CloudWatch console per creare il tipo di allarme che desideri. Puoi creare i seguenti tipi di allarmi:

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

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

     Per creare un allarme di rilevamento delle anomalie, consulta Creazione di un CloudWatch allarme basato sul rilevamento delle anomalie nella Amazon CloudWatch User Guide.
   - Allarme di espressione matematica del parametro: un allarme basato su uno o più parametri utilizzati in un'espressione matematica. Si specificano l'espressione, la soglia e i periodi di valutazione.

     Per creare un allarme con espressione matematica metrica, consulta Creazione di un CloudWatch allarme basato su un'espressione matematica metrica nella Amazon User Guide. CloudWatch
   - Allarme composito: un allarme che determina il suo stato di allarme osservando gli stati di allarme di altri allarmi. Un allarme composito può aiutare a ridurre il rumore di allarme.

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

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

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

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

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

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

Monitoraggio del gateway di nastri virtuali

Questa sezione illustra come monitorare il gateway di nastri virtuali, i nastri virtuali associati ad esso, lo storage della cache e il buffer di caricamento. Lo usi AWS Management Console per visualizzare le metriche per il tuo Tape Gateway. Con i parametri puoi monitorare l'integrità del gateway di nastri virtuali e configurare allarmi per ricevere notifiche quando uno o più parametri superano una soglia specificata.

Storage Gateway fornisce CloudWatch metriche senza costi aggiuntivi. I parametri Storage Gateway sono registrati per un periodo di due settimane. Usando questi parametri, puoi accedere a informazioni cronologiche e ottenere una prospettiva migliore delle prestazioni del gateway di nastri

virtuali e dei nastri virtuali. Per informazioni dettagliate in merito CloudWatch, consulta la Amazon CloudWatch User Guide.

Argomenti

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

Puoi utilizzare Amazon CloudWatch Logs per ottenere informazioni sullo stato del tuo Tape Gateway e delle risorse correlate. Puoi utilizzare i log per monitorare il gateway alla ricerca di errori riscontrati. Inoltre, puoi utilizzare i filtri di CloudWatch abbonamento Amazon per automatizzare l'elaborazione delle informazioni di registro in tempo reale. Per ulteriori informazioni, consulta Elaborazione in tempo reale dei dati di registro con abbonamenti nella Amazon CloudWatch User Guide.

Supponiamo, ad esempio, che il gateway sia distribuito in un cluster attivato con VMware HA e che vuoi essere informato su eventuali errori. Puoi configurare un gruppo di CloudWatch log per monitorare il gateway e ricevere una notifica quando il gateway rileva un errore. Puoi 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 CloudWatch log durante l'attivazione di un gateway, consulta Configura il tuo Tape Gateway. Per informazioni generali sui gruppi di CloudWatch log, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch User Guide.

Per informazioni su come risolvere errori di questo tipo, consulta Come risolvere i problemi dei nastri virtuali.

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

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

1. Accedere AWS Management Console e aprire la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.

2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per cui desideri configurare il CloudWatch Log Group.
3. Per Azioni, scegli Modifica informazioni sul gateway o nella scheda Dettagli, in Health logs e Not Enabled, scegli Configura gruppo di log per aprire la finestra di CustomerGatewayNamedialogo Modifica.
4. Per il Gruppo di log sullo stato del gateway, scegli una delle seguenti opzioni:

   - Disabilita la registrazione se non desideri monitorare il gateway utilizzando i gruppi di CloudWatch log.
   - Crea un nuovo gruppo di log per creare un nuovo gruppo di CloudWatch log.
   - Utilizza un gruppo di log esistente per utilizzare un gruppo di CloudWatch log già esistente.

     Scegli un gruppo di log dall'elenco dei gruppi di log esistenti.
5. Seleziona Salvataggio delle modifiche.
6. Per visualizzare i log sullo stato del gateway, procedi come indicato di seguito:

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

Di seguito è riportato un esempio di messaggio di evento Tape Gateway inviato a CloudWatch. Questo esempio mostra un messaggio `TapeStatusTransition`.

```
{
"severity": "INFO",
"source": "FZTT16FCF5",
"type": "TapeStatusTransition",
"gateway": "sgw-C51DFEAC",
"timestamp": "1581553463831",
"newStatus": "RETRIEVED"
}
```

Utilizzo di Amazon CloudWatch Metrics

Puoi ottenere i dati di monitoraggio per il tuo Tape Gateway utilizzando l'API AWS Management Console o l' CloudWatch API. La console visualizza una serie di grafici in base ai dati non elaborati dell'API di CloudWatch . L' CloudWatch API può essere utilizzata anche tramite uno degli Amazon AWS Software Development Kit (SDK) o gli strumenti Amazon CloudWatch API. In base alle tue esigenze, potresti decidere di utilizzare i grafici visualizzati nella console o quelli recuperati dall'API.

Indipendentemente dal metodo scelto per usare 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 di Storage Gateway sono `GatewayId` e `GatewayName`. Nella console CloudWatch puoi utilizzare la visualizzazione `Gateway Metrics` per selezionare in tutta semplicità dimensioni specifiche dei gateway e dei nastri. Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.
- Il nome del parametro, ad esempio `ReadBytes`.

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

Spazio dei CloudWatch nomi Amazon	Dimensione	Descrizione
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Queste dimensioni filtrano in base ai dati dei parametri che descrivono gli aspetti del gateway di nastri virtuali. Puoi identificare un gateway di nastri virtuali da usare specificando le dimensioni `GatewayId` e `GatewayName` . I dati di velocità di trasmissione effettiva e latenza di un gateway di nastri virtuali si basano su tutti i nastri virtuali nel gateway di nastri virtuali. I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.

L'uso di parametri di gateway e nastri 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 dei parametri disponibili
- Ottenimento di statistiche per un parametro
- Creazione di allarmi CloudWatch

Informazioni sui parametri dei nastri virtuali

Di seguito vengono fornite informazioni sui parametri Storage Gateway relativi a nastri virtuali. Ogni nastro ha una serie di parametri associati.

Alcuni parametri specifici dei nastri hanno lo stesso nome di alcuni parametri specifici del gateway. Questi parametri rappresentano lo stesso tipo di misure, ma vengono definiti per il nastro invece che per il gateway. Prima di iniziare, specifica se vuoi utilizzare un parametro di gateway o di nastro. Quando usi i parametri di nastri, specifica l'ID per il nastro di cui vuoi visualizzare i parametri. Per ulteriori informazioni, consulta Utilizzo di Amazon CloudWatch Metrics.

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

La tabella seguente descrive i parametri Storage Gateway che puoi utilizzare per ottenere informazioni sui nastri.

Parametro	Descrizione
`CachePercentDirty`	Contributo del nastro alla percentuale totale della cache del gateway non conservata in AWS. Il campione si riferisce al termine del periodo di reporting. Usa il parametro `CachePercentDirty` del gateway per visualizzare la percentuale

Parametro	Descrizione
	totale della cache del gateway non conservata in AWS. Per ulteriori informazioni, consulta Comprendere i parametri del gateway. Unità: percentuale
`CloudTraffic`	La quantità di byte caricati e scaricati dal cloud sul nastro. Unità: byte
`IoWaitPercent`	La percentuale di IoWait unità allocate attualmente utilizzate dal nastro. Unità: percentuale
`HealthNotification`	Il numero di notifiche di stato inviate dal nastro. Unità: conteggio
`MemUsedBytes`	Percentuale di memoria allocata attualmente utilizzata dal nastro. Unità: byte
`MemTotalBytes`	Percentuale di memoria totale attualmente utilizzata dal nastro. Unità: byte
`ReadBytes`	Numero totale di byte letti dalle applicazioni on-premise durante il periodo di reporting per una condivisione file. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Parametro	Descrizione
`UserCpuPercent`	Percentuale di unità di elaborazione della CPU per l'utente allocate attualmente utilizzate dal nastro. Unità: percentuale
`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

Misurazione delle prestazioni tra Tape Gateway e AWS

La velocità di trasmissione effettiva dei dati, la latenza dei dati e le operazioni al secondo sono tre misure che puoi usare per determinare le prestazioni dello storage dell'applicazione che usa il gateway di nastri virtuali. Se usi la statistica di aggregazione corretta, questi valori possono essere misurati tramite i parametri Storage Gateway disponibili.

Una statistica è un'aggregazione di un parametro in un periodo di tempo specificato. Quando visualizzate i valori di una metrica in CloudWatch, utilizzate la `Average` statistica per la latenza dei dati (millisecondi) e utilizzate la `Samples` statistica per le operazioni di input/output al secondo (IOPS). Per ulteriori informazioni, consulta Statistics nella Amazon CloudWatch User Guide.

La tabella seguente contiene un riepilogo dei parametri e delle statistiche corrispondenti che è possibile utilizzare per misurare velocità di trasmissione effettiva, latenza e operazioni di input/output al secondo (IOPS) tra il gateway di nastri virtuali e AWS.

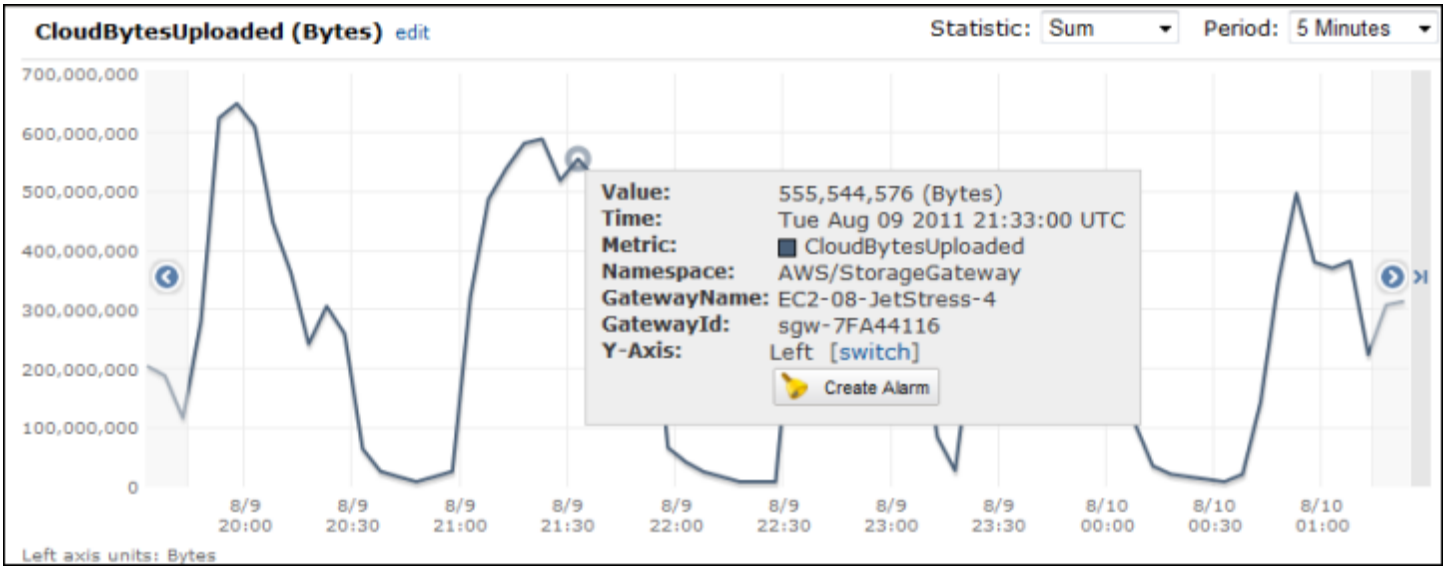
Articolo di interesse	Come misurare
Latenza	Utilizzare i parametri `ReadTime` e `WriteTime` con la statistica `Average` CloudWatch . Ad esempio, il valore `Average` del parametro `ReadTime` restituisce la latenza per ogni operazione in un periodo di tempo campione.

Articolo di interesse	Come misurare
Throughput a AWS	Usa le `CloudBytesUploaded` metriche `CloudBytesDownloaded` and con la `Sum` CloudWatch statistica. Ad esempio, il `Sum` valore della `CloudBytesDownloaded` metrica su un periodo di campionamento di 5 minuti diviso per 300 secondi fornisce la velocità effettiva proveniente dal Tape Gateway espressa in byte AWS al secondo.
Latenza dei dati verso AWS	Utilizzare il parametro `CloudDownloadLatency` con la statistica `Average`. Ad esempio, la statistica `Average` del parametro `CloudDownloadLatency` restituisce la latenza per ogni operazione.

Per misurare la velocità effettiva dei dati di caricamento da un Tape Gateway a AWS

1. Aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Seleziona la scheda Parametri.
3. Scegli la dimensione StorageGateway: Gateway Metrics e trova il Tape Gateway con cui desideri lavorare.
4. Scegliere il parametro `CloudBytesUploaded`.
5. Scegliere un valore per Time Range (Intervallo di tempo).
6. Scegliere la statistica `Sum`.
7. Per Period (Periodo), scegliere un valore maggiore o uguale a 5 minuti.
8. Nel set di punti dati in ordine cronologico risultante, dividere ogni punto dati per il periodo (in secondi) per ottenere la velocità di trasmissione effettiva in corrispondenza del periodo campione.

L'immagine seguente mostra il parametro `CloudBytesUploaded` per un nastro del gateway con la statistica `Sum`. Nell'immagine il posizionamento del cursore su un punto dati permette di visualizzare le informazioni sul punto dati, tra cui il valore e il numero di byte caricati. Dividere questo valore per il valore di Period (Periodo) (5 minuti) per ottenere la velocità di trasmissione effettiva in corrispondenza del punto campione. Per quanto riguarda il punto evidenziato, il throughput dal Tape Gateway a AWS è di 555.544.576 byte diviso per 300 secondi, ovvero 1,7 megabyte al secondo.



Per misurare la latenza dei dati da un Tape Gateway a AWS

1. Aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Seleziona la scheda Parametri.
3. Scegli la GatewayMetrics dimensione StorageGateway: e trova il Tape Gateway con cui desideri lavorare.
4. Scegliere il parametro `CloudDownloadLatency`.
5. Scegliere un valore per Time Range (Intervallo di tempo).
6. Scegliere la statistica `Average`.
7. Per Period (Periodo), selezionare un valore di 5 minuti corrispondente a un tempo di reporting predefinito.

Il set di punti dati in ordine cronologico risultante contiene la latenza in millisecondi.

Per impostare un allarme di soglia superiore per la velocità di trasmissione di un Tape Gateway su AWS

1. Aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegliere Create Alarm (Crea allarme) per avviare la procedura guidata di creazione allarme.
3. Scegli la dimensione StorageGateway: Gateway Metrics e trova il Tape Gateway con cui desideri lavorare.
4. Scegliere il parametro `CloudBytesUploaded`.

5. Definire l'allarme definendo lo stato di allarme quando il parametro `CloudBytesUploaded` è maggiore o uguale a un valore specificato per un determinato periodo di tempo. Ad esempio, è possibile definire uno stato di allarme quando il parametro `CloudBytesUploaded` è maggiore di 10 megabyte per 60 minuti.
6. Configurare le operazioni da eseguire per lo stato di allarme. Ad esempio, è possibile scegliere di ricevere una notifica tramite e-mail.
7. Scegli Crea allarme.

Per impostare un allarme di soglia superiore per la lettura dei dati da AWS

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegliere Create Alarm (Crea allarme) per avviare la procedura guidata di creazione allarme.
3. Scegli la dimensione StorageGateway: Gateway Metrics e trova il Tape Gateway con cui desideri lavorare.
4. Scegliere il parametro `CloudDownloadLatency`.
5. Definire l'allarme definendo lo stato di allarme quando il parametro `CloudDownloadLatency` è maggiore o uguale a un valore specificato per un determinato periodo di tempo. Ad esempio, è possibile definire uno stato di allarme quando il parametro `CloudDownloadLatency` è maggiore di 60.000 millisecondi per più di 2 ore.
6. Configurare le operazioni da eseguire per lo stato di allarme. Ad esempio, è possibile scegliere di ricevere una notifica tramite e-mail.
7. Scegli Crea allarme.

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. Se non è stato creato un gateway, consulta Creazione del gateway.

Argomenti

Spegnimento della macchina virtuale gateway

Potrebbe essere necessario arrestare o riavviare la macchina virtuale per la manutenzione, ad esempio durante l'applicazione di una patch al tuo hypervisor. Prima di spegnere la macchina virtuale, è necessario arrestare il gateway. Per il gateway di 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, è possibile 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.

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

> **Note**
>
> Se arresti il gateway mentre il software di backup scrive su un nastro o legge da esso, l'attività di scrittura o lettura potrebbe generare un errore. Prima di arrestare il gateway, è necessario verificare il software di backup e la pianificazione di backup per ogni attività in corso.

- Console locale della macchina virtuale del gateway: consulta Accedere alla console locale utilizzando credenziali predefinite.
- API Storage Gateway: vedere ShutdownGateway

Per il gateway di file, è sufficiente spegnere la macchina virtuale. Non eseguire lo shutdown del gateway.

Avvio e arresto di un gateway d nastri virtuali

Per arrestare un gateway di nastri virtuali

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere Gateways (Gateway) e quindi selezionare il gateway da arrestare. Lo stato del gateway è Running (In esecuzione).
3. Per Actions (Operazioni), selezionare Stop gateway (Arresta gateway) e verificare l'ID del gateway dalla finestra di dialogo, quindi scegliere Stop gateway (Arresta gateway).

   Durante l'arresto del gateway, è possibile che venga visualizzato un messaggio che indica lo stato del gateway. Quando il gateway viene arrestato, sulla scheda Details (Dettagli) vengono visualizzati un messaggio e un pulsante Start gateway (Avvia gateway).

Quando si arresta il gateway, le risorse di storage non saranno accessibili fino all'avvio dello storage. Se, al momento dell'arresto, il gateway stava caricando dei dati, il caricamento riprenderà al nuovo avvio del gateway.

Per avviare un gateway di nastri virtuali

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione scegliere Gateways (Gateway), quindi selezionare il gateway da avviare. Lo stato del gateway è Shutdown (Arrestato).
3. Scegliere Details (Dettagli) quindi scegliere Start gateway (Avvia gateway).

Gestione dei 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

- Determinazione della quantità di archiviazione su disco locale
- Ottimizzazione delle prestazioni del gateway
- Determinazione delle dimensioni del buffer di caricamento da allocare
- Determinazione delle dimensioni dell'archiviazione della cache da allocare
- Configurazione di un buffer di caricamento e dell'archiviazione della cache

Determinazione della quantità di archiviazione su disco locale

Il numero e la dimensione dei dischi da allocare per il gateway dipende da te. A seconda della soluzione di storage distribuita (consulta Pianifica l'implementazione di Storage Gateway), il gateway richiede lo storage aggiuntivo seguente:

- I gateway di nastri virtuali richiedono almeno due dischi. Uno da usare come cache e uno da usare come buffer di caricamento.

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.

Archiviazione locale	Descrizione
Buffer di caricamento	Il buffer di caricamento fornisce un'area di gestione temporane a per i dati prima che il gateway carichi i dati in Amazon S3. Il tuo gateway carica i dati del buffer in AWS tramite una connessio ne SSL (Secure Sockets Layer) crittografata.
Storage della cache	L'archiviazione della cache funge da archivio on-premise durevole per i dati in attesa di essere caricati in Amazon S3 dal buffer di caricamento. Quando l'applica zione esegue operazioni di I/O in un volume o un nastro, il gateway salva i dati nello storage della cache per permettere l'accesso a bassa latenza. Quando l'applica zione richiede i dati da un volume o un nastro, prima di scaricare i dati da AWS il gateway controlla se sono disponibili nello storage della cache.

Note

Quando effettui il provisioning dei dischi, è consigliabile non effettuare il provisioning di dischi locali per il buffer di caricamento e lo storage della cache se usano la stessa risorsa fisica (lo stesso disco). 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 o buffer di caricamento), puoi scegliere di archiviare il disco virtuale nello stesso datastore della macchina virtuale o in un datastore diverso.

Se hai più di un datastore, è consigliabile scegliere un datastore per lo storage della cache e un altro per il buffer di caricamento. 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 che per il buffer di caricamento. 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 o rimuovendo dischi per un buffer di caricamento. È anche possibile aggiungere dischi per lo storage della cache.

Ottimizzazione delle prestazioni del gateway

Per ottenere prestazioni ottimali, utilizza dischi SSD ad alta velocità di trasmissione effettiva sia per la cache che per il buffer di caricamento

- Utilizza dischi diversi per la cache e il buffer di caricamento. Se utilizzi RAID, assicurati che i dischi del buffer di cache e di upload utilizzino controller RAID separati a livello hardware.
- Aggiungi almeno 2 diversi dischi buffer di caricamento.
- Utilizza una configurazione RAID 0 con striping RAID per i dispositivi cache+buffer di caricamento per migliorare la velocità di trasmissione effettiva. Ciò è particolarmente importante per il disco della cache.

Determinazione delle dimensioni del buffer di caricamento da allocare

È possibile determinare le dimensioni del buffer di caricamento da allocare usando una formula. È consigliabile allocare almeno 150 GiB per il buffer di caricamento. Se la formula restituisce un valore inferiore a 150 GiB, alloca 150 GiB al buffer di caricamento. È possibile configurare fino a 2 TiB di capacità del buffer di caricamento per ogni gateway.

Note

Per i gateway di nastri virtuali, quando il buffer di caricamento raggiunge la capacità, le applicazioni possono continuare a leggere e scrivere i dati nei volumi di storage. Tuttavia, Tape Gateway non scrive alcun dato del volume nel suo buffer di caricamento e non carica nessuno di questi dati AWS fino a quando Storage Gateway non sincronizza i dati archiviati

localmente con la copia dei dati archiviati in. AWS Questa sincronizzazione si verifica quando i volumi si trovano nello stato BOOTSTRAPPING (PROCESSO DI BOOTSTRAP).

Per stimare la quantità di buffer di caricamento da allocare, determina la velocità prevista dei dati in ingresso e in uscita e inserisci i valori nella formula seguente.

Velocità dei dati in ingresso

Questa velocità si riferisce al throughput dell'applicazione e indica la velocità con cui le applicazioni locali scrivono i dati nel gateway in un determinato periodo di tempo.

Velocità dei dati in uscita

Questa velocità di riferisce al throughput di rete ed è la velocità con cui il gateway è in grado di caricare i dati in AWS. Questa velocità dipende dalla velocità di rete, dall'utilizzo e dall'attivazione del throttling della larghezza di banda. Questa velocità deve essere regolata in base alla compressione. Durante il caricamento dei dati su AWS, il gateway applica la compressione dei dati laddove possibile. Se, ad esempio, i dati dell'applicazione sono di solo testo, si può ottenere un rapporto di compressione effettivo di circa 2:1. Se tuttavia vengono scritti video, il gateway potrebbe non essere in grado di ottenere la compressione dei dati e potrebbe essere necessario un buffer di caricamento maggiore per il gateway.

Si consiglia di allocare almeno 150 GiB di spazio buffer di caricamento se si verifica una delle seguenti condizioni:

- La tariffa in entrata è superiore alla tariffa in uscita.
- La formula restituisce un valore inferiore a 150 GiB.

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor}\right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

Ad esempio, supponiamo che le applicazioni aziendali scrivano dati di testo nel gateway a una velocità di 40 MB al secondo per 12 ore al giorno e il throughput di rete sia pari a 12 MB al secondo. Considerando un fattore di compressione di 2:1 per i dati di testo, sarebbe necessario allocare circa 690 GiB di spazio del buffer di caricamento.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

Inizialmente puoi usare questa approssimazione per determinare le dimensioni del disco da allocare al gateway come spazio del buffer di caricamento. Per aggiungere altro spazio del buffer di caricamento, puoi usare la console Storage Gateway. Inoltre, puoi utilizzare i parametri CloudWatch operativi di Amazon per monitorare l'utilizzo del buffer di caricamento e determinare requisiti di storage aggiuntivi. Per informazioni sui parametri e sull'impostazione di allarmi, consulta Monitoraggio del buffer di caricamento.

Determinazione delle dimensioni dell'archiviazione della cache da allocare

Il gateway usa lo storage della cache per fornire accesso a bassa latenza ai dati usati di recente. L'archiviazione della cache funge da archivio on-premise durevole per i dati in attesa di essere caricati in Amazon S3 dal buffer di caricamento. In genere, le dimensioni dello storage della cache devono corrispondere a quelle del buffer di caricamento moltiplicate per 1,1. Per ulteriori informazioni su come stimare le dimensioni dello storage della cache, consulta Determinazione delle dimensioni del buffer di caricamento da allocare.

Inizialmente, puoi usare questa approssimazione per effettuare il provisioning dei dischi per lo storage della cache. Puoi quindi utilizzare i parametri CloudWatch operativi di Amazon per monitorare l'utilizzo dello storage della cache e fornire più spazio di archiviazione in base alle esigenze utilizzando la console. Per informazioni sull'uso dei parametri e sull'impostazione di allarmi, consulta Monitoraggio dello storage della cache.

Configurazione di un buffer di caricamento e dell'archiviazione della cache

Quando i requisiti della tua applicazione cambiano, puoi aumentare la capacità del buffer di caricamento o dello storage della cache. È possibile aggiungere capacità di archiviazione al gateway senza interrompere la funzionalità o causare tempi di inattività. Quando aggiungi ulteriore spazio di archiviazione, esegui l'operazione con la macchina virtuale del gateway attivata.

> **Important**
>
> Quando aggiungi la cache o il buffer di caricamento a un gateway esistente, devi creare nuovi dischi nell'hypervisor del gateway host o nell'istanza Amazon EC2. Non rimuovere o

modificare le dimensioni dei dischi esistenti che sono già stati allocati come cache o buffer di caricamento.

Per configurare un buffer di caricamento o l'archiviazione della cache per il gateway

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

Gestione della larghezza di banda per il gateway di nastri virtuali

Puoi limitare (o limitare) la velocità effettiva di upload dal gateway verso AWS o la velocità effettiva di download dal AWS gateway. L'uso del throttling della larghezza di banda permette di controllare la quantità di larghezza di banda di rete usata dal gateway. Per impostazione predefinita, un gateway attivato non ha limiti di velocità di caricamento o download.

È possibile specificare il limite di velocità utilizzando o a livello di codice utilizzando l' AWS Management Console API Storage Gateway (vedere UpdateBandwidthRateLimit) o un AWS Software Development Kit (SDK). Se si esegue la limitazione della larghezza di banda a livello di programmazione, è possibile modificare i limiti automaticamente durante il giorno, ad esempio pianificando attività per la modifica della larghezza di banda.

È inoltre possibile definire una limitazione della larghezza di banda basata su una pianificazione per il gateway. È possibile pianificare la limitazione della larghezza di banda definendo uno o più intervalli. bandwidth-rate-limit Per ulteriori informazioni, consulta Limitazione della larghezza di banda basata sulla pianificazione tramite la console Storage Gateway.

La configurazione di un'unica impostazione per la limitazione della larghezza di banda è l'equivalente funzionale della definizione di una pianificazione con un unico bandwidth-rate-limit intervallo impostato per Tutti i giorni, con un'ora di inizio e un'ora di fine di. **`00:00`** `23:59`

> **Note**
>
> Le informazioni contenute in questa sezione sono specifiche per i gateway di nastri virtuali e di volumi. Per gestire la larghezza di banda per un gateway di file Amazon S3, consulta Gestione della larghezza di banda per il gateway di file Amazon S3. I limiti di velocità di larghezza di banda non sono attualmente supportati per il gateway di file Amazon FSx.

Argomenti

- Per modificare la limitazione della larghezza di banda usando la console Storage Gateway
- Limitazione della larghezza di banda basata sulla pianificazione tramite la console Storage Gateway
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK for Java
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK for .NET
- Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Per modificare la limitazione della larghezza di banda usando la console Storage Gateway

La procedura seguente illustra come modificare la limitazione della larghezza di banda di un gateway usando la console Storage Gateway.

Per modificare il throttling della larghezza di banda di un gateway usando la console

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione di sinistra, scegliere Gateway e quindi scegliere il gateway da gestire.
3. Per Operazioni, scegliere Modifica limite di larghezza di banda.
4. Nella finestra di dialogo Modifica limiti velocità digitare nuovi valori per i limiti e quindi scegliere Salva. Le modifiche verranno visualizzate nella scheda Details (Dettagli) del gateway.

Limitazione della larghezza di banda basata sulla pianificazione tramite la console Storage Gateway

La procedura seguente illustra come pianificare modifiche nella limitazione della larghezza di banda di un gateway usando la console Storage Gateway.

Per aggiungere o modificare una pianificazione per la limitazione della larghezza di banda del gateway

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione di sinistra, scegliere Gateway e quindi scegliere il gateway da gestire.
3. Per Operazioni, scegliere Modifica pianificazione del limite di velocità di larghezza di banda.

   La bandwidth-rate-limit pianificazione del gateway viene visualizzata nella finestra di dialogo Modifica pianificazione del limite di velocità di larghezza di banda. Per impostazione predefinita, una nuova bandwidth-rate-limit pianificazione del gateway è vuota.
4. Nella finestra di dialogo Modifica pianificazione del limite di velocità di larghezza di banda, scegli Aggiungi nuovo elemento per aggiungere un nuovo bandwidth-rate-limit intervallo. Inserisci le seguenti informazioni per ogni bandwidth-rate-limit intervallo:

   - Giorni della settimana: puoi creare l' bandwidth-rate-limit intervallo per i giorni feriali (dal lunedì al venerdì), per i fine settimana (sabato e domenica), per tutti i giorni della settimana o per uno o più giorni specifici della settimana.

- Ora di inizio: immettere l'ora di inizio dell'intervallo di larghezza di banda nel fuso orario locale del gateway, utilizzando il formato HH:MM.

  > **Note**
  >
  > L' bandwidth-rate-limit intervallo inizia all'inizio del minuto specificato qui.

- Ora di fine: immettere l'ora di fine dell' bandwidth-rate-limit intervallo nel fuso orario locale del gateway, utilizzando il formato HH:MM.

  > **Important**
  >
  > L' bandwidth-rate-limit intervallo termina alla fine del minuto specificato qui. Per pianificare un intervallo che termini alla fine di un'ora, immettere. **`59`**
  > Per programmare intervalli continui consecutivi, con transizione all'inizio dell'ora, senza interruzioni tra gli intervalli, inserite **`59`** il minuto finale del primo intervallo. Immettete **`00`** il minuto di inizio dell'intervallo successivo.

- Velocità di download: inserisci il limite di velocità di download, in kilobit al secondo (Kbps), oppure seleziona Nessun limite per disattivare la limitazione della larghezza di banda per il download. Il valore minimo per la velocità di download è 100 Kbps.
- Velocità di caricamento: inserisci il limite di velocità di caricamento, in Kbps, o seleziona Nessun limite per disattivare la limitazione della larghezza di banda per il caricamento. Il valore minimo per la velocità di caricamento è 50 Kbps.

Per modificare bandwidth-rate-limit gli intervalli, è possibile inserire valori modificati per i parametri degli intervalli.

Per rimuovere gli bandwidth-rate-limit intervalli, puoi scegliere Rimuovi a destra dell'intervallo da eliminare.

Dopo aver completato le modifiche, scegli Salva.

5. Continua ad aggiungere bandwidth-rate-limit intervalli scegliendo Aggiungi nuovo elemento e inserendo il giorno, l'ora di inizio e di fine e i limiti di velocità di download e upload.

> **Important**
>
> andwidth-rate-limit Gli intervalli B non possono sovrapporsi. L'ora di inizio di un intervallo deve essere successiva all'ora di fine di un intervallo precedente, e precedente all'ora di inizio di un intervallo successivo.

6. Dopo aver inserito tutti gli bandwidth-rate-limit intervalli, scegli Salva modifiche per salvare la pianificazione. bandwidth-rate-limit

Quando la bandwidth-rate-limit pianificazione viene aggiornata correttamente, puoi visualizzare i limiti correnti di velocità di download e upload nel pannello Dettagli del gateway.

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK for Java

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare i 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 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 di larghezza di banda del gateway mediante AWS SDK for Java

L'esempio di codice Java seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per utilizzare questo codice di esempio, è necessario fornire l'endpoint del servizio, il nome della risorsa Amazon (ARN) del gateway e i limiti di download e caricamento. Per un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere AWS Storage Gateway Endpoints and Quotas nel. Riferimenti generali di AWS

```
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.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;
```

```
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 = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

    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, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
```

```
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
            System.out.println("Download bandwidth limit = " + downloadRate + " bits
 per second");
        }
        catch (AmazonClientException ex)
        {
            System.err.println("Error updating gateway bandwith.\n" + ex.toString());
        }
    }
}
```

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS SDK for .NET

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare i 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 AWS SDK for .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 di larghezza di banda del gateway utilizzando AWS SDK for .NET

L'esempio di codice C# seguente aggiorna i limiti di velocità della larghezza di banda di un gateway. Per utilizzare questo codice di esempio, è necessario fornire l'endpoint del servizio, il nome della risorsa Amazon (ARN) del gateway e i limiti di download e caricamento. Per un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere AWS Storage Gateway Endpoints and Quotas nel. Riferimenti generali di AWS

```
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 = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
```

```
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Se aggiorni i limiti di velocità della larghezza di banda a livello di programmazione, puoi modificare i 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 AWS Tools for Windows PowerShell. Per utilizzare il codice di esempio, è necessario avere dimestichezza con l'esecuzione di uno PowerShell script. Per ulteriori informazioni, consulta Nozioni di base nella Guida per l'utente di AWS Tools for Windows PowerShell .

Example : Aggiornamento dei limiti di velocità di larghezza di banda del gateway utilizzando il AWS Tools for Windows PowerShell

Il seguente esempio di PowerShell script aggiorna i limiti di velocità di larghezza di banda di un gateway. Per utilizzare questo script di esempio, è necessario fornire il nome della risorsa Amazon (ARN) del gateway e i limiti di download e caricamento.

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

.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 = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

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 Console di gestione Storage Gateway, altrimenti attendi che gli aggiornamenti vengano applicati automaticamente durante il periodo di manutenzione configurato. Anche se Storage Gateway verifica la presenza di aggiornamenti ogni minuto, esegue la manutenzione e il riavvio solo se sono presenti nuovi aggiornamenti.

Le versioni del software del gateway includeranno regolarmente aggiornamenti del sistema operativo e patch di sicurezza che sono state convalidate da AWS. Questi aggiornamenti vengono rilasciati in genere ogni sei mesi e vengono applicati come parte del normale processo di aggiornamento del gateway durante le finestre di manutenzione programmate.

> **Note**
>
> Devi trattare l'appliance Storage Gateway come una macchina virtuale gestita e non devi tentare di accedere o modificare la sua installazione in alcun modo. Il tentativo di installare

o aggiornare qualsiasi pacchetto software utilizzando metodi diversi rispetto al normale meccanismo di aggiornamento del gateway (ad esempio, strumenti SSM o Hypervisor) può compromettere il corretto funzionamento del gateway.
Per modificare l'indirizzo e-mail a cui vengono inviate le notifiche di aggiornamento software, vai alla pagina Gestione di un AWS account e aggiorna il contatto alternativo per «operazioni».

Prima di applicare qualsiasi aggiornamento al gateway, ti AWS avvisa con un messaggio sulla console di Storage Gateway e sul tuo AWS Health Dashboard. Per ulteriori informazioni, consulta 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).

Important

Puoi ridurre al minimo le probabilità di interruzione delle applicazioni a causa del riavvio del gateway aumentando i timeout dell'iniziatore iSCSI. Per ulteriori informazioni sull'aumento dei timeout dell'iniziatore iSCSI per Windows e Linux, consulta Personalizzazione delle impostazioni iSCSI di Windows e Personalizzazione delle impostazioni iSCSI di Linux.

Per modificare la pianificazione di manutenzione

1. Apri la console Storage Gateway all'indirizzo https://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 è selezionato 28, il giorno di inizio della manutenzione sarà il 28 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.

Esecuzione delle operazioni sulla console locale della VM di

Per un gateway 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 host VMware, Hyper-V e KVM (Linux Kernel-based Virtual Machine).

Argomenti

- Accedere alla console locale utilizzando credenziali predefinite
- Impostazione della password della console locale dalla console Storage Gateway
- Instradamento del gateway in locale tramite un proxy
- Configurazione di rete del gateway
- Verifica della connessione del gateway a Internet

- Sincronizzazione dell'ora della VM associata al gateway
- Esecuzione di comandi Storage Gateway sulla console locale
- Visualizzazione dello stato relativo alle risorse di sistema del gateway
- Configurazione delle schede di rete per il gateway

Accedere alla console locale utilizzando credenziali predefinite

Quando la VM è pronta per l'accesso, è visualizzata la schermata di autenticazione. Per il primo accesso alla console locale, utilizzare le credenziali predefinite per accedere. 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. Storage Gateway consente di impostare la propria password dalla AWS Storage Gateway console anziché modificare la password dalla console locale. Non è necessario conoscere la password predefinita per impostarne una nuova. Per ulteriori informazioni, consulta Impostazione della password della console locale dalla console Storage Gateway.

Come accedere alla console locale del gateway

1. 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**
   >
   > Si consiglia di modificare la password predefinita inserendo il numero corrispondente per Console del gateway dal menu principale Attivazione dell'appliance AWS : configurazione, eseguendo poi il comando `passwd`. Per informazioni su come eseguire il comando, consulta Esecuzione di comandi Storage Gateway sulla console locale. È inoltre possibile impostare la propria password dalla AWS Storage Gateway console. Per ulteriori informazioni, consulta Impostazione della password della console locale dalla console Storage Gateway.

> **Important**
>
> Per le versioni precedenti del gateway di volumi o di nastri virtuali, il nome utente è `sguser` e la password è `sgpassword`. Se si reimposta la password e il gateway viene aggiornato a una versione più recente, il nome utente verrà modificato in admin ma la password verrà mantenuta.

2. Dopo aver effettuato l'accesso, viene visualizzato il menu principale Configurazione di AWS Storage Gateway, dal quale è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurare un proxy SOCKS per il gateway	Instradamento del gateway in locale tramite un proxy.
Configurare la rete	Configurazione di rete del gateway.
Verificare la connettività di rete	Verifica della connessione del gateway a Internet.
Gestione dell'ora della VM	Sincronizzazione dell'ora della VM associata al gateway.
Esecuzione dei comandi della console Storage Gateway	Esecuzione di comandi Storage Gateway sulla console locale.
Visualizzare lo stato delle risorse di sistema	Visualizzazione dello stato relativo alle risorse di sistema del gateway.

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

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

Impostazione della password della console locale dalla console Storage Gateway

Per il primo accesso alla console locale, accedere alla VM con le credenziali predefinite: 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. Apri la console Storage Gateway all'indirizzo https://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 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.

Instradamento del gateway in locale tramite un proxy

I gateway di volumi e di nastri virtuali supportano la configurazione di un proxy Socket Secure versione 5 (SOCKS5) tra AWS e il gateway on-premise.

> **Note**
>
> L'unica configurazione proxy supportata è SOCKS5.

Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy SOCKS 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 tutto il traffico tramite il server proxy. Per informazioni sui requisiti di rete del gateway, consulta Requisiti di rete e firewall.

La procedura seguente illustra come configurare un proxy SOCKS per un gateway di volumi e un gateway di nastri virtuali.

Per configurare un proxy SOCKS5 per gateway di volumi e di nastri virtuali

1. Accedere alla console locale del gateway.
   - VMware ESXi: per ulteriori informazioni, consulta Accesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.
   - KVM: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale AWS Storage Gateway: configurazione, immettere il numero corrispondente per selezionare Configurazione proxy SOCKS.
3. Dal menu Configurazione del proxy SOCKS per AWS Storage Gateway, immettere il numero corrispondente per eseguire una delle seguenti attività:

Per eseguire questa attività	eseguire questa operazione
Configurare un proxy SOCKS	Immettere il numero corrispondente per selezionare Configura proxy SOCKS. Specificare un nome host e una porta per completare la configurazione.
Visualizzare l'attuale configurazione del proxy SOCKS	Immettere il numero corrispondente per selezionare Visualizza configurazione proxy SOCKS corrente. Se il proxy SOCKS non è configurato, viene visualizzato il messaggio `SOCKS Proxy not configured` . In caso contrario, vengono visualizzati il nome host e la porta del proxy.

Per eseguire questa attività	eseguire questa operazione
Rimuovere la configurazione di un proxy SOCKS	Immettere il numero corrispondente per selezionare Rimuovi configurazione proxy SOCKS. Viene visualizzato il messaggio `SOCKS Proxy Configuration Removed`

4. Per applicare la configurazione HTTP, riavviare la VM.

Configurazione di rete del gateway

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

Per configurare il gateway affinché utilizzi indirizzi IP statici

1. Accedere alla console locale del gateway.
   - VMware ESXi: per ulteriori informazioni, consulta Accesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.
   - KVM: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale AWS Storage Gateway: configurazione, immettere il numero corrispondente per selezionare Configurazione di rete.
3. Dal menu Configurazione di rete per AWS Storage Gateway, eseguire una delle seguenti attività:

Per eseguire questa attività	eseguire questa operazione
Descrivere la scheda di rete	Immettere il numero corrispondente per selezionare Descrivi scheda.

Per eseguire questa attività	eseguire questa operazione
	Viene visualizzato un elenco di nomi di schede e viene richiesto di digitare 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 attivato I nomi delle schede elencate qui vengono utilizzati quando si configura un indirizzo IP statico o si imposta la scheda predefinita del gateway.
Configurazione di DHCP	Immettere il numero corrispondente per selezionare Configura DHCP. Per l'utilizzo di DHCP, viene richiesto di configurare un'interfaccia di rete.

Per eseguire questa attività	eseguire questa operazione
Configurare un indirizzo IP statico per il gateway	Immettere il numero corrispondente per selezionare Configura IP statico. 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, consulta Spegnimento della macchina virtuale gateway.

Per eseguire questa attività	eseguire questa operazione
	Se il gateway utilizza più di un'interfaccia di rete, è necessario impostare tutte le interfacc e attivate 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 disattivata. Per riattivarla, sarà necessario configurarla con un indirizzo IP statico. Se entrambe le interfacce sono inizialmente configurate per l'utilizzo di indirizzi IP statici e poi si imposta il gateway in modo che si avvalga di DHCP, entrambe le interfacce, infine, utilizzeranno DHCP.
Configura un nome host per il gateway	Immettere il numero corrispondente per selezionare Configura nome host. Ti viene richiesto di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o ne acquisirà uno automaticamente tramite DCHP o rDNS. **Note** Se configuri un nome host statico per il gateway, devi creare un record A nel sistema DNS che punti l'indirizzo IP del gateway al relativo nome host statico.

Per eseguire questa attività	eseguire questa operazione
Reimpostare tutte le configurazioni di rete del gateway su DHCP	Immettere il numero corrispondente per selezionare Reimposta tutto su DHCP. Tutte le interfacce di rete sono impostate per l'utilizzo di DHCP. **Important** Se il gateway è già stato attivato, affinché le impostazioni abbiano effetto è necessario arrestare il gateway stesso e riavviarlo dalla console Storage Gateway. Per ulteriori informazioni, consulta Spegnimento della macchina virtuale gateway.
Impostare l'adattatore di routing predefinito del gateway	Immettere il numero corrispondente per selezionare Imposta scheda predefinita. Compaiono le schede disponibili per il gateway e viene richiesto di selezionarne una, ad esempio **`eth0`**.
Visualizzare la configurazione DNS del gateway	Immettere il numero corrispondente per selezionare Visualizza configurazione DNS. Vengono visualizzati gli indirizzi IP dei server di nomi DNS primario e secondario.

Per eseguire questa attività	eseguire questa operazione
Visualizzare le tabelle di routing	Immettere il numero corrispondente per selezionare Visualizza le route. Viene visualizzato l'instradamento predefinito del gateway.

Verifica della connessione del gateway a Internet

Avvalendoti della console locale del gateway, puoi testare la connessione a Internet. Questo test può essere utile per risolvere eventuali problemi di rete del gateway.

Per testare la connessione del gateway a Internet

1. Accedere alla console locale del gateway.
   - VMware ESXi: per ulteriori informazioni, consulta Accesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.
   - KVM: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale AWS Storage Gateway: configurazione, immettere il numero corrispondente per selezionare Testa connettività di rete.

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

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

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

Sincronizzazione dell'ora della VM associata al gateway

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, consulta 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, consulta Sincronizzazione dell'ora della VM associata al gateway.

Esecuzione di comandi Storage Gateway sulla console locale

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

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. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Console del gateway.
3. Dal prompt dei comandi della console del gateway, immettere **h**.

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

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, consulta Configurazione della rete del gateway.
ip	Mostra/manipola routing, dispositivi e tunnel.

Comando	Funzione
	Note Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, consulta Configurazione della rete del gateway.
iptables	Strumento di amministrazione per il filtraggio dei pacchetti IPv4 e NAT.
ncport	Testa la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support.
passwd	Aggiorna i token di autenticazione.
save-iptables	Tabelle IP persistenti.
save-routing-table	Salva la voce della tabella di routing appena aggiunta.
tcptraceroute	Raccogli l'output da traceroute sul traffico TCP verso una destinazione.

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

Per informazioni su un comando, immetere **`man`** + *`nome del comando`* nel prompt di comando.

Visualizzazione dello stato relativo alle risorse di sistema del gateway

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

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla 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. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

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

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

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

Configurazione 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 in modo che sia accessibile 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'uso 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.

> **Important**
>
> Per selezionare VMXNET3, il sistema operativo guest deve essere di tipo Other Linux64 (Altro Linux64).

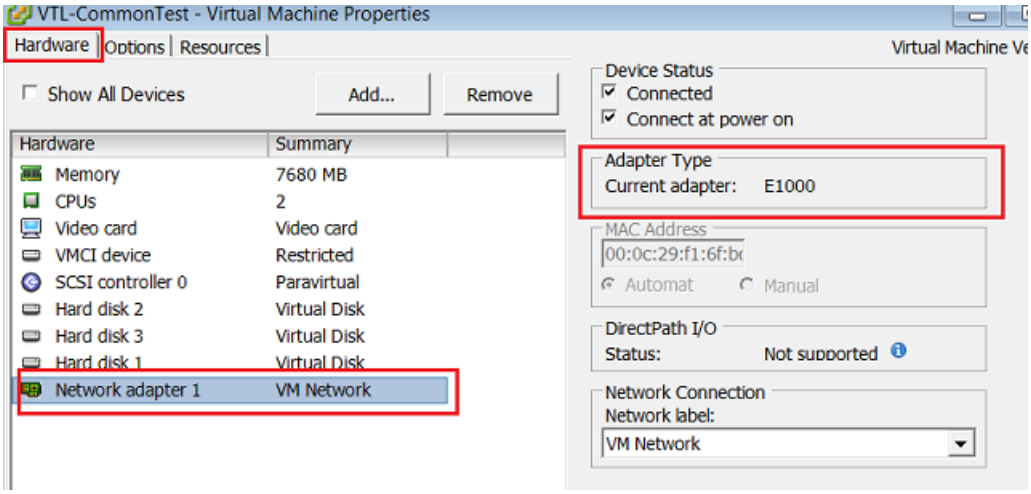
Passaggi necessari per configurare il gateway affinché utilizzi la scheda VMXNET3:

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 Type (Tipo di scheda) è riportata l'attuale scheda E1000, che può 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 Type (Tipo di scheda), quindi selezionare Next (Avanti).

8. Nel corso della procedura guidata dedicata alle proprietà della macchina virtuale, verificare che nella sezione Adapter Type (Tipo di scheda) il parametro Current Adapter (Scheda attuale) sia impostato su VMXNET3, quindi selezionare 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 informazioni su come accedere utilizzando le credenziali predefinite, consulta Accesso alla console locale utilizzando le credenziali predefinite.
2. Quando richiesto, immettere il numero corrispondente per selezionare Configurazione di rete.
3. Quando richiesto, digitare il numero corrispondente per selezionare Reimposta tutto su DHCP, quindi digitare **y** (ossia, sì) al prompt successivo affinché tutte le schede utilizzino il protocollo di configurazione per host dinamico (DHCP). Tutte le schede disponibili sono impostate per l'utilizzo di DHCP.

   Se il gateway è già stato attivato, occorre arrestarlo e riavviarlo dalla console di gestione di Storage Gateway. 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 connessione del gateway a Internet.

Configurazione del gateway per più NIC

Se configuri il gateway per l'uso di più schede di rete (NIC), puoi accedervi da più di un indirizzo IP. Tale condizione torna utile nei seguenti casi:

- Massimizzazione del throughput: è possibile massimizzare il throughput di un gateway quando le schede di rete rappresentano un ostacolo.
- Separazione delle applicazioni: potrebbe essere necessario distinguere le modalità di scrittura delle applicazioni sui volumi di un gateway. Potresti, ad esempio, scegliere di far utilizzare a un'applicazione critica di storage una scheda apposita per il tuo gateway.

- Vincoli di rete: l'ambiente applicativo potrebbe richiedere l'inclusione delle destinazioni iSCSI e degli iniziatori collegati in una rete isolata, diversa da quella con cui il gateway comunica con AWS.

In un tipico caso di utilizzo con più adattatori, un adattatore viene configurato come route con cui il gateway comunica AWS (ovvero come gateway predefinito). A eccezione di quest'unica rete, gli iniziatori devono trovarsi nella stessa sottorete della scheda che contiene le destinazioni iSCSI a cui si connettono, per non compromettere la comunicazione con le destinazioni programmate. Se una destinazione è configurata sullo stesso adattatore con cui viene utilizzata la comunicazione AWS, il traffico iSCSI per quella destinazione e il AWS traffico fluiranno attraverso lo stesso adattatore.

Se configuri una scheda per la connessione alla console di Storage Gateway e poi aggiungi un'altra scheda, Storage Gateway elabora automaticamente una tabella di routing per utilizzare la seconda come scheda di instradamento preferita. Per istruzioni su come configurare più schede, consulta le sezioni seguenti.

- Configurazione del gateway per più NIC in un host VMware ESXi
- Configurazione del gateway per più NIC nell'host Microsoft Hyper-V

Esecuzione delle operazioni sulla console locale Amazon EC2

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

Argomenti

- Accesso alla console locale del gateway Amazon EC2
- Instradamento del gateway distribuito in EC2 tramite un proxy HTTP
- Test della connettività di rete del gateway
- Visualizzazione dello stato relativo alle risorse di sistema del 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, consulta la pagina relativa alla connessione all'istanza nella Guida 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, consulta Coppie di chiavi Amazon EC2 nella Guida per l'utente di Amazon EC2.

Accedere alla console locale del gateway

1. Accedere alla tua console locale. Se ci si connette all'istanza EC2 da un computer Windows, accedere come amministratore.
2. Dopo aver effettuato l'accesso, viene visualizzato il menu principale AWS Storage Gateway: configurazione, dal quale è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurare un proxy SOCKS per il gateway	Instradamento del gateway distribuito in EC2 tramite un proxy HTTP
Verificare la connettività di rete	Test della connettività di rete del gateway
Esecuzione dei comandi della console Storage Gateway	Esecuzione di comandi Storage Gateway sulla console locale
Visualizzare un controllo delle risorse di sistema	Visualizzazione dello stato relativo alle risorse di sistema del gateway.

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

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

Instradamento del gateway distribuito in EC2 tramite un proxy HTTP

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

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

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

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

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

Test della connettività di rete del gateway

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

Per testare la connettività di rete del gateway

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

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

degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere AWS Storage Gateway endpoint e quote nel. Riferimenti generali di AWS

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

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

Visualizzazione dello stato relativo alle risorse di sistema del gateway

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

Per visualizzare lo stato di un controllo delle risorse di sistema

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

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

Messaggio	Descrizione
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti raccomand ati, ma il gateway può continuare a funzionar

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

Per eseguire un comando di diagnostica o di configurazione

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

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

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.

Comando	Funzione
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata.
ip	Mostra/manipola routing, dispositivi e tunnel. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata.
iptables	Strumento di amministrazione per il filtraggio dei pacchetti IPv4 e NAT.
ncport	Testa la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support.
save-iptables	Tabelle IP persistenti.
save-routing-table	Salva la voce della tabella di routing appena aggiunta.

Comando	Funzione
sslcheck	Verifica la validità SSL per la risoluzione dei problemi di rete.
tcptraceroute	Raccogli l'output da traceroute sul traffico TCP verso una destinazione.

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

Per informazioni su un comando, inserisci il nome del comando seguito dall'opzione `-h`, ad esempio: `sslcheck -h`.

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

Accesso alla console locale del gateway con Linux KVM

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

Per accedere alla console locale del gateway con KVM

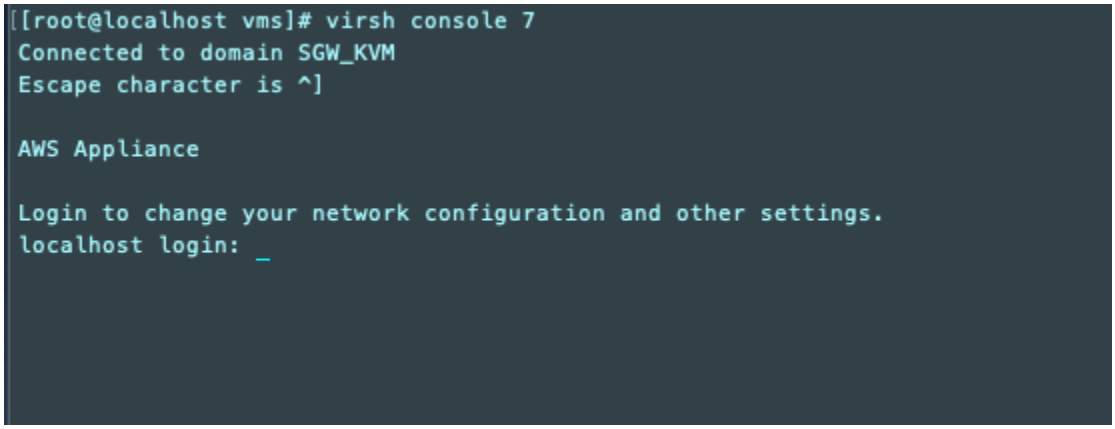
1. Utilizzare il comando seguente per elencare le macchine virtuali attualmente disponibili in KVM.

```
# virsh list
```

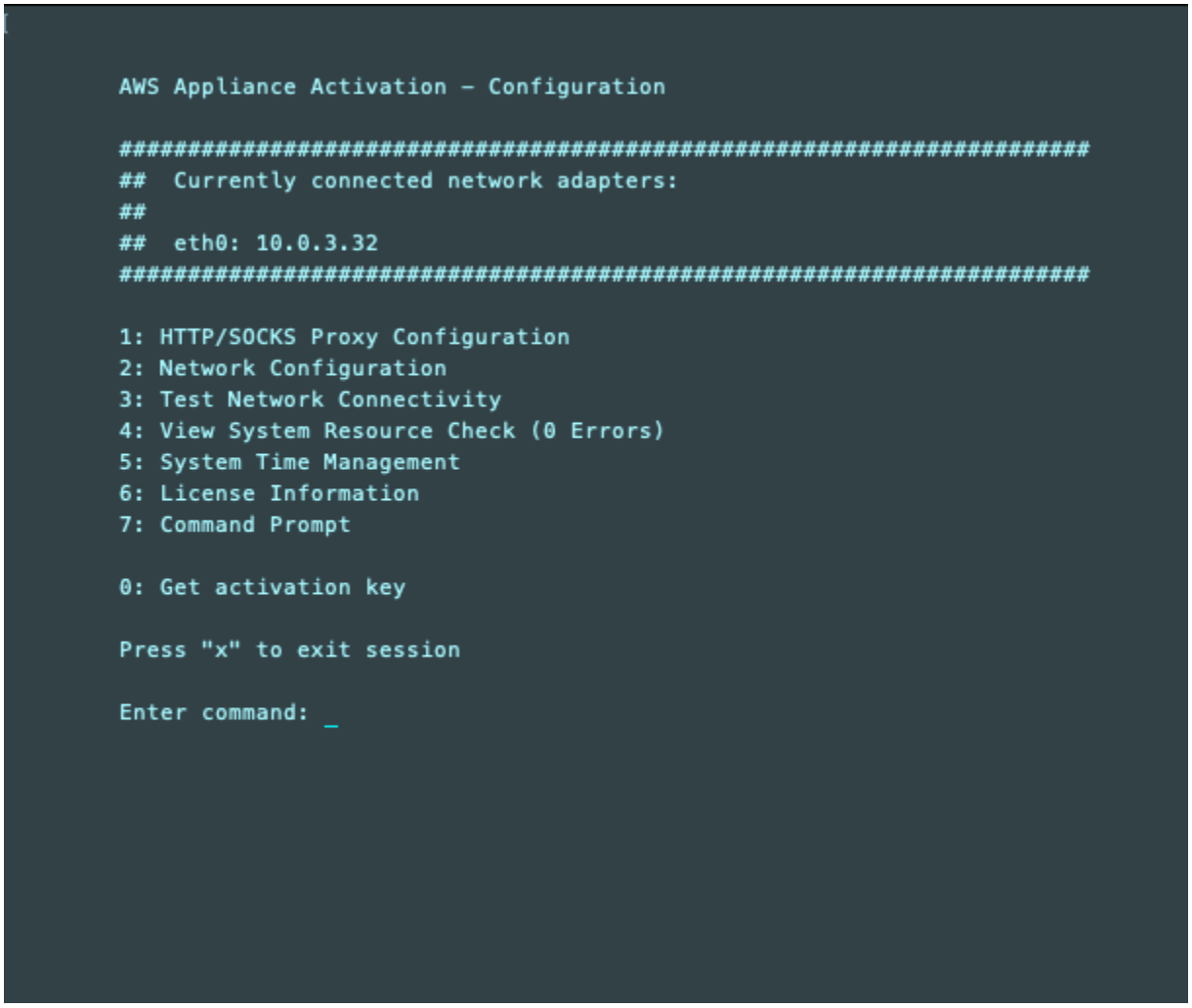
È possibile scegliere le macchine virtuali disponibili per `Id`.

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

```
# virsh console VM_Id
```



3. Per ottenere le credenziali predefinite per accedere alla console locale, consulta Accedere alla console locale utilizzando credenziali predefinite.
4. Dopo aver effettuato l'accesso, è possibile attivare e configurare il gateway.

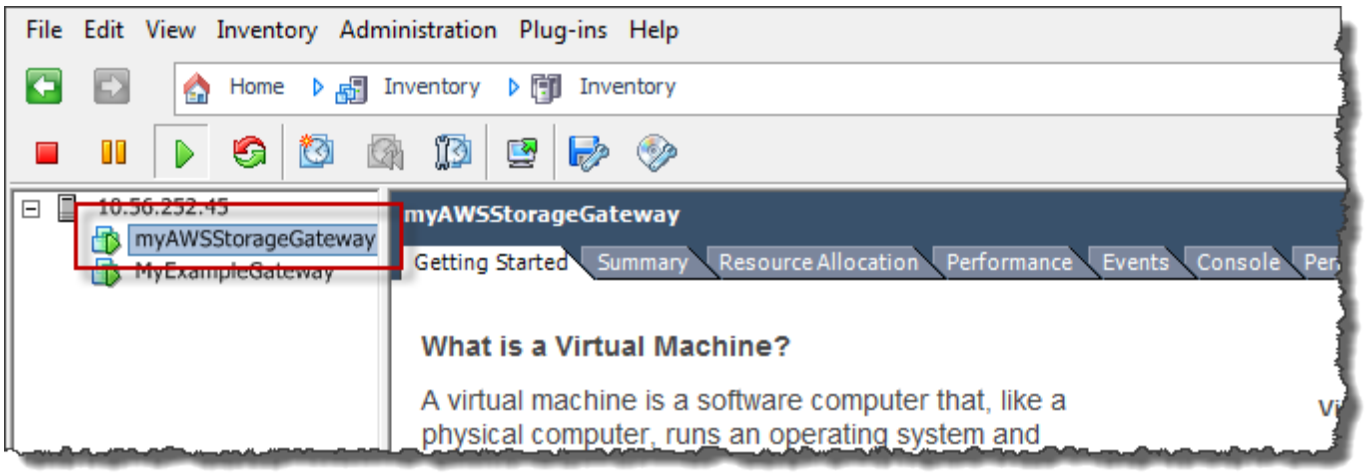


Accesso alla console locale del gateway con VMware ESXi

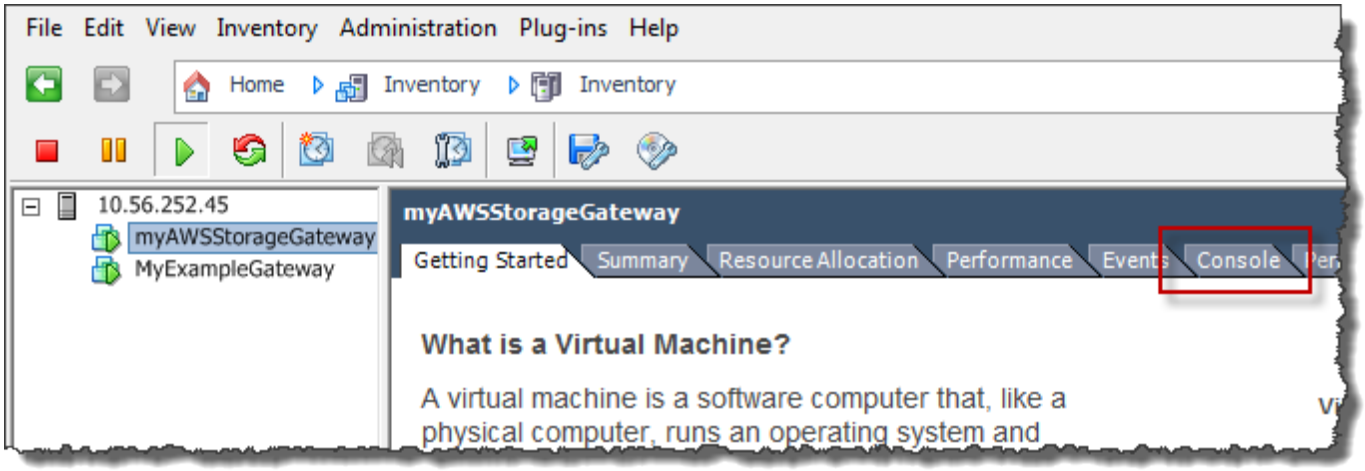
Per accedere alla console locale del gateway con VMware ESXi

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).

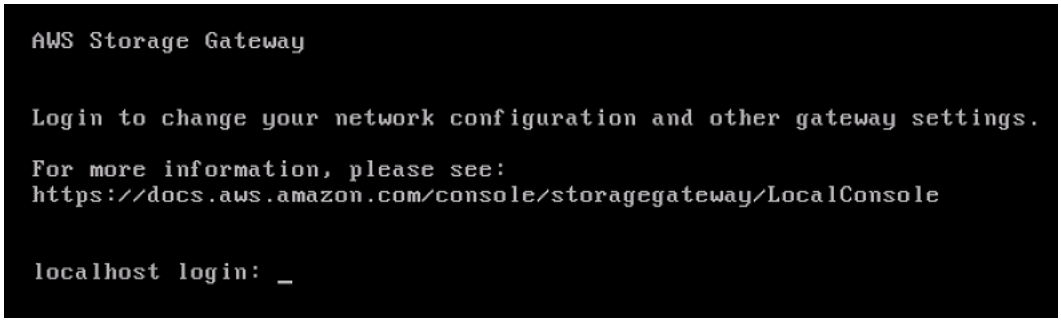


3. Scegli la scheda Console.



Dopo alcuni istanti, la macchina virtuale è pronta per l'accesso.

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



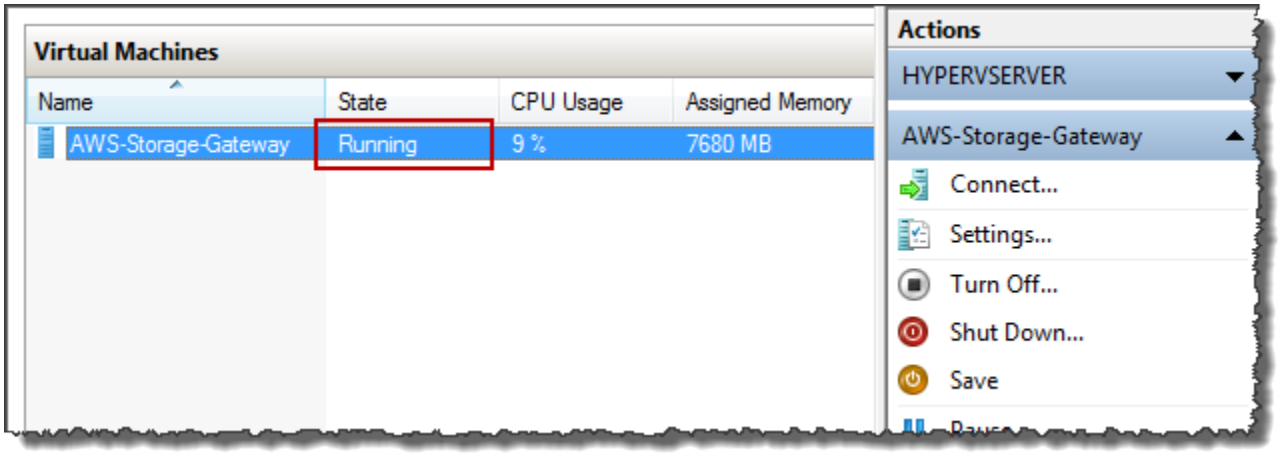
4. Per accedere tramite le credenziali predefinite, continua con la procedura Accedere alla console locale utilizzando credenziali predefinite.

Accesso alla console locale del gateway con Microsoft Hyper-V

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

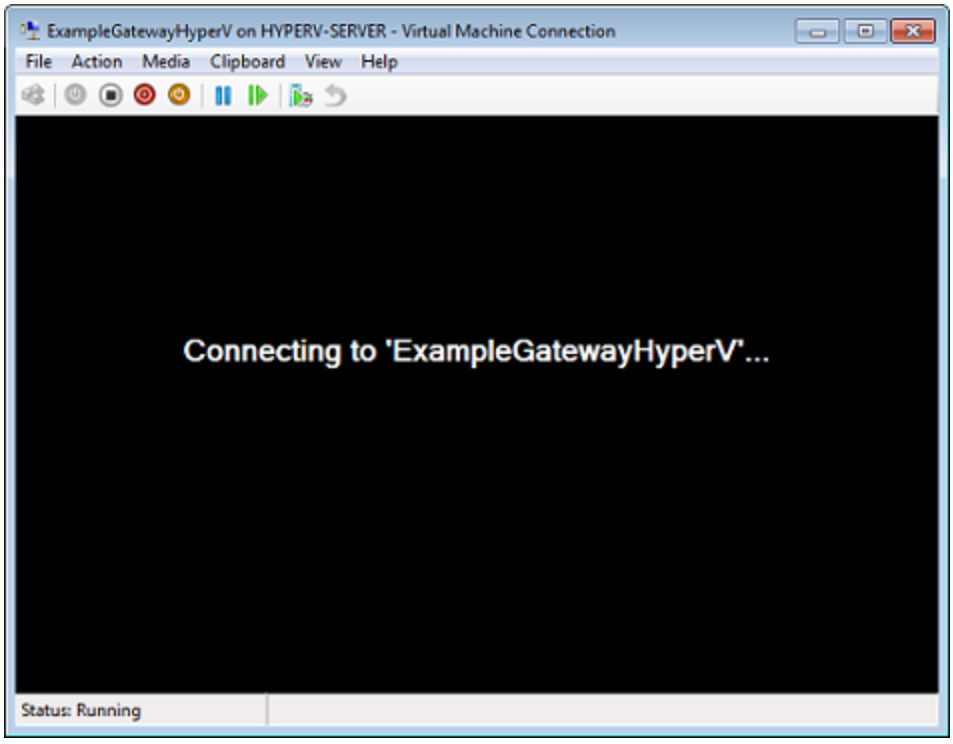
1. Nell'elenco Virtual Machines (Macchine virtuali) di Microsoft Hyper-V Manager, selezionare la macchina virtuale del gateway.
2. Verifica che il gateway sia attivo.

> **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).

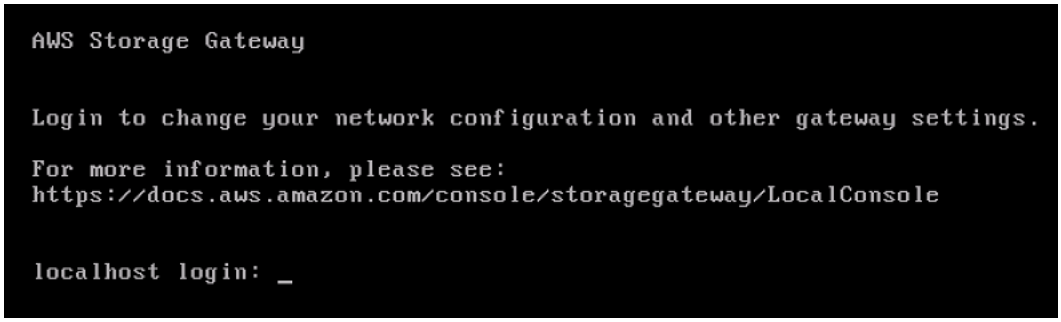


3. Nel riquadro Actions (Operazioni) scegliere Connect (Connetti).

   Verrà visualizzata la finestra Virtual Machine Connection (Connessione macchina virtuale). Se viene visualizzata una finestra di autenticazione, digitare le credenziali di accesso fornite 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 Accedere alla console locale utilizzando credenziali predefinite.

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 descrive come aggiungere una scheda su 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 VMXNET3. 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 Riepilogo della VM, quindi scegli Visualizza tutto accanto alla casella Indirizzo IP. Nella finestra Indirizzi IP macchina virtuale vengono visualizzati tutti gli indirizzi IP da poter utilizzare per accedere al gateway. Verifica che un secondo indirizzo IP sia elencato per il gateway.

   > **Note**
   >
   > Potrebbero volerci alcuni istanti prima che le modifiche della scheda diventino effettive e che le informazioni di riepilogo della VM si aggiornino.

7. Nella console Storage Gateway, accendere il gateway.

8. Nel riquadro Navigazione della console Storage Gateway, scegliere Gateway, quindi scegliere il gateway a cui aggiungere la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

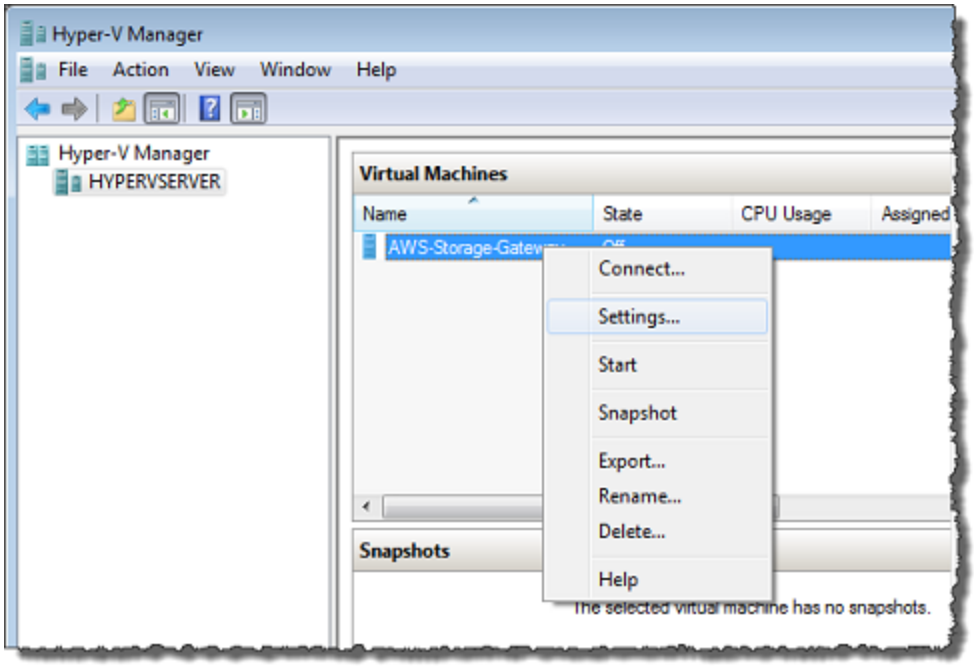
Per informazioni sulle attività locali della console comuni a VMware e agli Hyper-V e KVM, consulta Esecuzione delle operazioni sulla console locale della VM di

Configurazione del gateway per più NIC nell'host Microsoft Hyper-V

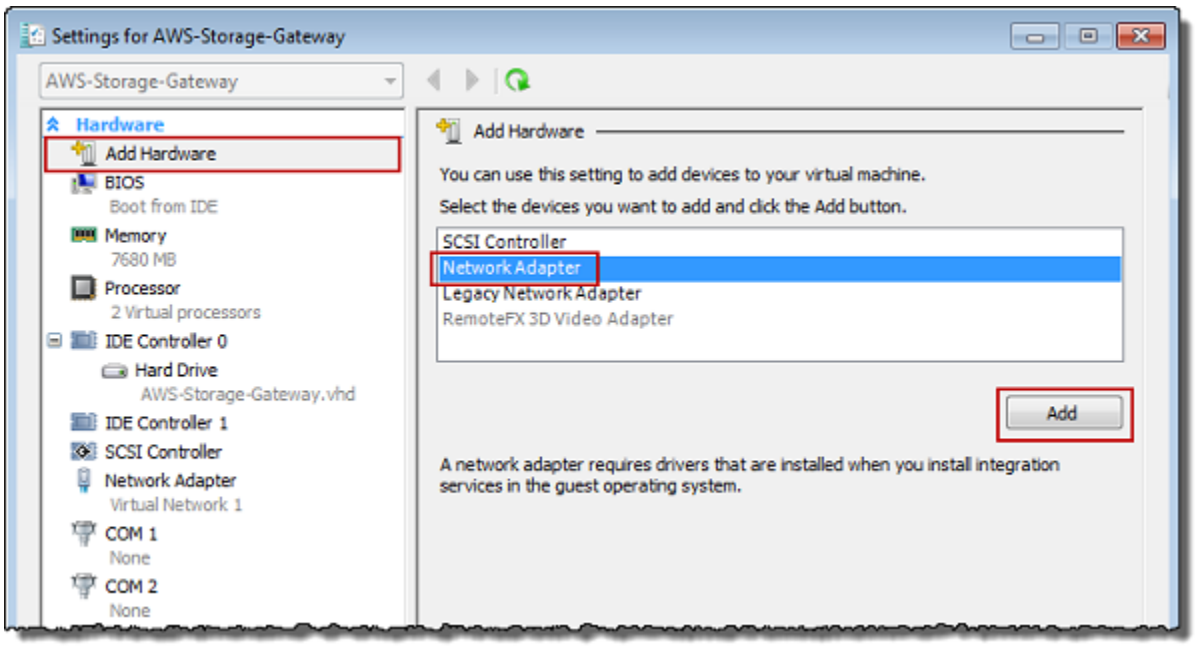
La procedura seguente presuppone che la macchina virtuale del gateway disponga già di una scheda di rete definita e che si aggiunga una seconda scheda. Questa procedura mostra come aggiungere una scheda per un host Microsoft Hyper-V.

Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host Microsoft Hyper-V

1. Nella console Storage Gateway, spegnere il gateway. Per istruzioni, consulta Per arrestare un gateway di nastri virtuali.
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).

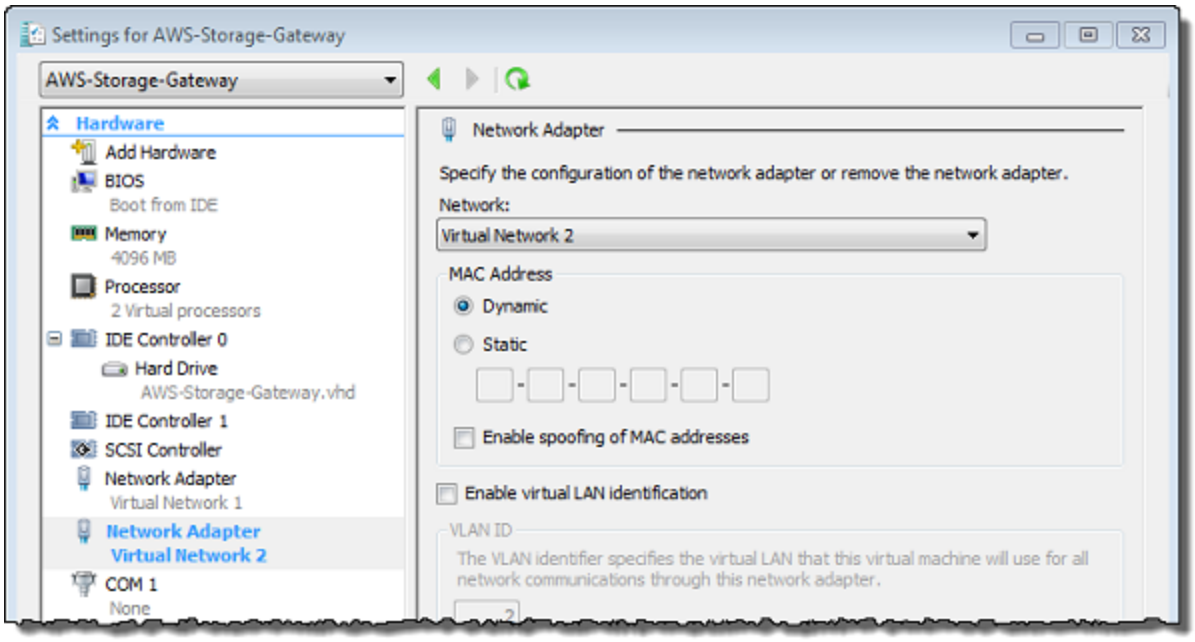


5. Nella finestra di dialogo Settings (Impostazioni) per la macchina virtuale, per Hardware scegliere Add Hardware (Aggiungi hardware).
6. Nel riquadro Add Hardware (Aggiungi hardware) scegliere Network Adapter (Scheda di rete) e quindi Add (Aggiungi) per aggiungere un dispositivo.



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, accendere il gateway. Per istruzioni, consulta Per avviare un gateway di nastri virtuali.
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).

> **Note**
>
> I comandi di montaggio di esempio forniti nella pagina delle informazioni per una condivisione di file nella console Storage Gateway includeranno sempre l'indirizzo IP della scheda di rete che è stata aggiunta più di recente al gateway associato alla condivisione di file.

Per informazioni sulle attività locali della console comuni a VMware e agli Hyper-V e KVM, consulta Esecuzione delle operazioni sulla console locale della VM di

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.

Quando si elimina un gateway, questo non viene più visualizzato nella console di AWS Storage Gateway gestione e la connessione iSCSI all'iniziatore viene chiusa. 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.

> **Note**
>
> Quando si elimina un Tape Gateway, vengono eliminati anche tutti i nastri attualmente presenti nello `AVAILABLE` stato e tutti i dati su tali nastri vengono persi. Se si desidera conservare i dati dai nastri utilizzati da un gateway che si desidera eliminare, è necessario archiviare i nastri prima di eliminare il gateway. Per ulteriori informazioni, consulta Archiving Virtual Tapes.

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

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'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Scegli Gateway, quindi seleziona uno o più gateway da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.

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

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

> **Important**
>
> A seguito dell'eliminazione del gateway, non si incorre più in alcun costo di software; tuttavia, risorse quali nastri virtuali, snapshot Amazon Elastic Block Store (Amazon EBS) e istanze Amazon EC2 restano disponibili. continuano a essere addebitate. È possibile rimuovere le istanze Amazon EC2 e gli snapshot Amazon EBS annullando l'abbonamento a Amazon EC2. Se non si vuole rinunciare all'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 nastri virtuali distribuito su una VM

Prima e dopo l'eliminazione di un gateway o una libreria di nastri virtuali (VTL) bisogna eseguire ulteriori operazioni. le risorse ormai inutilizzate e non continuare a pagarle.

Se il gateway di nastri virtuali da eliminare è distribuito su una macchina virtuale (VM), è consigliabile effettuare la pulizia delle risorse compiendo le seguenti azioni.

> **Important**
>
> Prima di eliminare un gateway di nastri virtuali, bisogna annullare tutte le operazioni di recupero dei nastri ed espellere in toto i nastri recuperati.

Una volta eliminato il gateway di nastri virtuali, occorre rimuovere eventuali risorse a esso associate e inutilizzate, per non pagarle.

Eliminando un gateway di nastri virtuali, è possibile imbattersi in due scenari.

- Il Tape Gateway è connesso a AWS: se il Tape Gateway è connesso a AWS e lo si elimina, le destinazioni iSCSI associate al gateway (ovvero le unità a nastro virtuali e il media changer) non saranno più disponibili.
- Il Tape Gateway non è connesso a AWS: se il Tape Gateway non è connesso a AWS, ad esempio se la VM sottostante è spenta o la rete è inattiva, non è possibile eliminare il gateway. Se tenti di farlo, una volta che l'ambiente sarà in esecuzione ed effettuerà il backup potresti ritrovarti un gateway di nastri virtuali eseguito on-premise con destinazioni iSCSI disponibili. Tuttavia, nessun dato Tape Gateway verrà caricato o scaricato da, AWS.

Se il gateway di nastri virtuali da eliminare non funziona, bisogna disabilitarlo prima di eliminarlo, come descritto di seguito:

- Per eliminare dalla libreria un nastro con lo stato RECUPERATO, espelli il nastro utilizzando il software di backup. Per istruzioni, consulta Archiviazione del nastro.

Dopo averlo disattivato e una volta eliminati i suoi nastri, puoi eliminare il gateway di nastri virtuali. Per istruzioni su come eliminare un gateway, consulta Eliminazione del gateway tramite la console Storage Gateway.

I nastri archiviati restano disponibili e continui a pagarne lo storage finché non li elimini. Per istruzioni su come eliminare un nastro da un archivio, consulta Eliminazione di nastri.

⚠ Important

Per lo storage dei nastri virtuali in un archivio viene addebitato un costo minimo di 90 giorni. Se si recupera un nastro virtuale rimasto in archivio per meno di 90 giorni, vengono comunque addebitati 90 giorni di storage.

Rimozione di risorse da un gateway distribuito su un'istanza Amazon EC2

Se desideri eliminare un gateway distribuito su un'istanza Amazon EC2, ti consigliamo di ripulire le risorse utilizzate con il gateway, in particolare AWS l'istanza Amazon EC2, eventuali volumi Amazon EBS e anche i nastri se hai distribuito un Tape Gateway. Così facendo, si evita di incorrere in costi di utilizzo indesiderati.

Rimozione di risorse da un gateway di nastri virtuali distribuito su Amazon EC2

Se è stato distribuito un gateway di nastri virtuali, si consiglia di eseguire le seguenti azioni per eliminare il gateway e ripulire le sue risorse:

1. Eliminare tutti i nastri virtuali recuperati dal gateway di nastri virtuali. Per ulteriori informazioni, consulta Eliminazione di nastri.
2. Eliminare tutti i nastri virtuali dalla propria libreria. Per ulteriori informazioni, consulta Eliminazione di nastri.
3. Eliminare il gateway di nastri virtuali. Per ulteriori informazioni, consulta Eliminazione del gateway tramite la console Storage Gateway.
4. Terminare tutte le istanze Amazon EC2 ed eliminare in toto i volumi Amazon EBS. Per ulteriori informazioni, consulta Pulizia dell'istanza e del volume nella Guida per l'utente di Amazon EC2 per le istanze Linux.
5. Eliminare tutti i nastri virtuali archiviati. Per ulteriori informazioni, consulta Eliminazione di nastri.

> **Important**
>
> Per lo storage dei nastri virtuali nell'archivio viene addebitato un costo minimo di 90 giorni. Se si recupera un nastro virtuale rimasto in archivio per meno di 90 giorni, vengono comunque addebitati 90 giorni di storage.

Prestazioni

Questa sezione descrive le prestazioni di Storage Gateway.

Argomenti

Linee guida sulle prestazioni per il gateway di nastri virtuali

In questa sezione è possibile trovare linee guida di configurazione per il provisioning dell'hardware per la macchina virtuale del gateway di nastri virtuali. Le dimensioni delle istanze Amazon EC2 e i tipi elencati nella tabella sono esempi e vengono forniti a scopo di riferimento.

Configurazione	Throughput di scrittura Gbps	Lettura dal throughput della cache Gbps	Lettura dalla velocità di trasmissione effettiva Gbps del Cloud Amazon Web Services
Piattaforma host: istanza Amazon EC2 - c5.4xlarge CPU: 16 vCPU | RAM: 32 GB Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: RAID con striping (2 x 500 GB, SSD io1 EBS, 25000 IOPS) Disco buffer di caricamento: 450 GB, io1 SSD, 2000 IOPs	2.3	4.0	2.2

Configurazione	Throughput di scrittura Gbps	Lettura dal throughput della cache Gbps	Lettura dalla velocità di trasmissione effettiva Gbps del Cloud Amazon Web Services
Larghezza di banda di rete al cloud: 10 Gbps			
Piattaforma host: Dispositivo hardware Storage Gateway Disco cache: 2,5 TB Disco buffer di caricamento: 2 TB Larghezza di banda di rete al cloud: 10 Gbps	2.3	8.8	3.8
Piattaforma host: istanza Amazon EC2 - c5d.9xlarge CPU: 36 vCPU | RAM: 72 GB Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: disco 900 GB NVMe Disco buffer di caricamento: disco 900 GB NVMe Larghezza di banda di rete al cloud: 10 Gbps	5.2	11.6	5.2

Configurazione	Throughput di scrittura Gbps	Lettura dal throughput della cache Gbps	Lettura dalla velocità di trasmissione effettiva Gbps del Cloud Amazon Web Services
Piattaforma host: istanza Amazon EC2 - c5d.metal CPU: 96 vCPU | RAM: 192 GB Disco root: 80 GB, io1 SSD, 4.000 IOPS Disco cache: RAID con striping (2 dischi NVMe da 900 GB) Disco buffer di caricamento: disco 900 GB NVMe Larghezza di banda di rete al cloud: 10 Gbps	5.2	11.6	7.2

Note

Queste prestazioni sono state raggiunte usando una dimensione di blocco pari a 1 MB e dieci unità nastro contemporaneamente.
Le configurazioni EC2 nella tabella precedente sono destinate esclusivamente a essere rappresentative delle prestazioni che è possibile ottenere sui propri server fisici con risorse simili. Ad esempio, le configurazioni EC2 che utilizzano un RAID con striping sono state eseguite tramite un meccanismo speciale che generalmente non è supportato dal nostro gateway su EC2. Per ottenere prestazioni simili, dovresti invece utilizzare un controller RAID hardware collegato al server on-premise su cui è installato il gateway.
Le prestazioni potrebbero variare in base alla configurazione della piattaforma host e alla larghezza di banda della rete.

Per migliorare le prestazioni di velocità di trasmissione effettiva di scrittura e lettura del gateway di nastri virtuali, consulta Ottimizzazione delle impostazioni iSCSI, Utilizzare una dimensione del blocco maggiore per le unità nastro e Ottimizzare le prestazioni delle unità nastro virtuali nel software di backup.

Ottimizzazione delle prestazioni del gateway

Configurazione consigliata del server gateway

Per ottenere le migliori prestazioni dal gateway, Storage Gateway consiglia la seguente configurazione del gateway per il server host del gateway:

- Almeno 64 core CPU fisici dedicati
- Per Gateway di nastri virtuali, l'hardware deve dedicare le seguenti quantità di RAM:
  - Almeno 16 GiB di RAM riservata per gateway con dimensioni della cache fino a 16 TiB
  - Almeno 32 GiB di RAM riservata per gateway con dimensioni della cache da 16 TiB a 32 TiB
  - Almeno 48 GiB di RAM riservata per gateway con dimensioni della cache da 32 TiB a 64 TiB

> **Note**
>
> Per prestazioni ottimali del gateway, è necessario fornire almeno 32 GiB di RAM.

- Disco 1, da utilizzare come cache del gateway come segue:
  - RAID (redundant array of independent disks) con striping costituito da SSD NVMe.
- Disco 2, da utilizzare come buffer di caricamento del gateway come segue:
  - RAID con striping composto da SSD NVMe.
- Disco 3, da utilizzare come buffer di caricamento del gateway come segue:
  - RAID con striping composto da SSD 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.

Aggiungere risorse al gateway

I seguenti punti deboli possono ridurre le prestazioni del Tape Gateway Volume Gateway il cloud): AWS

- Numero core CPU
- Velocità di trasmissione effettiva del disco del buffer di caricamento/cache
- Quantità totale di RAM
- Larghezza di banda della rete a AWS
- Larghezza di banda di rete dall'iniziatore al gateway

Questa sezione contiene i passaggi che è possibile eseguire per ottimizzare le prestazioni del gateway. Queste linee guida sono basate sull'aggiunta di risorse al gateway o al server dell'applicazione.

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

Utilizzare dischi a elevate prestazioni

La velocità di trasmissione effettiva del disco buffer di caricamento e cache può limitare le prestazioni di caricamento e download del gateway. Se le prestazioni del gateway sono notevolmente inferiori a quelle previste, prendete in considerazione la possibilità di migliorare la velocità di trasmissione effettiva del disco buffer di caricamento e cache mediante:

- Utilizzo di un RAID con striping come RAID 10 per migliorare la velocità del disco, idealmente con un controller RAID hardware.

> **Note**
>
> Il RAID (redundant array of independent disks), o in particolare le configurazioni RAID con striping su disco come RAID 10, è il processo di divisione di un corpo di dati in blocchi e di distribuzione dei blocchi di dati su più dispositivi di archiviazione. Il livello RAID utilizzato influisce sulla velocità esatta e sulla tolleranza ai guasti che è possibile ottenere. Con lo striping dei carichi di lavoro IO su più dischi, la velocità di trasmissione effettiva complessiva del dispositivo RAID è molto più elevata di quella di qualsiasi disco a membro singolo.

- Utilizzo di dischi ad alte prestazioni collegati direttamente

  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 una velocità di trasmissione effettiva migliore e un maggior numero di operazioni di input/output al secondo (IOPS).

  Per misurare il throughput, utilizza le `WriteBytes` metriche `ReadBytes` and con la statistica di `Samples` Amazon CloudWatch . Ad esempio, le statistiche `Samples` del parametro `ReadBytes` in un periodo di 5 minuti divisi 300 secondi forniscono gli IOPS. In generale, quando si prendono in esame questi parametri per un gateway, cercare un throughput basso e andamenti IOPS bassi per indicare colli di bottiglia correlati al disco. Per ulteriori informazioni sui parametri del gateway, consulta Misurazione delle prestazioni tra Tape Gateway e AWS.

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

Aggiunta di altri dischi del buffer di caricamento

Per ottenere una velocità di trasmissione effettiva di scrittura più elevata, aggiungi almeno due dischi del buffer di caricamento. Quando i dati vengono scritti sul gateway, vengono scritti e archiviati localmente sui dischi del buffer di caricamento. Successivamente, i dati locali archiviati vengono letti in modo asincrono dai dischi per essere elaborati e caricati su AWS. L'aggiunta di altri dischi del buffer di caricamento può ridurre la quantità di operazioni di I/O simultanee eseguite su ogni singolo disco. Ciò può comportare un aumento della velocità di trasmissione effettiva di scrittura sul gateway.

Supportare dischi virtuali gateway con dischi fisici separati

Quando viene effettuato il provisioning dei dischi del gateway, è consigliabile non effettuare il provisioning di dischi locali per il buffer di caricamento e lo storage della cache 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 o RAID 6, può portare a prestazioni mediocri.

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 ciascun processore virtuale assegnato alla macchina virtuale del gateway sia supportato da un core dedicato. 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 in 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.

Aumenta la larghezza di banda tra il gateway e il cloud AWS

L'aumento della larghezza di banda da e verso il AWS cloud aumenterà la velocità massima di ingresso e uscita dei dati dal gateway al gateway. AWS Ciò può migliorare le prestazioni del gateway se la velocità della rete è il fattore limitante nella configurazione del gateway, anziché altri fattori come la lentezza dei dischi o la scarsa larghezza di banda della connessione gateway-iniziatore.

La larghezza di banda di rete da e verso AWS definisce le prestazioni medie massime teoriche del Tape Gateway durante carichi di lavoro sostenuti.

- La velocità media alla quale è possibile scrivere dati sul gateway di nastri virtuali per lunghi intervalli non supererà la larghezza di banda di caricamento a AWS.
- La velocità media alla quale è possibile leggere i dati dal Tape Gateway per lunghi intervalli non supererà la larghezza di banda di download. AWS

> **Note**
>
> Le prestazioni del gateway osservate saranno probabilmente inferiori alla larghezza di banda della rete a causa di altri fattori limitanti elencati qui, come la velocità di trasmissione effettiva del disco nel buffer di caricamento/cache, il numero di core della CPU, la quantità totale di RAM o la larghezza di banda tra l'iniziatore e il gateway. Inoltre, il normale funzionamento del gateway comporta l'adozione di numerose azioni per proteggere i dati, che potrebbero far sì che le prestazioni osservate siano inferiori alla larghezza di banda della rete.

Ottimizzazione delle impostazioni iSCSI

È possibile ottimizzare le impostazioni iSCSI sull'iniziatore iSCSI per ottenere prestazioni I/O più elevate. Si consiglia di scegliere 256 KiB per `MaxReceiveDataSegmentLength` e `FirstBurstLength` e 1 MiB per `MaxBurstLength`. Per ulteriori informazioni sulla configurazione delle impostazioni di iSCSI, consulta Personalizzazione delle impostazioni iSCSI.

> **Note**
>
> Queste impostazioni consigliate possono consentire prestazioni complessive migliori. Tuttavia, le impostazioni iSCSI specifiche necessarie per ottimizzare le prestazioni variano a seconda del software di backup utilizzato. Per ulteriori informazioni, consultare la documentazione del software di backup.

Utilizzare una dimensione del blocco maggiore per le unità nastro

Per un gateway di nastri virtuali, la dimensione del blocco predefinita per un'unità nastro è 64 KB. Tuttavia, è possibile aumentarla fino a 1 MB per migliorare le prestazioni di I/O.

La dimensione del blocco scelta dipende dalla dimensione del blocco massima supportata dal software di backup. È consigliabile impostare la dimensione del blocco delle unità nastro nel software di backup alla dimensione più grande possibile. Tuttavia, questa dimensione del blocco non deve superare la dimensione massima di 1 MB supportata dal gateway.

I gateway di nastri virtuali negoziano la dimensione del blocco per le unità nastro virtuali per farla corrispondere automaticamente a quanto impostato nel software di backup. Quando si aumenta

la dimensione del blocco nel software di backup, è consigliabile anche controllare le impostazioni per accertarsi che l'iniziatore host supporti la nuova dimensione. Per ulteriori informazioni, consulta la documentazione per il tuo software di backup. Per ulteriori informazioni sulle linee guida delle prestazioni specifiche del gateway, consulta Prestazioni.

Ottimizzare le prestazioni delle unità nastro virtuali nel software di backup

Il software di backup è in grado di eseguire il backup dei dati su un massimo di 10 unità nastro virtuali su un gateway di nastri virtuali contemporaneamente. È consigliabile configurare i processi di backup nel software di backup per l'utilizzo di almeno 4 unità nastro virtuali contemporaneamente su un gateway di nastri virtuali. È possibile ottenere un throughput di scrittura migliore quando il software di backup esegue il backup dei dati su più di un nastro virtuale nello stesso momento.

Come regola generale, è possibile ottenere una velocità di trasmissione effettiva massima più elevata operando (leggendo o scrivendo da) più nastri virtuali contemporaneamente. Utilizzando più unità nastro, si consente al gateway di soddisfare più richieste contemporaneamente, migliorando potenzialmente le prestazioni.

Aggiungere risorse per l'ambiente applicativo

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

La connessione tra l'iniziatore iSCSI e il gateway può limitare le prestazioni di upload e download. Se il gateway presenta prestazioni notevolmente peggiori del previsto e hai già migliorato il numero di core della CPU e la velocità di trasmissione effettiva del disco, prendi in considerazione:

- Aggiornamento dei cavi di rete per disporre di una maggiore larghezza di banda tra iniziatore e gateway.
- Utilizzo del maggior numero possibile di unità nastro contemporaneamente. iSCSI non supporta l'accodamento di più richieste per la stessa destinazione, il che significa che più unità nastro si utilizzano, più richieste il gateway può soddisfare contemporaneamente. Ciò consentirà di utilizzare in modo più completo la larghezza di banda tra il gateway e l'iniziatore, aumentando la velocità di trasmissione effettiva apparente del gateway.

Per ottimizzare le prestazioni del gateway, garantire che la larghezza di banda di rete tra l'applicazione e il gateway sia in grado di far fronte alle esigenze dell'applicazione. È possibile utilizzare i parametri `ReadBytes` e `WriteBytes` del gateway per misurare la velocità di trasmissione effettiva totale dei dati. Per ulteriori informazioni su questi parametri, consulta Misurazione delle prestazioni tra Tape Gateway e AWS.

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.

vSphere HA funziona raggruppando le macchine virtuali e gli host su cui risiedono in un cluster per la ridondanza. Gli host del cluster vengono monitorati e, in caso di guasto, le macchine virtuali su un host guasto vengono riavviate su host alternativi. In genere, questo ripristino avviene rapidamente e senza perdita di dati. Per ulteriori informazioni su vSphere HA, vedere How vSphere HA Works nella documentazione di VMware.

> **Note**
>
> Il tempo necessario per riavviare una macchina virtuale guasta e ristabilire la connessione iSCSI su un nuovo host dipende da molti fattori, come il sistema operativo host e il carico di risorse, la velocità del disco, la connessione di rete e l'infrastruttura SAN/storage.

Per utilizzare VMware HA con Storage Gateway, attieniti alla procedura indicata di seguito.

Argomenti

- Configurazione del cluster vSphere VMware HA
- Scarica l'immagine .ova dalla console Storage Gateway
- Distribuzione del gateway

- (Facoltativo) Aggiunta di opzioni di sostituzione per altre macchine virtuali nel cluster
- 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.

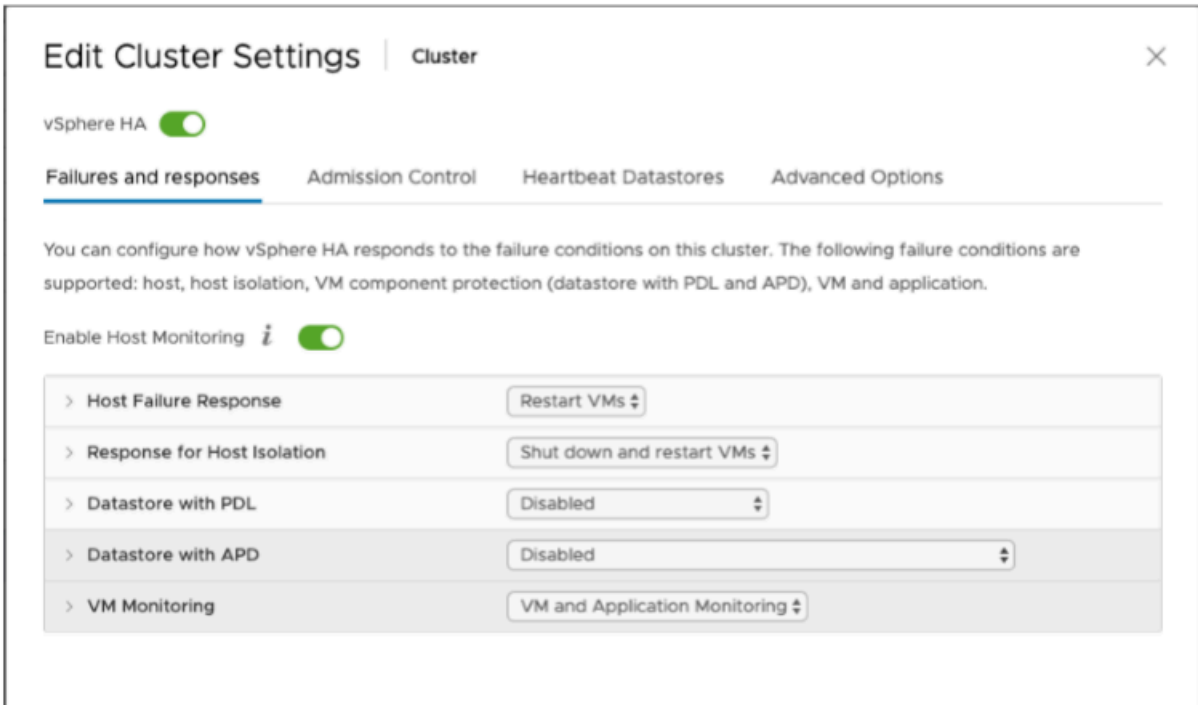
Successivamente, configura il cluster VMware da utilizzare con Storage Gateway.

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:

   - Host Failure Response (Risposta errore host): Restart VMs (Riavvia VM)
   - Response for Host Isolation (Risposta per isolamento host): Shut down and restart VMs (Arresta e riavvia VM)
   - Datastore with PDL (Datastore con PDL): Disabled (Disabilitato)
   - Datastore with APD (Datastore con APD): Disabled (Disabilitato)
   - VM Monitoring (Monitoraggio VM) : VM and Application Monitoring (Monitoraggio VM e applicazioni)

   Per un esempio, vedere le immagini seguenti.



2. Ottimizzare la sensibilità del cluster regolando i seguenti valori:

   - Intervallo di errore: dopo questo intervallo, la macchina virtuale viene riavviata se non viene ricevuto un heartbeat VM.
   - Tempo di attività minimo: tempo di attesa del cluster dopo che una macchina virtuale inizia a monitorare gli heartbeat degli strumenti VM.
   - Numero massimo di reimpostazioni per VM: il cluster riavvia la macchina virtuale per un numero massimo di volte all'interno della finestra temporale massima di ripristino.
   - Finestra temporale massima reimpostazioni: la finestra temporale entro cui contare il numero massimo di reimpostazioni per VM.

   Se non si è sicuri di quali valori impostare, utilizzare queste impostazioni di esempio:

   - Failure interval (Intervallo di errore): **30** secondi
   - Minimum uptime (Tempo di attività minimo): **120** secondi
   - Maximum per-VM resets (Numero massimo reimpostazioni VM): **3**
   - Maximum resets time window (Finestra temporale massima reimpostazioni): **1** ora

Se 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.

Scarica l'immagine .ova dalla console Storage Gateway

Per scaricare l'immagine .ova per il gateway

- Nella pagina Configura gateway nella console di Gateway di archiviazione AWS, seleziona il tipo di gateway e la piattaforma host, quindi utilizza il collegamento fornito nella console per scaricare il file .ova, come descritto in Configurare un gateway di nastri virtuali.

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. Quando si implementa il file .ova Storage Gateway in un ambiente VMware o on-premise, i dischi vengono descritti come dischi SCSI paravirtualizzati. La paravirtualizzazione è una modalità in cui la macchina virtuale del gateway opera con il sistema operativo host in modo che la console possa identificare i dischi aggiunti alla macchina virtuale.

   Per configurare la macchina virtuale per l'uso di controller paravirtualizzati

   1. Nel client VMware vSphere aprire il menu contestuale (clic con il pulsante destro del mouse) per la macchina virtuale del gateway e quindi scegliere Edit Settings (Modifica impostazioni).
   2. Nella finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale) scegliere la scheda Hardware, selezionare SCSI controller 0 (Controller SCSI 0)e quindi scegliere Change Type (Cambia tipo).
   3. Nella finestra di dialogo Change SCSI Controller Type (Cambia tipo di controller SCSI) selezionare VMware Paravirtual (Paravirtuale VMware) e quindi scegliere OK.

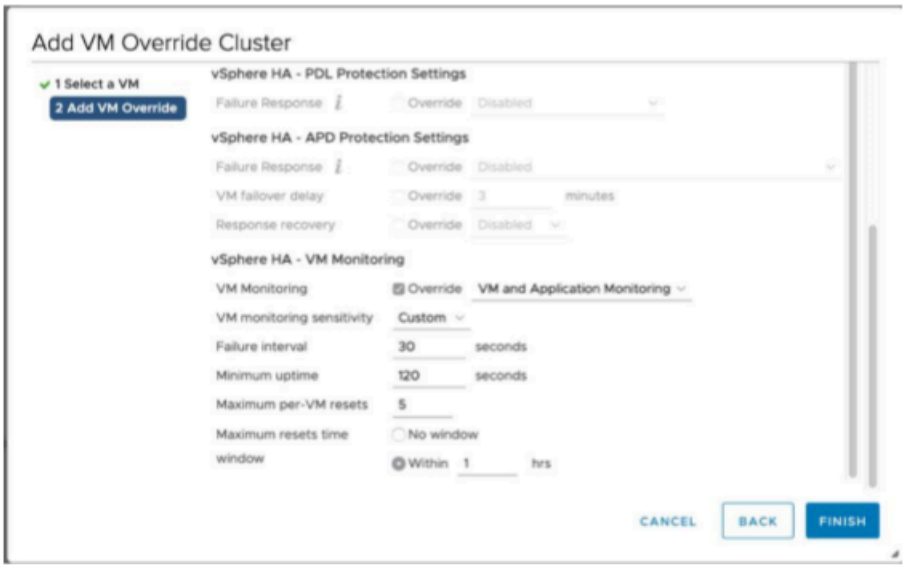
(Facoltativo) Aggiunta di opzioni di sostituzione per altre macchine virtuali nel cluster

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

- Segui le procedure illustrate nei seguenti argomenti:

a. Connect Tape Gateway a AWS
b. Revisione delle impostazioni e attivazione del gateway di nastri virtuali
c. Configurazione del gateway di nastri virtuali

Test della configurazione VMware High Availability

Dopo aver attivato il gateway, esegui il test della configurazione.

Per testare la configurazione VMware HA

1. Apri la console Storage Gateway all'indirizzo https://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).

Puoi trovare informazioni sugli eventi VMware HA nei gruppi di CloudWatch log di Amazon. Per ulteriori informazioni, vedere Getting Tape Gateway Health Logs with Log Log CloudWatch Log of Log di Log Gateway Gateway Gateway con CloudWatch Log Groups

Sicurezza nello AWS Storage Gateway

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Amazon Web Services Cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Storage Gateway, vedere AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio utilizzato. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa Storage Gateway. Gli argomenti seguenti illustrano come configurare Storage Gateway per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse dello Storage Gateway.

Argomenti

Protezione dei dati in AWS Storage Gateway

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Storage Gateway. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog AWS Shared Responsibility Model and GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

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

Crittografia dei dati tramite AWS KMS

Storage Gateway utilizza SSL/TLS (Secure Socket Layers/Transport Layer Security) per crittografare i dati trasferiti tra l'appliance gateway e lo storage. AWS 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. È possibile utilizzare l'API Storage Gateway per configurare il gateway per crittografare i dati archiviati nel cloud utilizzando la crittografia lato server con chiavi AWS Key Management Service (SSE-KMS).

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

Crittografia di una condivisione file

Per una condivisione file, è possibile configurare il gateway per crittografare gli oggetti con chiavi gestite da AWS KMS utilizzando SSE-KMS. Per informazioni sull'utilizzo dell'API Storage Gateway per crittografare i dati scritti in una condivisione di file, consulta CreateNFS FileShare nel AWS Storage Gateway riferimento API.

Crittografia di un volume

Per i volumi memorizzati nella cache, puoi configurare il gateway per crittografare i dati di volume archiviati nel AWS KMS cloud con chiavi gestite utilizzando l'API Storage Gateway. È possibile specificare una delle chiavi gestite come chiave di KMS. La chiave utilizzata per crittografare il volume non può essere modificata dopo che il volume è stato creato. Per informazioni sull'utilizzo dell'API Storage Gateway per crittografare i dati scritti su un volume memorizzato nella cache, vedere CreateCachediscsiVolume o scsiVolume nel riferimento API. CreateStoredi AWS Storage Gateway

Crittografia di un nastro

Per un nastro virtuale, puoi configurare il gateway per crittografare i dati su nastro archiviati nel AWS KMS cloud con chiavi gestite utilizzando l'API Storage Gateway. È possibile specificare una delle chiavi gestite come chiave di KMS. La chiave utilizzata per crittografare i dati del nastro non può essere modificata dopo che il nastro è stato creato. Per informazioni sull'utilizzo dell'API Storage

Gateway per crittografare i dati scritti su un nastro virtuale, vedere CreateTapesnell'AWS Storage Gateway API Reference.

Quando si utilizza AWS KMS per crittografare i dati, è necessario tenere presente quanto segue:

- I dati vengono crittografati nel cloud mentre sono inattivi. Ciò significa che i dati vengono crittografati in Amazon S3.
- Gli utenti IAM devono disporre delle autorizzazioni necessarie per chiamare le operazioni AWS KMS API. Per ulteriori informazioni, consulta Utilizzo delle policy IAM con AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .
- Se elimini o disattivi la AWS AWS KMS chiave o revochi il token di concessione, non puoi accedere ai dati sul volume o sul nastro. Per ulteriori informazioni, consulta la sezione Eliminazione delle chiavi KMS nella Guida per gli sviluppatori di AWS Key Management Service .
- 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 What is? AWS Key Management Service

Identity and Access Management per AWS Storage Gateway

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

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS SGW.

Utente del servizio: se utilizzi il servizio AWS SGW per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità AWS SGW per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di SGW AWS , consulta Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway.

Amministratore del servizio: se sei responsabile delle risorse AWS SGW della tua azienda, probabilmente hai pieno accesso a SGW. AWS È tuo compito determinare a quali funzionalità e risorse AWS SGW devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS SGW, consulta. Come funziona AWS Storage Gateway con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a AWS SGW. Per visualizzare esempi di policy AWS SGW basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per AWS Storage Gateway

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per

ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM

può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona AWS Storage Gateway con IAM

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

Funzionalità IAM che puoi utilizzare con AWS Storage Gateway

Funzionalità IAM	AWS Supporto SGW
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come AWS SGW e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per SGW AWS

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per SGW AWS

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

Politiche basate sulle risorse all'interno di SGW AWS

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per AWS SGW

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

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

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

```
sgw
```

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

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

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

Risorse politiche per SGW AWS

Supporta le risorse di policy	Sì

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

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

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

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

Chiavi relative alle condizioni delle politiche per SGW AWS

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

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

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

AWS ACL in SGW

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con SGW AWS

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con SGW AWS

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per SGW AWS

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AWS SGW

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità AWS SGW. Modificate i ruoli di servizio solo quando AWS SGW fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per SGW AWS

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per AWS Storage Gateway

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS SGW. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l' AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da AWS SGW, incluso il formato degli ARN per ciascun tipo di risorsa, vedere Actions, Resources and Condition Keys for AWS Storage Gateway nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console SGW AWS
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse AWS SGW nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console SGW AWS

Per accedere alla console AWS Storage Gateway, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli

sulle risorse AWS SGW presenti nel proprio. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console AWS SGW, collega anche la AWS SGW *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS SGW e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in SGW AWS
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AWS SGW

Non sono autorizzato a eseguire un'azione in SGW AWS

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `sgw:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `sgw:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AWS SGW.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS SGW. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AWS SGW

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS SGW supporta queste funzionalità, consulta. Come funziona AWS Storage Gateway con IAM

- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Registrazione e monitoraggio AWS Storage Gateway

Storage Gateway è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Storage Gateway. CloudTrail acquisisce tutte le chiamate API per Storage Gateway come eventi. Le chiamate acquisite includono le chiamate dalla Storage Gateway e le chiamate di codice alle operazioni API Storage gateway. Se crei un trail, puoi attivare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Storage Gateway. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Storage Gateway, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sullo Storage Gateway in CloudTrail

CloudTrail viene attivato sul tuo account Amazon Web Services al momento della creazione dell'account. Quando si verifica un'attività in Storage Gateway, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'account Amazon Web Services. Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell'account Amazon Web Services che includa gli eventi per Storage Gateway, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si

applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le operazioni di Storage Gateway sono registrate e documentate nell'argomento Operazioni. Ad esempio, le chiamate a `ActivateGatewayListGateways`, e `ShutdownGateway` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di Storage Gateway.

Un trail è una configurazione che consente la consegna di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                     "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
            }]
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' ListGateways azione.

```
{
 "Records": [{
               "eventVersion": "1.02",
```

```
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 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 per AWS Storage Gateway

I revisori di terze parti valutano la sicurezza e la conformità di AWS Storage Gateway nell'ambito di più programmi di AWS conformità. Questi includono SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere AWS Servizi inclusi nell'ambito del programma di conformitàAWS . Per informazioni generali, vedere Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La responsabilità per la conformità quando utilizzi Storage Gateway è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. AWS fornisce le risorse seguenti per semplificare la conformità:

- Guide rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi all'HIPAA. AWS
- AWS Risorse per la conformità Risorse per la conformità: questa raccolta di potrebbe riguardare il settore e la località in cui operate.
- Valutazione delle risorse in base alle regole contenute nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza nello AWS Storage Gateway

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Storage Gateway offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati:

- 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, consulta Utilizzo di VMware vSphere High Availability con Storage Gateway.
- Archivia nastri virtuali in S3 Glacier Flexible Retrieval. Per ulteriori informazioni, consulta Archiviazione di nastri virtuali.

Sicurezza dell'infrastruttura in AWS Storage Gateway

In quanto servizio gestito, AWS Storage Gateway è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Si utilizzano chiamate API AWS pubblicate per accedere a Storage Gateway attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS Best practice per la sicurezza

AWS fornisce una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste pratiche potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni. Per ulteriori informazioni, consulta Best practice di sicurezza AWS.

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 di gateway di file. 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 virtuali. Le informazioni sulla risoluzione dei problemi relativi al gateway si riferiscono all'utilizzo CloudWatch delle metriche. 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 on-premise

Di seguito sono riportate informazioni sui problemi tipici che potresti riscontrare lavorando con i gateway locali e su come attivarli per AWS Support 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.

Problema	Operazione da eseguire
	• 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. • La convalida/ispezione del certificato SSL non deve essere attivata. Storage Gateway utilizza l'autenticazione TLS reciproca che non riuscirebbe se un'applicazione di terze parti tenta di intercettare/firmare uno dei due certificati. • Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS. Per ulteriori informazioni sui requisiti di rete e del firewall, consulta Requisiti di rete e firewall.

Problema	Operazione da eseguire
L'attivazione del gateway non riesce se si fa clic sul pulsante Continua con l'attivazione nella console di gestione Storage Gateway.	• Verificare l'accessibilità della VM del gateway eseguendone il ping dal client. • Verificare la connettività di rete a Internet della VM, senza la quale occorrerà configurare un proxy SOCKS. Per ulteriori informazioni in merito, consulta Instradamento del gateway in locale tramite un proxy. • 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 l'orario di host degli hypervisor e VM, consulta Sincronizzazione dell'ora della VM associata al gateway. • Dopo queste fasi, è possibile riprovare l'implementazione del gateway con la console Storage Gateway e la procedura guidata Configura e attiva il gateway. • La convalida/ispezione del certificato SSL non deve essere attivata. Storage Gateway utilizza l'autenticazione TLS reciproca che non riuscirebbe se un'applicazione di terze parti tenta di intercettare/firmare uno dei due certificati. • 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, consulta Requisiti.
È necessario rimuovere un disco allocato come spazio del buffer di caricamento. Ad esempio, si intende ridurre lo spazio del buffer di caricamento di un gateway o bisogna sostituire un disco utilizzato come buffer di caricamento in cui si sono verificati errori.	Per istruzioni sulla rimozione di un disco allocato come spazio del buffer di caricamento, consulta Rimozione di dischi dal gateway.

Problema	Operazione da eseguire
Occorre aumentare la larghezza di banda tra il gateway e AWS.	È possibile migliorare la larghezza di banda dal gateway al AWS configurando la connessione Internet AWS su un adattatore di rete (NIC) separato da quello che collega le applicazioni e la macchina virtuale gateway. Questo approccio è utile se si dispone di una connessione a larghezza di banda elevata AWS e si desidera evitare conflitti in termini di larghezza di banda, specialmente durante il ripristino di un'istantanea. Utilizzando AWS Direct Connect si può stabilire una connessione di rete dedicata tra il gateway on-premise e AWS, perfetta per i carichi di lavoro con elevata velocità di trasmissione effettiva. Per misurare la larghezza di banda della connessione dal gateway a AWS, utilizza le metriche e del `CloudBytesDownloaded` gateway. `CloudBytesUploaded` Per ulteriori informazioni su questo argomento, consulta Misurazione delle prestazioni tra Tape Gateway e AWS. Ottimizzando la connettività a Internet si evita il riempimento del buffer di caricamento.

Problema	Operazione da eseguire

Il throughput da o verso il gateway si azzera.	• Nella scheda Gateway della console Storage Gateway, verificare che gli indirizzi IP della VM del gateway corrispondano a quelli visualizzati con il software 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 in Spegnimento della macchina virtuale gateway. Dopo il riavvio, gli indirizzi dell'elenco Indirizzi IP nella scheda Gateway della console Storage Gateway dovrebbero 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.
	• Verifica la connettività del gateway a AWS come descritto in. Verifica della connessione del gateway a Internet
	• Controllare la configurazione della scheda di rete del gateway per assicurarsi che tutte le interfacce necessarie siano effettivamente attivate. Per farlo, attenersi alle istruzioni riportate in Configurazione di rete del gateway e selezionare l'opzione inerente alla visualizzazione della configurazione di rete del gateway.
	
	Puoi visualizzare la velocità effettiva da e verso il gateway dalla CloudWatch console Amazon. Per ulteriori informazioni sulla misurazione della velocità effettiva da e verso il gateway e AWS, consulta. Misurazione delle prestazioni tra Tape Gateway e AWS

Si sono verificati problemi durante l'importazione (distribuzione) di Storage Gateway su Microsoft Hyper-V.	Consultare Come risolvere i problemi di configurazione di Microsoft Hyper-V, documento dedicato ai problemi che più comunemente possono verificarsi distribuendo un gateway su Microsoft Hyper-V.

Problema	Operazione da eseguire
Viene visualizzato il seguente messaggio: "I dati scritti sul volume del gateway non sono archiviati in modo sicuro su AWS".	Questo messaggio viene ricevuto se la VM del gateway è stata creata da un clone o uno snapshot di un'altra VM di gateway. Se così non fosse, rivolgersi a AWS Support.

Consente di contribuire AWS Support alla risoluzione dei problemi del gateway ospitato in locale

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, inclusa l'attivazione dell'accesso AWS Support al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, AWS Support l'accesso al gateway è disattivato. È possibile consentire l'accesso tramite la console locale dell'host. Per AWS Support consentire l'accesso al gateway, è necessario innanzitutto accedere alla console locale dell'host, accedere alla console di Storage Gateway e quindi connettersi al server di supporto.

Per consentire AWS Support l'accesso al gateway

1. Accedere alla console locale dell'host.
   - VMware ESXi: per ulteriori informazioni, consulta Accesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.
2. Quando richiesto, immetti il numero corrispondente per selezionare Console gateway.
3. Immetti **h** per aprire la finestra dei comandi disponibili.
4. Esegui una di queste operazioni:
   - Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

- Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

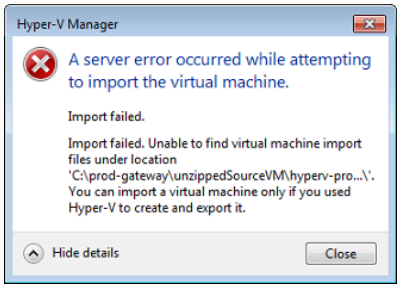
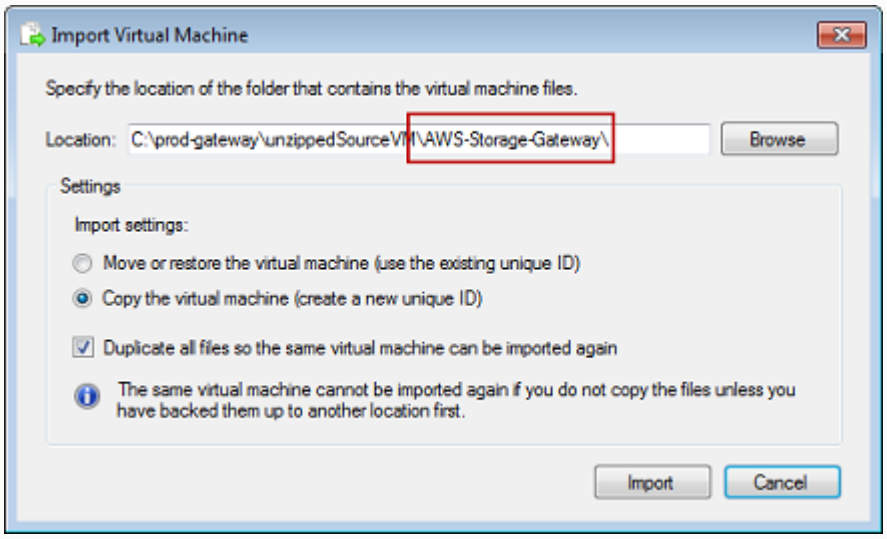
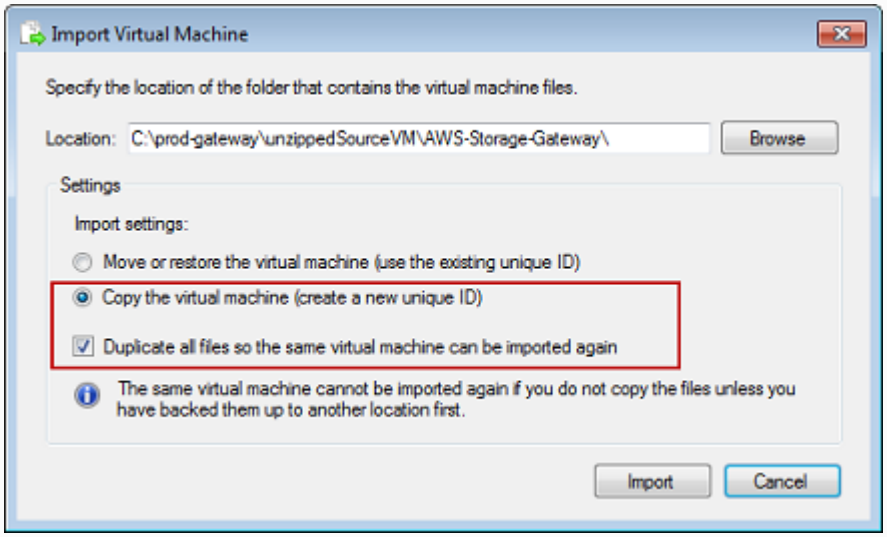
> **Note**
>
> Il numero del canale non è un numero di porta Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

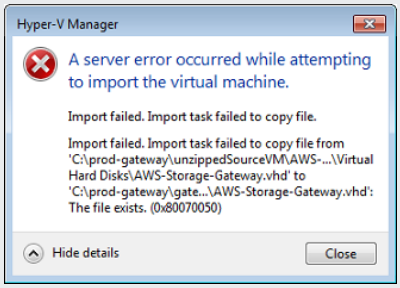
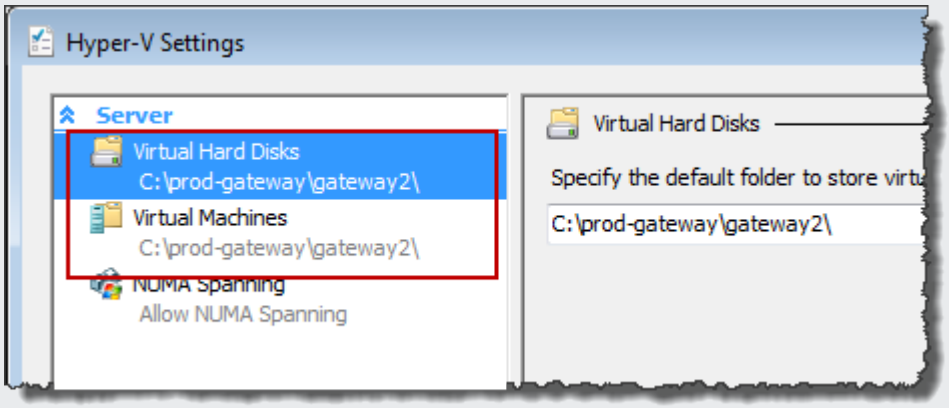
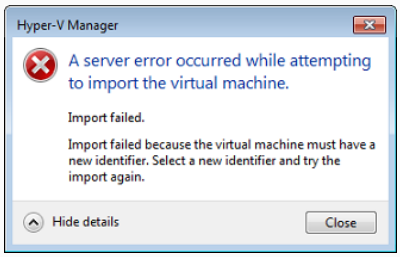
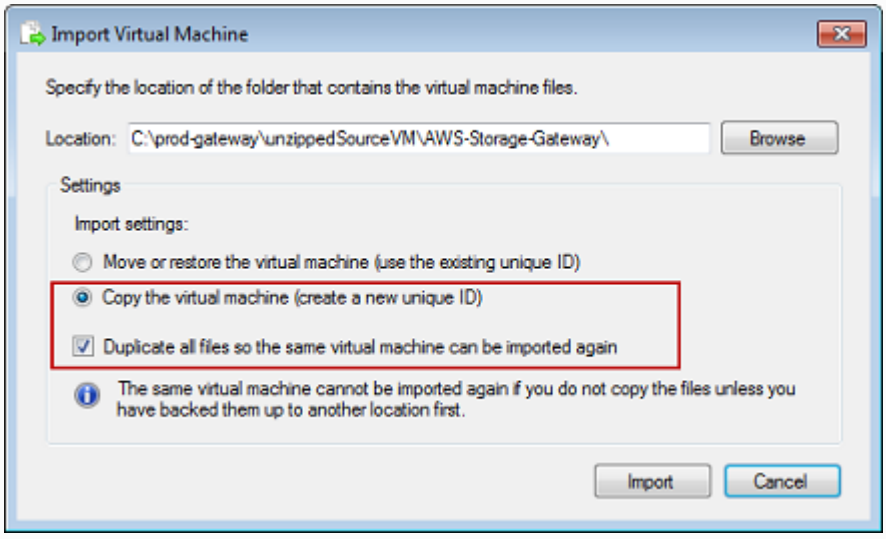
5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto in AWS Support modo da AWS Support poterti fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **`q`** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Immetti **`exit`** per disconnetterti dalla console gateway.
8. Seguire le istruzioni per uscire dalla console locale.

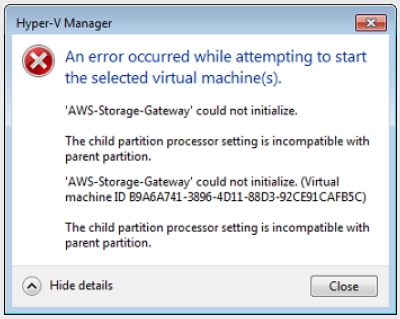
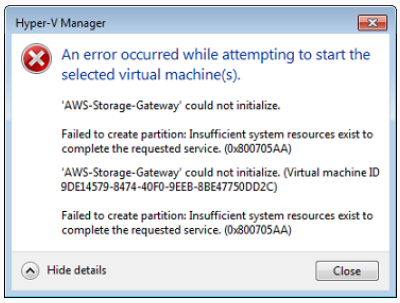
Come risolvere i problemi di configurazione di Microsoft Hyper-V

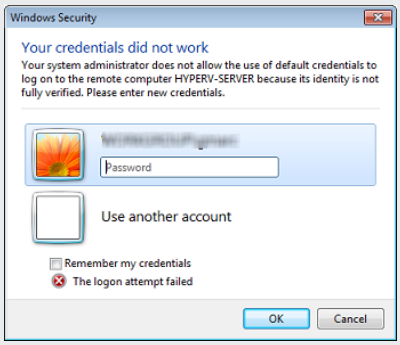
Nella tabella seguente sono elencati i problemi che più comunemente possono verificarsi quando si implementa Storage Gateway sulla piattaforma Microsoft Hyper-V.

Problema	Operazione da eseguire
Nel tentativo di importare un gateway si riceve il messaggio di errore "Importazione non riuscita. Impossibile trovare il file di importazione della	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:

Problema	Operazione da eseguire
macchina virtuale nella sede...".  	 • 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 non riuscita. 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). 
Nel tentativo di importare un gateway si riceve un messaggio di errore: "Importazione non riuscita. 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). 

Problema	Operazione da eseguire
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, consulta Requisiti.
Tentando di avviare una VM del gateway si visualizz a il messaggio di errore "Impossibile creare la partizione: risorse insuffici enti per erogare 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, consulta Requisiti.

Problema	Operazione da eseguire
Gli aggiornamenti di software di gateway e snapshot si verificano con tempistiche leggermente diverse da quelle previste.	L'orologio della VM del gateway potrebbe essere soggetto allo scostamento del clock, cioè differire dall'orario effettivo. Controlla re e correggere l'orario della VM utilizzando l'opzione di sincroniz zazione oraria della console del gateway locale. Per ulteriori informazioni, consulta Sincronizzazione dell'ora della VM associata al gateway.
Bisogna inserire i file decompressi di Storage Gateway con Microsoft Hyper-V nel file system dell'host.	Accedere all'host come si fa generalmente con un server Microsoft Windows. Ad esempio, se il nome dell'host dell'hypervisor è `hyperv-server` , si può utilizzare il percorso UNC `\\hyperv-server\c$` , presupponendo che il nome `hyperv-server` possa essere risolto o sia definito nel file degli host in locale.
Nel connettersi all'hyper visor viene richiesto di immettere le credenziali. 	Aggiungere le credenziali utente da amministratore locale per l'host dell'hypervisor, avvalendosi dello strumento Sconfig.cmd.
Potresti notare prestazioni di rete scadenti se attivi la coda di macchine virtuali (VMQ) su un host Hyper-V che utilizza una scheda di rete Broadcom.	Per informazioni su una soluzione alternativa, consulta la documentazione Microsoft, vedi Scarse prestazioni di rete sulle macchine virtuali su un host Hyper-V Windows Server 2012 se VMQ è attivato.

Come risolvere i problemi di gateway distribuiti su Amazon EC2

Nelle sezioni seguenti, sono elencati i classici problemi che potrebbero verificarsi utilizzando gateway distribuiti su Amazon EC2. Per ulteriori informazioni sulla differenza tra un gateway on-premise e uno distribuito su Amazon EC2, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali.

Argomenti

Dopo qualche secondo, il gateway ancora non si attiva

Nella console Amazon EC2 accertati di quanto segue:

- La porta 80 è abilitata nel gruppo di sicurezza associato all'istanza. Per ulteriori informazioni sulla modifica delle regole del gruppo di sicurezza, consulta Aggiunta di regole a un gruppo di sicurezza nella Guida per l'utente di Amazon EC2 per le istanze Linux.
- L'istanza del gateway è contrassegnata come in esecuzione. Lo State (Stato) dell'istanza nella console Amazon EC2 dovrebbe essere IN ESECUZIONE.
- Il tipo di istanza Amazon EC2 soddisfa i requisiti minimi, come descritto in Requisiti di storage.

Dopo aver risolto il problema, provare di nuovo ad attivare il gateway. A tale scopo, aprire la console Storage Gateway, scegliere Deploy a new Gateway on Amazon EC2 (Distribuisci un nuovo gateway su Amazon EC2) e inserire nuovamente l'indirizzo IP dell'istanza.

L'istanza del gateway EC2 non è inclusa nell'elenco delle istanze

Se non si assegna all'istanza un tag di risorsa e si dispone di molte istanze in esecuzione, può risultare difficile stabilire quale istanza è stata avviata. Per individuare l'istanza del gateway, in tal caso, occorre procedere come di seguito:

- Controllare il nome dell'Amazon Machine Image (AMI) nella scheda Description (Descrizione) dell'istanza. Il nome di un'istanza basata sull'AMI di Storage Gateway dovrebbe iniziare con il testo **`aws-storage-gateway-ami`**.
- Se si dispone di più istanze basate sull'AMI di Storage Gateway, controllarne l'orario di avvio per trovare quella giusta.

Un volume Amazon EBS creato non può essere collegato all'istanza del gateway EC2

Controlla che il volume Amazon EBS in questione si trovi nella stessa zona di disponibilità dell'istanza del gateway. Qualora le zone di disponibilità differissero, crea un nuovo volume nella stessa zona di disponibilità dell'istanza.

Nel tentativo di aggiungere volumi di storage viene visualizzato un messaggio che denuncia l'indisponibilità di dischi

Per un gateway appena attivato, non è ancora definito alcuno storage di volumi. Prima di poter definire uno storage di volumi, è necessario allocare i dischi locali del gateway, da utilizzare come buffer di caricamento e storage della cache. Per un gateway distribuito su Amazon EC2, i dischi locali sono volumi Amazon EBS collegati all'istanza. Questo messaggio di errore solitamente viene generato quando non vi sono volumi Amazon EBS definiti per l'istanza.

Controlla i dispositivi a blocchi definiti per l'istanza che esegue il gateway. Se sono disponibili solo due dispositivi a blocchi (quelli predefiniti per l'AMI), è necessario aggiungere storage. Per ulteriori informazioni in merito, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali. Dopo aver collegato due o più volumi Amazon EBS, puoi provare a creare storage di volumi nel gateway.

Occorre rimuovere un disco allocato per ridurre lo spazio del buffer di caricamento

Seguire la procedura riportata in Determinazione delle dimensioni del buffer di caricamento da allocare.

La velocità di trasmissione effettiva da o verso il gateway EC2 si azzera

Verifica che l'istanza del gateway sia in esecuzione. Attendi l'eventuale avvio o riavvio dell'istanza.

Inoltre, verifica che l'IP del gateway non sia cambiato. Se l'istanza è stata arrestata e poi riavviata, il suo indirizzo IP potrebbe essere cambiato, nel qual caso è necessario attivare un nuovo gateway.

Puoi visualizzare la velocità effettiva da e verso il gateway dalla CloudWatch console Amazon. Per ulteriori informazioni sulla misurazione della velocità effettiva da e verso il gateway e AWS, consulta. Misurazione delle prestazioni tra Tape Gateway e AWS

Vuoi aiutarci AWS Support a risolvere i problemi del tuo gateway EC2

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, inclusa l'attivazione dell'accesso AWS Support al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, AWS Support l'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 del gruppo di sicurezza, consulta la sezione Gruppi di sicurezza Amazon EC2 nella Guida per l'utente di .

Per consentire la AWS Support connessione al gateway, devi prima accedere alla console locale dell'istanza Amazon EC2, accedere alla console di Storage Gateway e quindi fornire l'accesso.

Per attivare AWS Support l'accesso a un gateway distribuito su un'istanza Amazon EC2

1. Accedere alla console locale dell'istanza Amazon EC2. Per le relative istruzioni, consultare la sezione Connettersi all'istanza nella Guida utente Amazon EC2.

   Per accedere alla console locale dell´istanza EC2, è possibile utilizzare il seguente comando.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY* è il file `.pem` che contiene il certificato privato della coppia di chiavi EC2 utilizzata per avviare l´istanza Amazon EC2. Per ulteriori informazioni, consulta Recuperare la chiave pubblica della propria coppia di chiavi nella Guida per l'utente di Amazon EC2.
   > *INSTANCE-PUBLIC-DNS-NAME* è il nome pubblico sul DNS (Domain Name System) dell'istanza Amazon EC2 su cui è in esecuzione il gateway. È possibile ottenere questo nome pubblico su DNS selezionando l´istanza Amazon EC2; nella console EC2 e facendo clic sulla scheda Description (Descrizione).

2. Quando richiesto, immettere **`6 - Command Prompt`** per aprire la console del canale AWS Support .
3. Immettere **h** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Esegui una di queste operazioni:

   - Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.
   - Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

> **Note**
>
> Il numero del canale non è un numero di porta Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto in AWS Support modo da AWS Support poterti fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **q** per terminare. Non chiudere la sessione finché AWS Support non ti viene comunicato che la sessione di supporto è completa.
7. Accedere **`exit`** per uscire dalla console Storage Gateway.
8. Seguire i menu della console per uscire dall'istanza Storage Gateway.

Vuoi connetterti a un'istanza gateway tramite la Console seriale Amazon EC2

Puoi utilizzare la Console seriale Amazon EC2 per la risoluzione dei problemi di avvio, di configurazione di rete e di altro tipo. Per istruzioni e suggerimenti per la risoluzione dei problemi, consulta Console seriale Amazon EC2 nella Guida per l'utente di Amazon Elastic Compute Cloud.

Risoluzione dei problemi dell'appliance hardware

I seguenti argomenti illustrano i problemi che possono verificarsi con l'appliance hardaware Storage Gateway e i suggerimenti per risolverli.

Impossibile determinare l'indirizzo IP del servizio

Durante il tentativo di connessione al servizio, assicurarsi di utilizzare l'indirizzo IP del servizio e non l'indirizzo IP dell'host. Configurare l'indirizzo IP del servizio nella console di servizio e l'indirizzo IP dell'host nella console hardware. La console hardware viene visualizzata quando si avvia l'appliance hardware. Per accedere alla console di servizio dalla console hardware, scegliere Open Service Console (Apri console di servizio).

Come si esegue una reimpostazione ai valori di fabbrica?

Se è necessario reimpostare l'appliance ai valori di fabbrica, contattare il team dell'appliance hardware Storage Gateway per supporto, come descritto nella sezione di supporto seguente.

Come si esegue il riavvio remoto?

Se è necessario eseguire un riavvio remoto del dispositivo, è possibile farlo utilizzando l'interfaccia di gestione Dell iDRAC. Per ulteriori informazioni, vedere iDRAC9 Virtual Power Cycle: accensione remota dei PowerEdge server Dell EMC sul sito Web di Dell Technologies. InfoHub

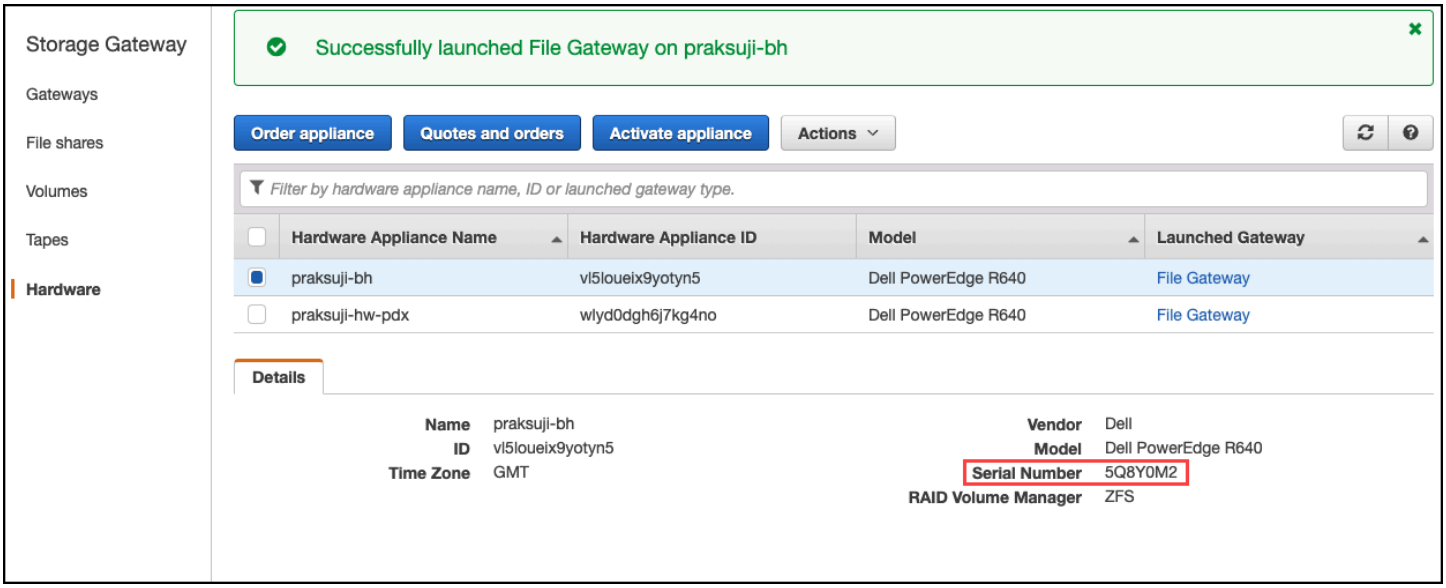
Dove si ottiene il supporto Dell iDRAC?

Il server Dell PowerEdge R640 è dotato dell'interfaccia di gestione Dell iDRAC. Consigliamo quanto segue:

- Se si utilizza l'interfaccia di gestione iDRAC, è necessario modificare la password predefinita. Per ulteriori informazioni sulle credenziali iDRAC, vedere PowerEdge Dell - Quali sono le credenziali di accesso predefinite per iDRAC? .
- Assicurati che il firmware up-to-date serva a prevenire violazioni della sicurezza.
- Spostare l'interfaccia di rete iDRAC su una porta normale (`em`) può causare problemi di prestazioni o prevenire il normale funzionamento dell'appliance.

Impossibile trovare il numero di serie dell'appliance hardware

Per trovare il numero di serie dell'appliance hardware, andare alla pagina Panoramica dell'appliance hardware nella console Storage Gateway, come illustrato di seguito.
Scheda hardware della console Storage Gateway con l'appliance selezionata e i dettagli visualizzati.



Scheda hardware della console Storage Gateway con l'appliance selezionata e i dettagli visualizzati.

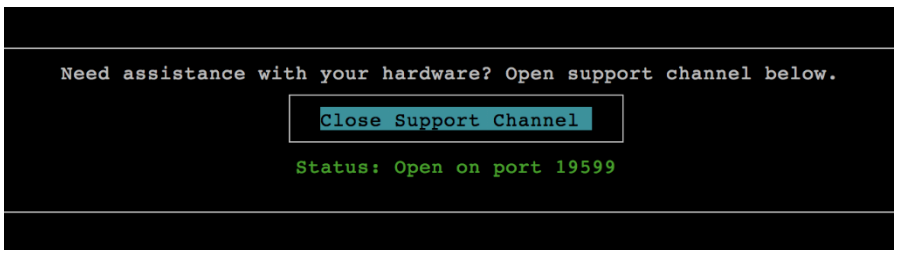
Dove ottenere supporto per l'appliance hardware

Per contattare il supporto per l'appliance hardware Storage Gateway, consulta AWS Support.

Il AWS Support team potrebbe chiederti di attivare il canale di supporto per risolvere i problemi relativi al gateway da remoto. Non è necessario che questa porta sia aperta per il normale funzionamento del gateway, ma è necessario per la risoluzione dei problemi. È possibile attivare il canale di supporto dalla console hardware, come illustrato nella procedura seguente.

Per aprire un canale di supporto per AWS

1. Aprire la console hardware.
2. Scegliere Open Support Channel (Apri canale di supporto) come mostrato di seguito.
   console dell'appliance hardware con lo stato del canale di supporto visualizzato.

   console dell'appliance hardware con lo stato del canale di supporto visualizzato.

   Il numero di porta assegnato dovrebbe essere visualizzato entro 30 secondi, se non ci sono problemi di connettività di rete o di firewall.

3. Annota il numero di porta e forniscilo a AWS Support.

Come risolvere i problemi dei nastri virtuali

Di seguito è spiegato cosa fare se si verificano problemi imprevisti nell'utilizzo dei nastri virtuali.

Argomenti

Recupero di un nastro virtuale da un gateway compromesso

Sebbene sia improbabile, il gateway di nastri virtuali potrebbe comunque imbattersi in un errore irreversibile. a livello dell'host dell'hypervisor, dei dischi della cache o del gateway stesso. Se si verifica un errore, è possibile recuperare i nastri attenendosi alle istruzioni per la risoluzione dei problemi illustrate in questa sezione.

Argomenti

È necessario recuperare un nastro virtuale da un gateway di nastri virtuali non funzionante

Se il tuo Tape Gateway o l'host dell'hypervisor riscontra un errore irreversibile, puoi ripristinare tutti i dati che sono già stati caricati su un altro Tape Gateway. AWS

Finché un nastro non risulta correttamente archiviato in VTS, i suoi dati potrebbero non essere completamente caricati. Tali dati dei nastri ripristinati su un altro gateway potrebbero quindi rivelarsi incompleti o mancanti. Pertanto, consigliamo di fare l'inventario di tutti i nastri recuperati per verificare che contengano quanto previsto.

Come recuperare un nastro su un gateway di nastri virtuali alternativo

1. Identificare un gateway di nastri virtuali funzionante da poter utilizzare come gateway di destinazione per il recupero. Qualora non vi fosse, creare un nuovo gateway di nastri virtuali per

il recupero dei nastri. Per informazioni su come creare un gateway, consulta Creazione di un gateway.

2. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
3. Nel riquadro di navigazione, scegliere Gateway e selezionare il gateway di nastri virtuali da cui recuperare i nastri.
4. Seleziona la scheda Details (Dettagli). Nella scheda compare un messaggio di recupero dei nastri.
5. Scegliere Crea nastri di recupero per disabilitare il gateway.
6. Nella finestra di dialogo visualizzata, selezionare Disable gateway (Disabilita gateway).

   Questa procedura compromette definitivamente la normale funzionalità del gateway di nastri virtuali ed espone tutti i punti di ripristino disponibili. Per le istruzioni, consulta Disattivazione del gateway di nastri virtuali.
7. Tra i nastri che il gateway disattivato mostra, scegliere il nastro virtuale e il punto di ripristino da recuperare. Un nastro virtuale può disporre di più punti di ripristino.
8. Per ripristinare un nastro su un gateway di nastri virtuali di destinazione, innanzitutto scegliere Crea nastro di recupero.
9. Nella finestra di dialogo Create recovery tape (Crea nastro di recupero), controllare il codice a barre del nastro virtuale da recuperare.
10. In Gateway, scegliere il gateway di nastri virtuali sul quale ripristinare il nastro virtuale.
11. Selezionare Create recovery tape (Crea nastro di recupero).
12. Eliminare il gateway di nastri virtuali inutilizzabile, per evitarne l'addebito. Per istruzioni, consulta Eliminazione del gateway tramite la console AWS Storage Gateway e rimozione delle risorse associate.

Storage Gateway sposta il nastro dal gateway di nastri virtuali guasto al gateway di nastri virtuali specificato. Il gateway di nastri virtuali contrassegna il nastro con lo stato RECUPERATO.

È necessario recuperare un nastro virtuale da un disco della cache non funzionante

Se il disco della cache restituisce un errore, il gateway impedisce le operazioni di lettura e di scrittura sui suoi nastri virtuali. Un errore può generarsi, ad esempio, se un disco è danneggiato o è stato rimosso dal gateway. La console Storage Gateway, in tal caso, mostra un messaggio relativo all'errore.

Nel messaggio di errore, Storage Gateway richiede di eseguire una delle due operazioni con cui è possibile recuperare i nastri:

- Arresta e aggiungi di nuovo i dischi: l'approccio suggerito se è stato rimosso un disco con dati non danneggiati. Se la generazione dell'errore è dovuta, ad esempio, alla rimozione accidentale dall'host di un disco con dati intatti, è possibile riaggiungere il disco. La procedura del caso è illustrata più avanti in questo argomento.
- Reimposta disco della cache: l'approccio suggerito se il disco della cache è danneggiato o non accessibile. Se viene generato un errore che ne causa l'inaccessibilità, l'inutilità o il danneggiamento, il disco della cache può essere reimpostato. Se si reimposta il disco della cache, i nastri con dati puliti (ovvero, quelli per i quali i dati nel disco della cache e in Amazon S3 sono sincronizzati) continueranno a essere disponibili per l'uso. Tuttavia, i nastri con dati non sincronizzati con Amazon S3 vengono ripristinati automaticamente. Lo stato di questi nastri è impostato su RECUPERATO, ma i nastri saranno di sola lettura. Per informazioni su come rimuovere un disco dall'host, consulta Determinazione delle dimensioni del buffer di caricamento da allocare.

  > **Important**
  >
  > I dati contenuti nel disco della cache reimpostato e non ancora caricati su Amazon S3 potrebbero andare perduti. La reimpostazione comporta la perdita dei dischi della cache precedentemente configurati nel gateway; pertanto, occorrerà configurare almeno un nuovo disco della cache per il gateway, affinché funzioni correttamente.

  Per reimpostare il disco della cache, attieniti alla procedura riportata più avanti in questo argomento.

Come arrestare e riaggiungere un disco

1. Arresta il gateway. Per informazioni su come arrestare un gateway, consulta Spegnimento della macchina virtuale gateway.
2. Riaggiungere il disco all'host e accertarsi che il numero del nodo del disco non sia cambiato. Per informazioni su come aggiungere un disco, consulta Determinazione delle dimensioni del buffer di caricamento da allocare.
3. Riavviare il gateway. Per informazioni su come riavviare un gateway, consulta Spegnimento della macchina virtuale gateway.

Dopo il riavvio del gateway, è possibile verificare lo stato dei dischi della cache, che può essere uno dei seguenti:

- present (presente): il disco è disponibile per l'uso.
- missing (mancante): il disco non è più connesso al gateway.
- mismatch (incongruente): il nodo del disco è occupato da un disco con metadati errati o i contenuti del disco sono danneggiati.

Come reimpostare e riconfigurare un disco della cache

1. Nel messaggio di errore A disk error has occurred (Si è verificato un errore del disco) illustrato in precedenza, selezionare Reset Cache Disk (Reimposta disco della cache).
2. Dalla pagina Configurazione del gateway, configurare il disco per lo storage della cache. Per informazioni su come farlo, consulta Configurazione del gateway di nastri virtuali.
3. Dopo aver configurato lo storage della cache, arrestare e riavviare il gateway, come descritto nella procedura precedente.

Il gateway dovrebbe procedere al recupero dopo il riavvio, in seguito al quale è possibile verificare lo stato del disco della cache.

Come verificare lo stato del disco della cache

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, scegliere Gateways (Gateway) e selezionare il proprio gateway.
3. Dal menu Actions (Operazioni), selezionare Configure Local Storage (Configura lo storage locale) per visualizzare la finestra di dialogo Configure Local Storage (Configura lo storage locale). Questa finestra di dialogo mostra tutti i dischi locali del gateway.

Lo stato relativo al nodo del disco della cache viene visualizzato accanto al disco.

> **Note**
>
> Se non si completa la procedura di ripristino, il gateway mostra un banner che richiede di configurare lo storage locale.

Come risolvere i problemi relativi ai nastri irrecuperabili

Se inaspettatamente un nastro virtuale diviene inutilizzabile, Storage Gateway ne imposta lo stato su IRRECUPERABILE. L'operazione da compiere successivamente dipende dalle circostanze. Il paragrafo che segue illustra alcuni problemi in cui ci si potrebbe imbattere con relative soluzioni.

È necessario recuperare dati da un nastro IRRECUPERABILE

Per utilizzare un nastro virtuale contrassegnato dallo stato IRRECUPERABILE, procedere come di seguito:

- Attivare un nuovo gateway di nastri virtuali se non si dispone di gateway attivi. Per ulteriori informazioni, consulta Creazione di un gateway.
- Disattivare il gateway di nastri virtuali contenente il nastro irrecuperabile e ripristinare il nastro da un punto di ripristino sul nuovo gateway di nastri virtuali. Per ulteriori informazioni, consulta È necessario recuperare un nastro virtuale da un gateway di nastri virtuali non funzionante.

> **Note**
>
> Per utilizzare il nuovo gateway di nastri virtuali bisogna riconfigurare l'iniziatore iSCSI e l'applicazione di backup. Per ulteriori informazioni, consulta Connessione dei dispositivi VTL.

Non occorre un nastro IRRECUPERABILE che non è stato archiviato

Un nastro virtuale con lo stato IRRECUPERABILE, inutile e mai archiviato, dovrebbe essere eliminato. Per ulteriori informazioni, consulta Eliminazione di nastri.

Un disco della cache nel gateway rileva un errore

Se uno o più dischi della cache nel gateway restituiscono un errore, il gateway impedisce le operazioni di lettura e di scrittura su nastri virtuali e volumi. Per ripristinare la normale funzionalità, riconfigura il gateway come descritto di seguito:

- Se il disco della cache è inaccessibile o inutilizzabile, eliminalo dalla configurazione del gateway.
- Se il disco della cache è ancora accessibile e utilizzabile, ricollegalo al gateway.

> **Note**
>
> Se elimini un disco della cache, i nastri virtuali o i volumi con dati puliti (ovvero, per i quali i dati nel disco della cache e Amazon S3 sono sincronizzati) continueranno a essere disponibili quando il gateway riprenderà la normale funzionalità. Ad esempio, se il gateway ha tre dischi della cache e ne elimini due, i nastri virtuali o i volumi puliti avranno lo stato DISPONIBILE. Gli altri nastri virtuali e volumi avranno lo stato IRRECUPERABILE.
> Se si utilizzano dischi temporanei come dischi della cache per il gateway o si montano i dischi della cache su un'unità temporanea, i dischi della cache andranno persi quando si spegne il gateway. Lo spegnimento del gateway quando il disco della cache e Amazon S3 non sono sincronizzati può causare la perdita di dati. Di conseguenza, non è consigliato l'uso di unità o dischi temporanei.

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 Risoluzione dei problemi relativi alla disponibilità elevata.

Risoluzione dei problemi relativi alla disponibilità elevata

Di seguito sono riportate le informazioni sulle azioni da intraprendere in caso di problemi di disponibilità.

Argomenti

Notifiche di stato

Quando esegui il gateway su VMware vSphere HA, tutti i gateway generano le seguenti notifiche di integrità per il gruppo di log Amazon configurato. CloudWatch Queste notifiche vengono inserite in un flusso di log chiamato `AvailabilityMonitor`.

Argomenti

Notifica: riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console di gestione VM Hypervisor o la console Storage Gateway. È inoltre possibile riavviare utilizzando il software del gateway durante il ciclo di manutenzione del gateway.

Operazione da eseguire

Se il riavvio viene eseguito entro 10 minuti dall'ora di avvio della manutenzione configurata del gateway, probabilmente si tratta di un evento normale e non un'indicazione di problema. Se il riavvio è stato eseguito al di fuori della finestra di manutenzione in modo significativo, verifica se il gateway è stato riavviato manualmente.

Notifica: HardReboot

Puoi ricevere una notifica `HardReboot` quando la VM del gateway viene riavviata in modo imprevisto. Questo riavvio può essere dovuto a mancanza di alimentazione, a un guasto hardware o a un altro evento. Per i gateway VMware, un ripristino da parte di vSphere High Availability Application Monitoring può avviare 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.

Notifica: 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, contatta AWS Support.

Notifica: AvailabilityMonitorTest

Per un gateway su VMware vSphere HA, puoi ricevere una notifica `AvailabilityMonitorTest` quando esegui un test del sistema di disponibilità e monitoraggio delle applicazioni in VMware.

Metriche

Il parametro `AvailabilityNotifications` è disponibile in tutti i gateway. Questo parametro è il conteggio del numero di notifiche di stato relative alla disponibilità generate dal gateway. Utilizza la statistica `Sum` per verificare se il gateway sta riscontrando eventi correlati alla disponibilità. Per informazioni dettagliate sugli eventi, rivolgiti CloudWatch al gruppo di log configurato.

Best practice per il ripristino dei dati

Sebbene improbabile, si potrebbe verificare un errore irreversibile del gateway. Tale errore può verificarsi nella macchina virtuale (VM), nel gateway stesso, nello storage locale o in altre posizioni. Se si verifica un errore, è consigliabile seguire le istruzioni nella sezione appropriata di seguito per ripristinare i dati.

> **Important**
>
> Storage Gateway non supporta il ripristino di una macchina virtuale del gateway da uno snapshot creato dall'hypervisor o dall'Amazon Machine Image (AMI) di Amazon EC2. Se la macchina virtuale del gateway non funziona correttamente, attiva un nuovo gateway e ripristina i dati in tale gateway in base alle istruzioni seguenti.

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 Verifica della connessione del gateway a Internet.
- Per le configurazioni con e nastri, quando il gateway diventa raggiungibile i o i nastri passano allo stato BOOTSTRAPPING (PROCESSO DI BOOTSTRAP). Questa funzionalità garantisce che i dati archiviati localmente continuino a essere sincronizzati con AWS. Per ulteriori informazioni su questo stato, consulta Comprendere lo stato del nastro.
- 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 gateway o una macchina virtuale malfunzionante

Se il gateway di nastri virtuali o l'host hypervisor rileva un errore irreversibile, è possibile usare le fasi seguenti per ripristinare i nastri dal gateway di nastri virtuali malfunzionante in un altro gateway di nastri virtuali:

1. Identificare il gateway di nastri virtuali da usare come destinazione per il ripristino oppure crearne uno nuovo.
2. Disattiva il gateway malfunzionante.
3. Creare nastri di ripristino per ogni nastro da ripristinare e specificare il gateway di nastri virtuali di destinazione.

4. Eliminare il gateway di nastri virtuali malfunzionante.

Per informazioni dettagliate su come ripristinare i nastri da un gateway di nastri virtuali malfunzionante in un altro gateway di nastri virtuali, consulta È necessario recuperare un nastro virtuale da un gateway di nastri virtuali non funzionante.

Ripristino dei dati da un nastro irrecuperabile

Se si verifica un errore nel nastro e lo stato è IRRECUPERABILE, è consigliabile usare una delle opzioni seguenti per ripristinare i dati o risolvere l'errore, in base alla situazione:

- Se i dati sul nastro irrecuperabile sono necessari, è possibile ripristinare il nastro in un nuovo gateway.
- Se i dati sul nastro non sono necessari e il nastro non è mai stato archiviato, è possibile semplicemente eliminare il nastro dal gateway di nastri virtuali.

  Per informazioni dettagliate su come ripristinare i dati o risolvere l'errore se il nastro ha lo stato IRRECUPERABILE, consulta Come risolvere i problemi relativi ai nastri irrecuperabili.

Ripristino dei dati da un disco della cache malfunzionante

Se nel disco della cache si verifica un errore, è consigliabile usare le opzioni seguenti per ripristinare i dati, in base alla situazione:

- Se il malfunzionamento si è verificato perché un disco della cache è stato rimosso dall'host, arresta il gateway, aggiungi di nuovo il disco e riavvia il gateway.
- 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, consulta È necessario recuperare un nastro virtuale da un disco della cache non funzionante.

Ripristino dei dati da un data center inaccessibile

Se il gateway o il data center diventa inaccessibile per qualsiasi motivo, è possibile ripristinare i dati in un altro gateway in un data center diverso oppure in un gateway ospitato in un'istanza Amazon EC2.

Se non hai accesso a un altro data center, è consigliabile creare il gateway in un'istanza Amazon EC2. Le fasi da seguire dipendono dal tipo di gateway da cui vengono ripristinati i dati.

Per ripristinare i dati da un gateway di nastri virtuali in un data center inaccessibile

1. Creare e attivare un nuovo gateway di nastri virtuali in un host Amazon EC2. Per ulteriori informazioni, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali.
2. Ripristinare i nastri dal gateway di origine nel data center nel nuovo gateway creato in Amazon EC2. Per ulteriori informazioni, consulta Recupero di un nastro virtuale da un gateway compromesso.

   I nastri verranno rispristinati nel nuovo gateway Amazon EC2.

Risorse Storage Gateway aggiuntive

Questa sezione descrive software, strumenti AWS e risorse di terze parti che possono aiutarti a configurare o gestire il gateway e anche le quote dello Storage Gateway.

Argomenti

Configurazione dell'host

Argomenti

Configurazione di VMware per Storage Gateway

Nel configurare VMware per 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

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).

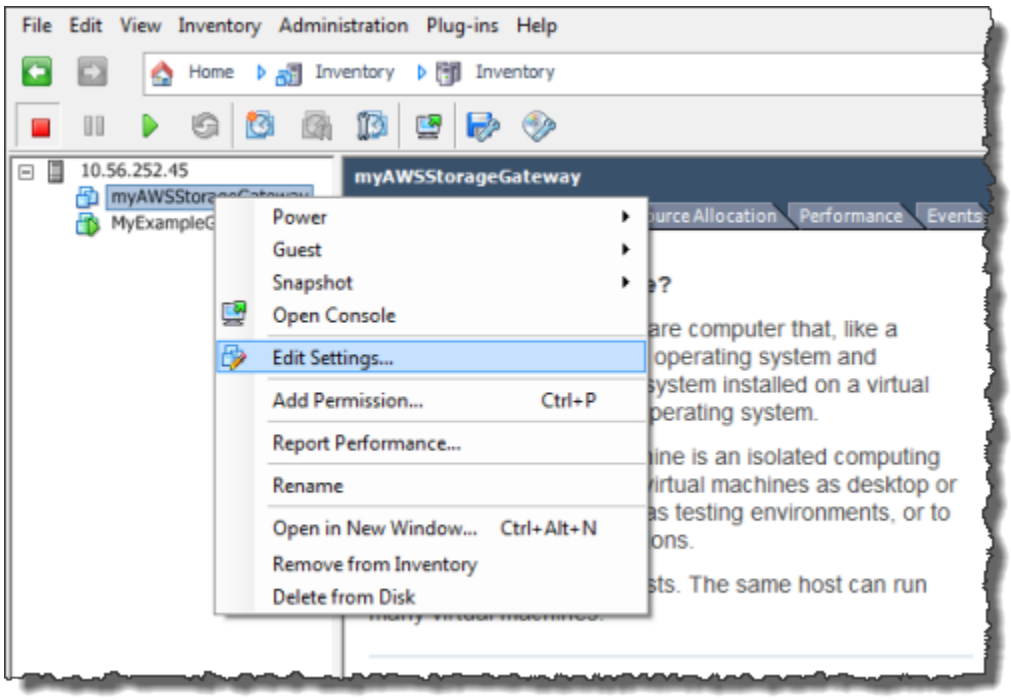
> **Important**
>
> La sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host è necessaria per una corretta attivazione del gateway.

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).

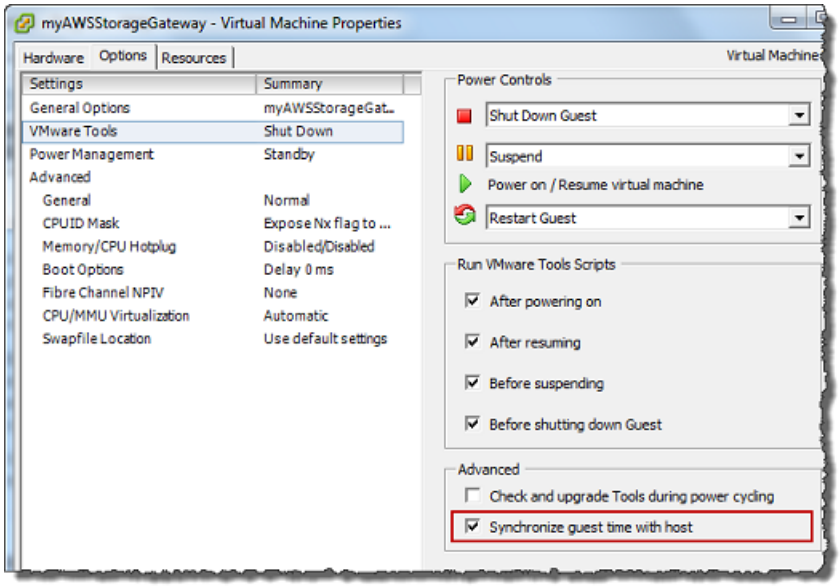
      Viene visualizzata la finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale).



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.



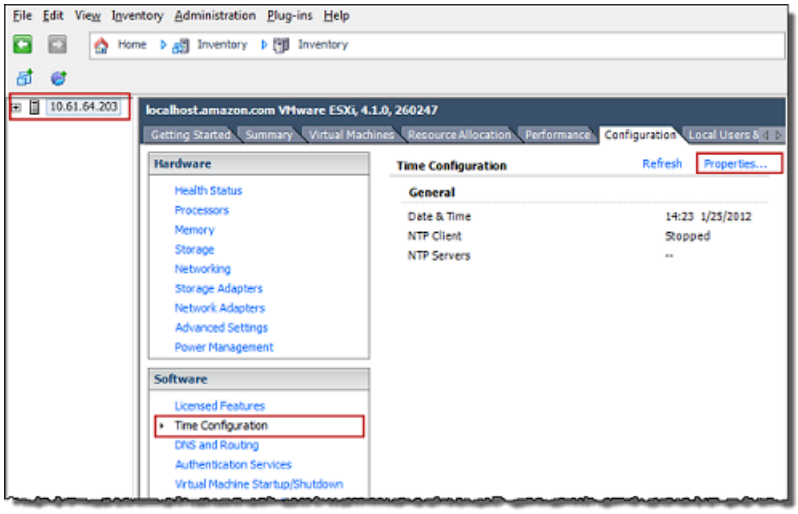
2. Configurare la data e l'ora dell'host.

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.

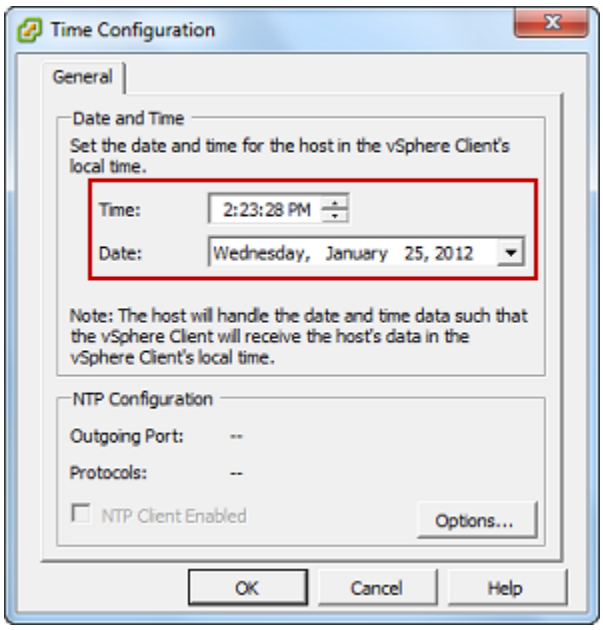
a. Nel client VMware vSphere selezionare il nodo host vSphere nel riquadro a sinistra e quindi scegliere la scheda Configuration (Configurazione).

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).

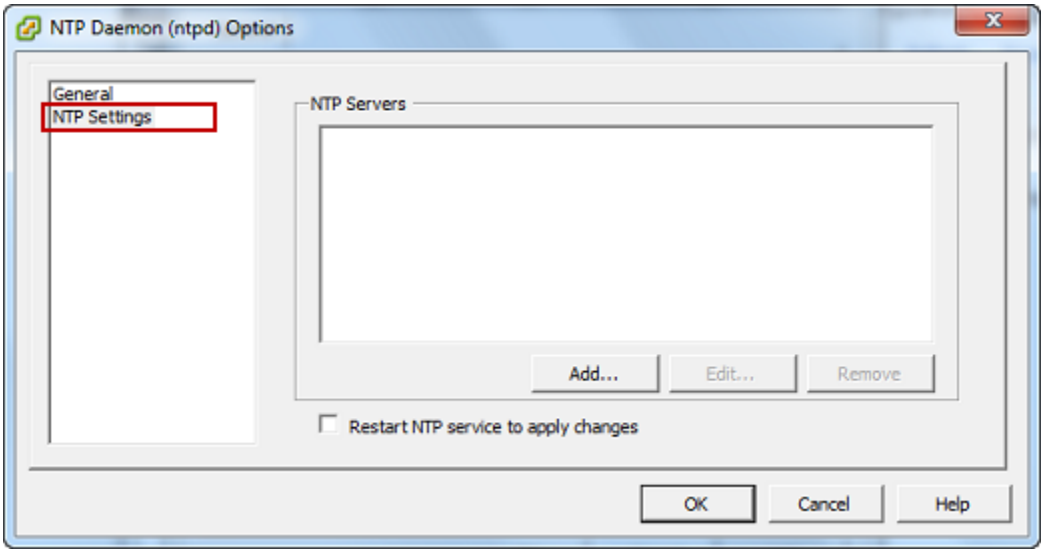


c. Nel pannello Date and Time (Data e ora) impostare la data e l'ora.



d. Configurare l'host per la sincronizzazione automatica di data e ora con un server NTP.

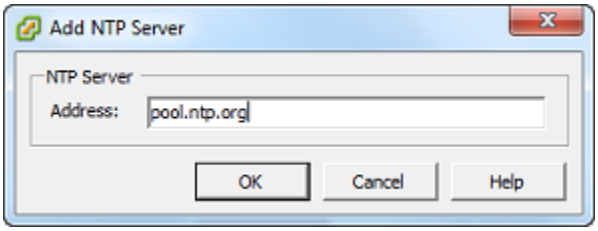
   i. Scegliere Options (Opzioni) nella finestra di dialogo Time Configuration (Configurazione data e ora) e quindi nella finestra di dialogo NTP Daemon (ntpd) (Daemon NTP - ntpd) scegliere NTP Settings (Impostazioni NTP) nel riquadro a sinistra.



   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.

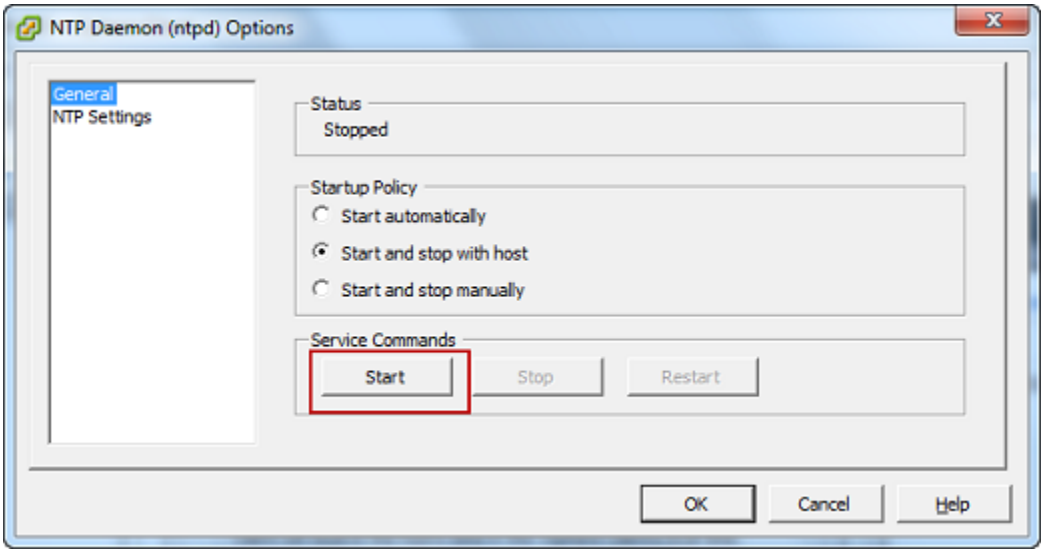
   È possibile usare `pool.ntp.org` come mostrato nell'esempio seguente.



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).

Configurazione della macchina AWS Storage Gateway virtuale per l'utilizzo di controller di disco paravirtualizzati

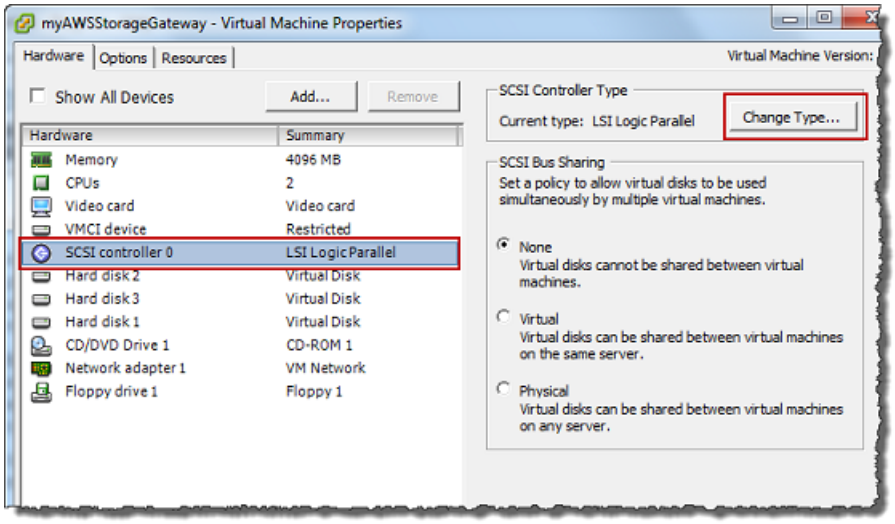
In questa attività imposterai il controller iSCSI in modo che la macchina virtuale usi la paravirtualizzazione. La paravirtualizzazione è una modalità in cui la macchina virtuale del gateway

opera con il sistema operativo host in modo che la console possa identificare i dischi aggiunti alla macchina virtuale.

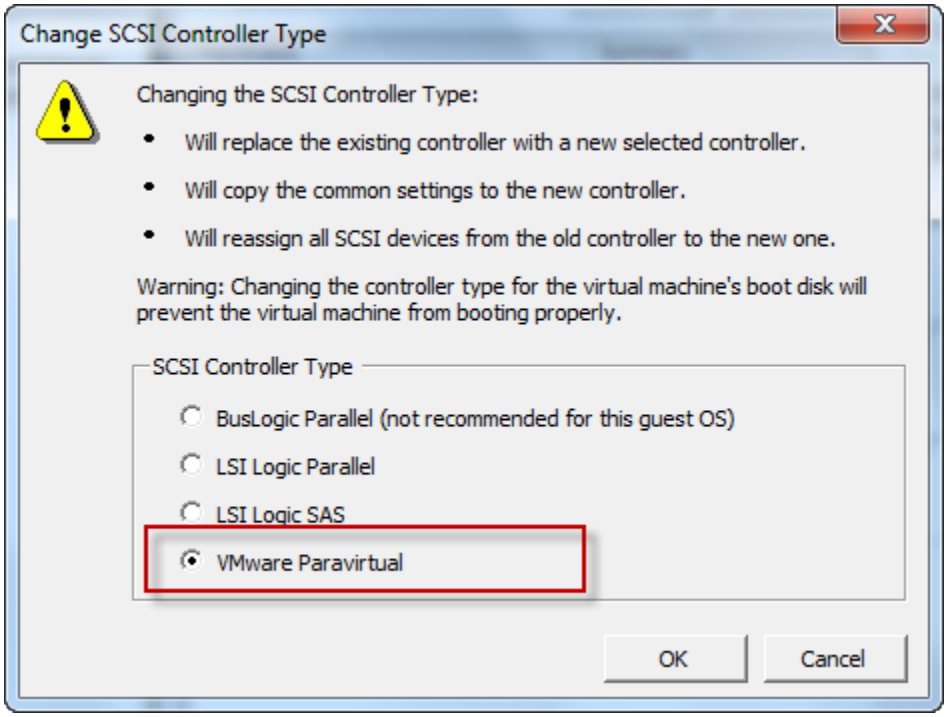
> **Note**
>
> Devi completare questa procedura per evitare problemi di identificazione dei dischi quando li configuri nella console del gateway.

Per configurare la macchina virtuale per l'uso di controller paravirtualizzati

1. Nel client VMware vSphere aprire il menu contestuale (clic con il pulsante destro del mouse) per la macchina virtuale del gateway e quindi scegliere Edit Settings (Modifica impostazioni).
2. Nella finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale) scegliere la scheda Hardware, selezionare SCSI controller 0 (Controller SCSI 0)e quindi scegliere Change Type (Cambia tipo).



3. Nella finestra di dialogo Change SCSI Controller Type (Cambia tipo di controller SCSI) selezionare VMware Paravirtual (Paravirtuale VMware) e quindi scegliere OK.



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, consulta VMware HA: Concepts and Best Practices sul sito web VMware.

Per usare Storage Gateway con VMware HA, ti consigliamo di svolgere queste operazioni:

- Distribuire il pacchetto scaricabile VMware ESX `.ova` che contiene la macchina virtuale Storage Gateway su un solo host in un cluster.
- Quando si distribuisce il pacchetto `.ova`, selezionare un 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.
- Per impedire che l'iniziatore si disconnetta dalle destinazioni dei volumi di storage durante il failover, seguire le impostazioni iSCSI consigliate per il proprio sistema operativo. Nel caso di un failover, può richiedere da pochi secondi ad alcuni minuti per avviare una macchina

virtuale gateway su un nuovo host nel cluster di failover. I timeout iSCSI consigliati per i client Windows e Linux superano i tempi tipici necessari per un failover. Per ulteriori informazioni sulla personalizzazione delle impostazioni del timeout dei client Windows, consulta Personalizzazione delle impostazioni iSCSI di Windows. Per ulteriori informazioni sulla personalizzazione delle impostazioni del timeout dei client Linux, consulta Personalizzazione delle impostazioni iSCSI di Linux.

- 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

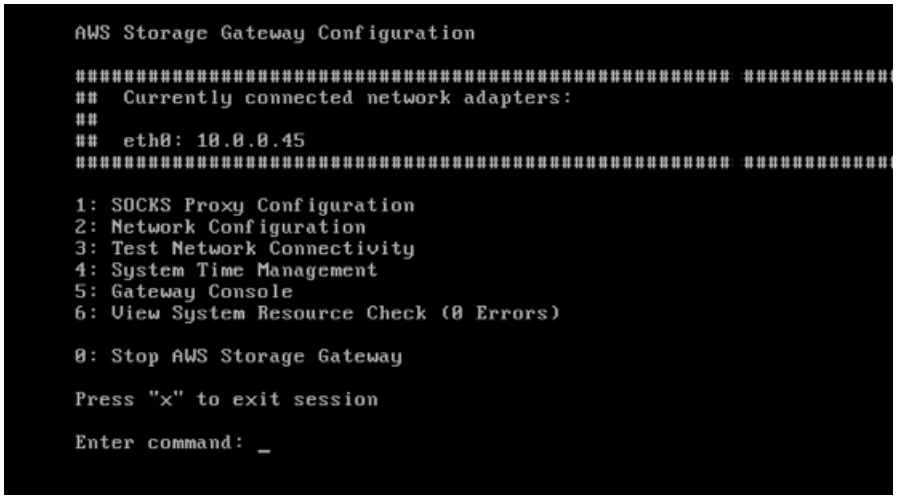
In caso di gateway distribuito su VMware ESXi, per evitare scostamenti temporali basta impostare l'ora dell'host dell'hypervisor e sincronizzazione l'ora della VM con quella dell'host. Per ulteriori informazioni, consulta Sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host. 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)

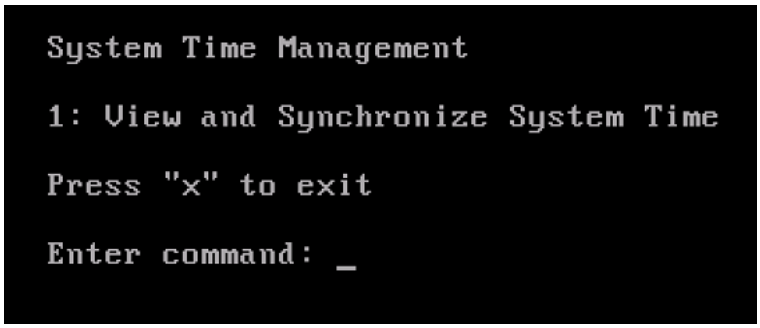
1. Accedere alla console locale del gateway:

   - 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. Nel menu principale Configurazione di Storage Gateway digitare **4** per Gestione ora di sistema.



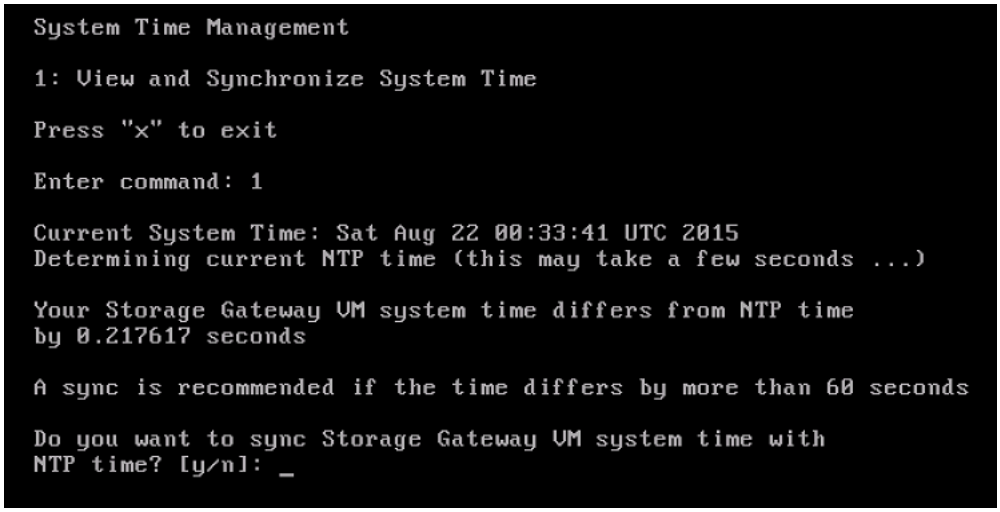
3. Nel menu System Time Management (Gestione ora di sistema), digitare **1** per View and Synchronize System Time (Visualizza e sincronizza ora di sistema).



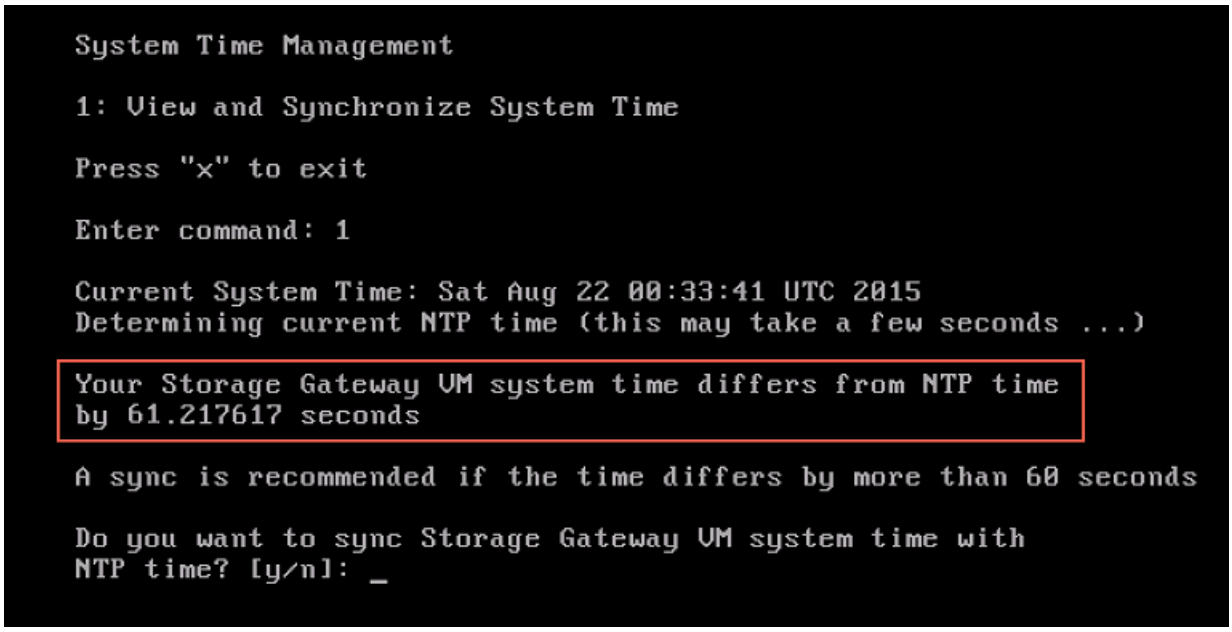
4. Se il risultato indica che è necessario sincronizzare l'ora della macchina virtuale con l'ora NTP, digitare **y**. In caso contrario, inserire **n**.

   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.



Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali

Puoi distribuire e attivare un gateway di nastri virtuali su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) del AWS Storage Gateway è disponibile come AMI della community.

> **Note**
>
> Le AMI della community Storage Gateway sono pubblicate e completamente supportate da AWS. Puoi vedere che l'editore è AWS un fornitore verificato.

Per implementare un'istanza Amazon EC2 per ospitare il gateway di nastri virtuali

1. Inizia a configurare un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, vedere Configurare un gateway di nastri virtuali. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come Piattaforma host, quindi segui i passaggi seguenti per avviare l'istanza Amazon EC2 che ospiterà il gateway di nastri virtuali.
2. Scegli Launch instance per aprire il modello AWS Storage Gateway AMI nella console Amazon EC2, dove puoi configurare impostazioni aggiuntive.

   Usa Quicklaunch per avviare l'istanza Amazon EC2 con le impostazioni predefinite. Per ulteriori informazioni sulle specifiche predefinite di Amazon EC2 Quicklaunch, consulta Specifiche di configurazione di Quicklaunch per Amazon EC2.
3. Per Nome, inserire un nome per l'istanza Amazon EC2. Dopo aver distribuito l'istanza, puoi cercare questo nome per trovare l'istanza nelle pagine di elenco nella console Amazon EC2.
4. Nella sezione Tipo di istanza, per Tipo di istanza scegli la configurazione hardware per l'istanza. La configurazione hardware deve soddisfare determinati requisiti minimi per supportare il gateway. Consigliamo di iniziare con il tipo di istanza m5.xlarge, che soddisfa i requisiti minimi di hardware per il funzionamento corretto del gateway. Per ulteriori informazioni, consulta Requisiti per i tipi di istanze Amazon EC2.

   È possibile ridimensionare l'istanza dopo l'avvio, se necessario. Per ulteriori informazioni, consulta Ridimensionamento dell'istanza nella Guida per l'utente di Amazon EC2 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 di nastri virtuali; ad esempio, è possibile perdere i dati dalla cache. Monitora la CloudWatch metrica di `CachePercentDirty` Amazon e avvia o arresta il sistema solo quando tale parametro

lo è0. Per ulteriori informazioni sui parametri di monitoraggio per il gateway, consulta Metriche e dimensioni dello Storage Gateway nella CloudWatch documentazione.

5. Nella sezione Coppia di chiavi (accesso), in Nome coppia di chiavi: obbligatorio, seleziona la coppia di chiavi che desideri utilizzare per connetterti in modo sicuro alla tua istanza. Se necessario, puoi creare una nuova coppia di key pair. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux.
6. Nella sezione Impostazioni di rete, rivedi le impostazioni preconfigurate e scegli Modifica per apportare modifiche ai seguenti campi:
   a. Per VPC, obbligatorio, scegli il VPC in cui vuoi lanciare l'istanza Amazon EC2. Per ulteriori informazioni, consulta Come funziona Amazon VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
   b. (Facoltativo) Per Subnet, scegli la sottorete in cui vuoi lanciare l'istanza Amazon EC2.
   c. Per Assegna automaticamente IP pubblico, scegli Abilita.
7. Nella sottosezione Firewall (gruppi di sicurezza), esamina le impostazioni preconfigurate. Puoi modificare il nome e la descrizione predefiniti del nuovo gruppo di sicurezza da creare per la tua istanza Amazon EC2, se lo desideri, oppure scegliere di applicare le regole firewall di un gruppo di sicurezza esistente.
8. Nella sottosezione sulle regole dei gruppi di sicurezza in entrata, aggiungi le regole del firewall per aprire le porte che i client utilizzeranno per connettersi alla tua istanza. Per ulteriori informazioni sulle porte richieste per gateway di nastri virtuali, consulta Requisiti delle porte . Per ulteriori informazioni sull'aggiunta di regole firewall, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Linux.

   > **Note**
   >
   > Il gateway di nastri virtuali richiede che la porta TCP 80 sia aperta per il traffico in entrata e per l'accesso HTTP una tantum durante l'attivazione del gateway. Dopo l'attivazione, è possibile chiudere questa porta.
   > Inoltre, è necessario aprire la porta TCP 3260 per l'accesso iSCSI.

9. Nella sottosezione Configurazione di rete avanzata, rivedete le impostazioni preconfigurate e, se necessario, apportate le modifiche.

10. Nella sezione Configura archiviazione scegliere Aggiungi nuovo volume per aggiungere spazio di archiviazione all'istanza del gateway.

    > **Important**
    >
    > È necessario aggiungere almeno un volume Amazon EBS con almeno 165 GiB di capacità per lo storage della cache e almeno un volume Amazon EBS con almeno 150 GiB di capacità per il buffer di caricamento, oltre al volume root preconfigurato. Per migliorare le prestazioni, consigliamo di allocare più volumi EBS per lo storage della cache con almeno 150 GiB ciascuno.

11. Nella sezione Dettagli avanzati, rivedi le impostazioni preconfigurate e apporta le modifiche se necessario.
12. Scegli Avvia istanza per avviare la nuova istanza gateway Amazon EC2 con le impostazioni configurate.
13. Per verificare che la tua nuova istanza sia stata lanciata correttamente, vai alla pagina Istanze nella console Amazon EC2 e cerca la tua nuova istanza per nome. Assicurati che lo stato dell'istanza sia visualizzato in esecuzione con un segno di spunta verde e che il controllo dello stato sia completo e mostri un segno di spunta verde.
14. Selezionare l'istanza dalla pagina dei dettagli. Copia l'indirizzo IPv4 pubblico dalla sezione di riepilogo dell'istanza, quindi torna alla pagina Configura gateway nella console Storage Gateway per riprendere la configurazione del gateway di nastri virtuali.

È possibile determinare l'ID AMI da utilizzare per avviare un Tape Gateway utilizzando la console Storage Gateway o interrogando l'archivio AWS Systems Manager dei parametri.

Per determinare l'ID AMI, procedi in uno dei seguenti modi:

- Inizia a configurare un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, vedere Configurare un gateway di nastri virtuali. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi scegli Launch instance per aprire il modello AWS Storage Gateway AMI nella console Amazon EC2.

  Verrai reindirizzato alla pagina AMI della community EC2, dove puoi vedere l'ID AMI per la tua AWS regione nell'URL.
- Esegui una query sull'archivio dei parametri Systems Manager. È possibile utilizzare l'API AWS CLI o Storage Gateway per interrogare il parametro pubblico Systems Manager nello spazio dei

nomi/`aws/service/storagegateway/ami/VTL/latest`. Ad esempio, l'utilizzo del seguente comando CLI restituisce l'ID dell'AMI corrente nel campo Regione AWS specificato.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/
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/VTL/
latest",
        "Name": "/aws/service/storagegateway/ami/VTL/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Implementazione di Amazon EC2 con impostazioni predefinite

Questo argomento elenca i passaggi per implemetare un host Amazon EC2 utilizzando le specifiche predefinite.

Puoi implementare e attivare un gateway di nastri virtuali su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'Amazon Machine Image (AMI) di AWS Storage Gateway è disponibile come AMI della community.

> **Note**
>
> Le AMI della community Storage Gateway sono pubblicate e completamente supportate da AWS. Puoi vedere che l'editore è AWS un fornitore verificato.

1. Per configurare l'istanza Amazon EC2, scegli Amazon EC2 come piattaforma host nella sezione Opzioni piattaforma del flusso di lavoro. Per istruzioni sulla configurazione dell'istanza Amazon EC2, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali.

2. Seleziona Launch instance per aprire il modello AMI AWS Storage Gateway nella console Amazon EC2 e personalizzare impostazioni aggiuntive come tipi di istanza, impostazioni di rete e Configura storage.
3. Facoltativamente, puoi selezionare Usa le impostazioni predefinite nella console Storage Gateway per implemetare un'istanza Amazon EC2 con la configurazione predefinita.

   L'istanza Amazon EC2 creata da Usa le impostazioni predefinite ha le seguenti specifiche predefinite:

   - Tipo di istanza: m5.xlarge
   - Impostazioni di rete
     - Per VPC, seleziona il VPC nel quale desideri che venga eseguita l'istanza EC2.
     - Per Sottorete, specifica la sottorete in cui deve essere avviata l'istanza EC2.

     > **Note**
     >
     > Le sottoreti VPC verranno visualizzate nel menu a discesa solo se hanno l'impostazione di assegnazione automatica dell'indirizzo IPv4 pubblico attivata dalla console di gestione VPC.

     - Assegnazione automatica di IP pubblico: attivata

   Un gruppo di sicurezza EC2 viene creato e associato all'istanza EC2. Il gruppo di sicurezza presenta le seguenti regole per la porta in ingresso:

   > **Note**
   >
   > È necessario che la porta 80 sia aperta durante l'attivazione del gateway. La porta viene chiusa immediatamente dopo l'attivazione. Successivamente, è possibile accedere all'istanza EC2 solo tramite le altre porte del VPC selezionato.
   > Le destinazioni iSCSI sul gateway sono accessibili solo dagli host nello stesso VPC del gateway. Se è necessario accedere alle destinazioni iSCSI da host esterni al VPC, è necessario aggiornare le regole del gruppo di sicurezza appropriate.
   > Puoi modificare i gruppi di sicurezza in qualsiasi momento accedendo alla pagina dei dettagli dell'istanza Amazon EC2, selezionando Sicurezza, accedendo a Dettagli del gruppo di sicurezza e scegliendo l'ID del gruppo di sicurezza.

Porta	Protocollo	Protocollo del file system				
80	TCP	Accesso HTTP per l'attivazione				
3260	TCP	iSCSI				

- Configurare l'archiviazione

Impostazioni predefinite	Volume root AMI	Cache del volume 2	Cache del volume 3			
Nome dispositivo		'/dev/sdb'	'/dev/sdc'			
Size	80 Gib	165 GiB	150 GiB			
Tipo di volume	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Elimina al termine	Sì	Sì	Sì			
Crittografato	No	No	No			
Prestazioni	125	125	125			

Modifica le opzioni dei metadati delle istanze Amazon EC2

Il servizio di metadati dell'istanza (IMDS) è un componente su istanza che fornisce un accesso sicuro ai metadati delle istanze Amazon EC2. Un'istanza può essere configurata per accettare richieste di metadati in entrata che utilizzano IMDS versione 1 (IMDSv1) o richiedere che tutte le richieste di metadati utilizzino IMDS versione 2 (IMDSv2). IMDSv2 utilizza le richieste orientate alla sessione e attenua diversi tipi di vulnerabilità che potrebbero essere utilizzate per tentare di accedere a IMDS. Per informazioni su IMDSv2, consulta How Instance Metadata Service Version 2 nella Amazon Elastic Compute Cloud User Guide.

Ti consigliamo di richiedere IMDSv2 per tutte le istanze Amazon EC2 che ospitano Storage Gateway. IMDSv2 è richiesto per impostazione predefinita su tutte le istanze gateway appena lanciate. Se disponi di istanze esistenti che sono ancora configurate per accettare richieste di metadati IMDSv1, consulta Richiedi l'uso di IMDSv2 nella Amazon Elastic Compute Cloud User Guide per istruzioni su come modificare le opzioni di metadati dell'istanza per richiedere l'uso di IMDSv2. L'applicazione di questa modifica non richiede il riavvio dell'istanza.

Gateway di nastri virtuali

Argomenti

Rimozione di dischi dal gateway

Anche se non consigliamo di rimuovere i dischi sottostanti dal gateway, è possibile rimuovere i dischi dal gateway, ad esempio in caso di errore di un disco.

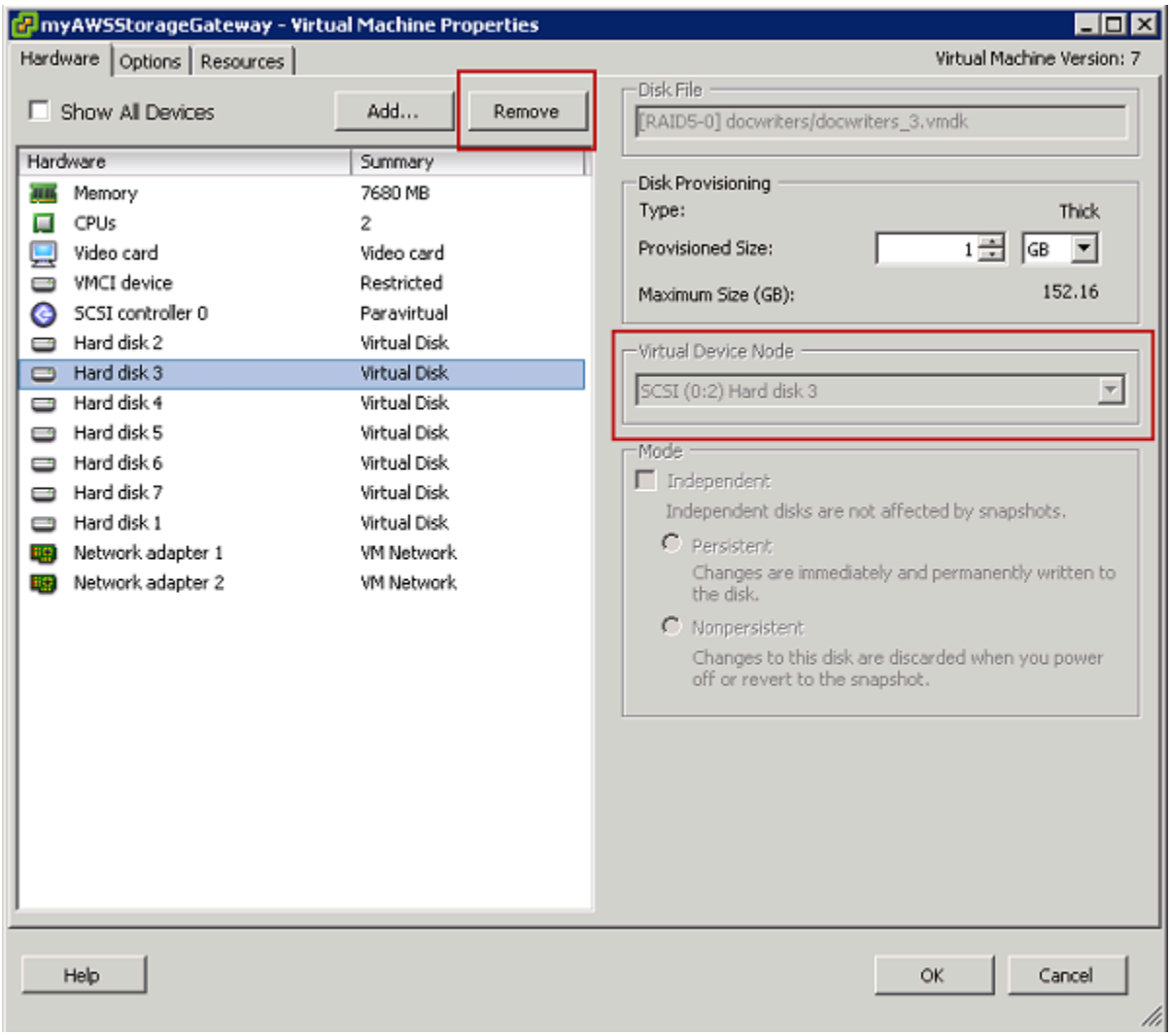
Rimozione di un disco da un gateway ospitato su VMware ESXi

Puoi utilizzare la procedura seguente per rimuovere un disco dal gateway ospitato su un hypervisor VMware.

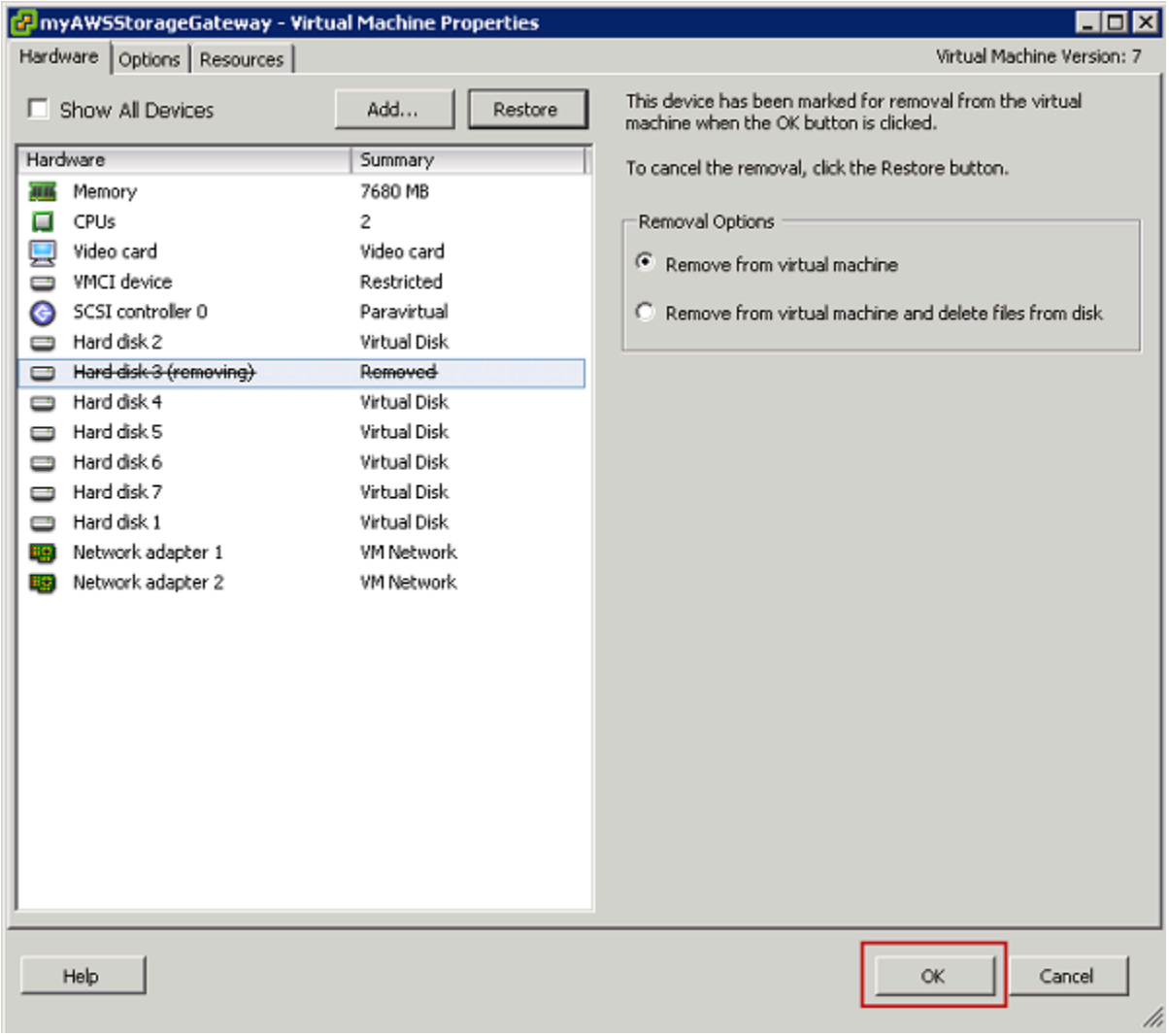
Per rimuovere un disco allocato al buffer di caricamento (VMware ESXi)

1. Nel client vSphere, aprire il menu contestuale (clic con il pulsante destro del mouse), scegliere il nome della macchina virtuale del gateway, quindi scegliere Edit Settings (Modifica impostazioni).
2. Sulla scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), selezionare il disco allocato come spazio per il buffer di caricamento, quindi selezionare Remove (Rimuovi).

   Verifica che il valore Virtual Device Node (Nodo dispositivo virtuale) nella finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale) sia lo stesso valore annotato in precedenza. In questo modo si ha la garanzia di rimuovere il disco corretto.



3. Selezionare un'opzione nel riquadro Removal Options (Opzioni di rimozione), quindi selezionare OK per completare il processo di rimozione del disco.



Rimozione di un disco da un gateway ospitato su Microsoft Hyper-V

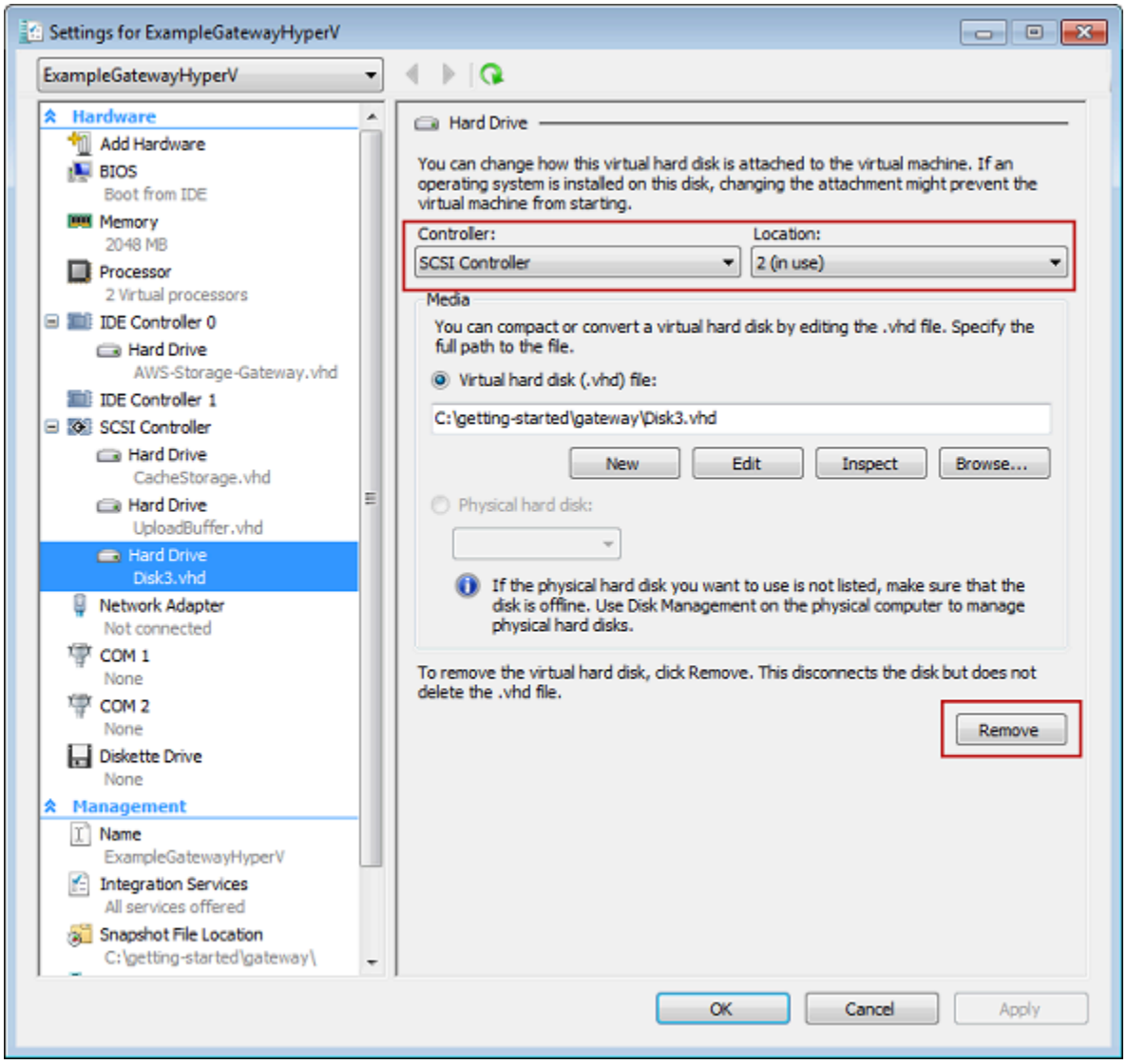
Utilizzando la seguente procedura, puoi rimuovere un disco dal gateway ospitato su un hypervisor Microsoft Hyper-V.

Per rimuovere un disco sottostante allocato per il buffer di caricamento (Microsoft Hyper-V)

1. In Microsoft Hyper-V Manager, aprire il menu contestuale (clic con il pulsante destro del mouse), selezionare il nome della macchina virtuale del gateway, quindi selezionare Settings (Impostazioni).
2. Nell'elenco Hardware della finestra di dialogo Settings (Impostazioni), selezionare il disco da rimuovere, quindi Remove (Rimuovi).

I dischi aggiunti al gateway vengono visualizzati sotto la voce SCSI Controller (Controller SCSI) nell'elenco Hardware. Verificare che i valori Controller e Location (Ubicazione) siano lo stesso valore annotato in precedenza. In questo modo si ha la garanzia di rimuovere il disco corretto.

Il primo controller SCSI visualizzato in Microsoft Hyper-V Manager è il controller 0.



3. Per applicare le modifiche, scegliere OK.

Rimozione di un disco da un gateway ospitato su Linux KVM

Per scollegare un disco dal gateway ospitato sull'hypervisor di macchina virtuale basata su kernel Linux, è possibile utilizzare un comando `virsh` simile a quello seguente.

```
$ virsh detach-disk domain_name /device/path
```

Per ulteriori dettagli sulla gestione dei dischi KVM, vedere la documentazione della distribuzione Linux.

Aggiunta e rimozione di volumi Amazon EBS per il gateway ospitato in Amazon EC2

Quando inizialmente il gateway è stato configurato per l'esecuzione come istanza Amazon EC2, sono stati allocati volumi Amazon EBS per l'uso come buffer di caricamento e storage della cache. Nel tempo, con l'evolversi delle esigenze delle applicazioni, puoi allocare volumi Amazon EBS aggiuntivi per questo uso. Puoi anche ridurre l'archiviazione allocata rimuovendo volumi Amazon EBS precedentemente allocati. Per ulteriori informazioni su Amazon EBS, consulta Amazon Elastic Block Store (Amazon EBS) nella Guida per l'utente di Amazon EC2 per istanze Linux.

Prima di aggiungere altro spazio di storage al gateway, determina come dimensionare il buffer di caricamento e lo storage della cache in base alle esigenze delle applicazioni per un gateway. A tale scopo, consulta Determinazione delle dimensioni del buffer di caricamento da allocare e Determinazione delle dimensioni dell'archiviazione della cache da allocare.

Sono previste quote per la capacità di storage massima che è possibile allocare come buffer di caricamento e storage della cache. È possibile collegare un numero qualsiasi di volumi Amazon EBS all'istanza, ma è possibile configurare questi volumi come spazio di buffer di caricamento e storage della cache solo fino alle quote di storage previste. Per ulteriori informazioni, consulta AWS Storage Gateway quote.

Per aggiungere un volume Amazon EBS e configurarlo per il gateway

1. Creazione di un volume Amazon EBS. Per le istruzioni, consulta Creazione o ripristino di un volume Amazon EBS nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Collega il volume Amazon EBS alla tua istanza Amazon EC2. Per istruzioni, consulta Collegamento di un volume Amazon EBS a un'istanza nella Guida per l'utente di Amazon EC2 per le istanze Linux.
3. Configurare il volume Amazon EBS aggiunto come buffer di caricamento o archiviazione della cache. Per istruzioni, consulta Gestione dei dischi locali per Storage Gateway.

Talvolta la quantità di storage allocata per il buffer di caricamento potrebbe risultare non necessaria.

Per rimuovere un volume Amazon EBS

> **Warning**
>
> Queste fasi si applicano solo ai volumi Amazon EBS allocati come spazio del buffer di caricamento, non ai volumi allocati alla cache. Se rimuovi da un gateway di nastri virtuali un volume Amazon EBS allocato come archiviazione della cache, i nastri virtuali nel gateway avranno lo stato IRRECUPERABILE e puoi rischiare di perdere i dati. Per ulteriori informazioni sullo stato IRRECUPERABILE, consulta Comprendere le informazioni sullo stato del nastro in una VTL.

1. Arrestare il gateway seguendo la procedura descritta nella sezione Spegnimento della macchina virtuale gateway.
2. Scollega il volume Amazon EBS dall'istanza Amazon EC2. Per istruzioni, consulta Scollegamento di un volume Amazon EBS da un'istanza nella Guida per l'utente di Amazon EC2 per le istanze Linux.
3. Elimina il volume Amazon EBS. Per le istruzioni, consulta Eliminazione di un volume Amazon EBS nella Guida per l'utente di Amazon EC2 per le istanze Linux.
4. Avviare il gateway seguendo la procedura descritta nella sezione Spegnimento della macchina virtuale gateway.

Utilizzo di dispositivi VTL

La configurazione del gateway di nastri virtuali supporta i seguenti dispositivi SCSI, da selezionare quando si attiva il gateway.

Argomenti

- Selezione di un'unità di sostituzione dei supporti dopo l'attivazione del gateway
- Aggiornamento del driver del dispositivo per l'unità di sostituzione dei supporti
- Visualizzazione di codici a barre per nastri in Microsoft System Center DPM

Per i cambiatori medi, AWS Storage Gateway funziona con quanto segue:

- AWS-Gateway-VTL: questo dispositivo è fornito con il gateway.
- STK-L700: questa emulazione di dispositivo è fornita con il gateway.

Al momento dell'attivazione del gateway di nastri virtuali, selezioni l'applicazione di backup dall'elenco e lo Storage Gateway utilizza l'unità di sostituzione dei supporti appropriata. Se l'applicazione di backup che occorre non è inclusa nell'elenco, scegliere Other (Altro) e selezionare l'unità di sostituzione dei supporti funzionante con tale applicazione.

Il tipo di unità di sostituzione dei supporti scelta dipende dall'applicazione di backup che si intende utilizzare. La tabella seguente elenca le applicazioni di backup di terze parti che sono state testate e risultate compatibili con gateway di nastri virtuali. Questa tabella include il tipo di unità di sostituzione dei supporti consigliata per ogni applicazione di backup.

Applicazione di backup	Tipo di unità di sostituzione dei supporti
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` o `STK-L700`
Commvault V11	`STK-L700`
Dell EMC 19.5 NetWorker	`AWS-Gateway-VTL`
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus (HPE) Data Protector 9 o 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 o 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Network 6.4 o 7.1	`STK-L700`
Quest NetVault Backup 12.4 o 13.x	`STK-L700`
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`
Veritas Backup Exec 2014 o 15 o 16 o 20 o 22.x	`AWS-Gateway-VTL`

Applicazione di backup	Tipo di unità di sostituzione dei supporti
Veritas Backup Exec 2012 **Note** Veritas ha terminato il supporto per Backup Exec 2012.	`STK-L700`
Veritas NetBackup versione 7.x o 8.x	`AWS-Gateway-VTL`

Important

Consigliamo vivamente di scegliere l'unità di sostituzione dei supporti elencata per la tua applicazione di backup. Altre unità di sostituzione dei supporti potrebbero non funzionare correttamente. Si può scegliere un'unità di sostituzione dei supporti diversa una volta attivato il gateway. Per ulteriori informazioni, consulta Selezione di un'unità di sostituzione dei supporti dopo l'attivazione del gateway.

Per quel che riguarda le unità nastro, Storage Gateway funziona con quanto segue:

- IBM-ULT3580-TD5 (emulazione di dispositivo fornita con il gateway).

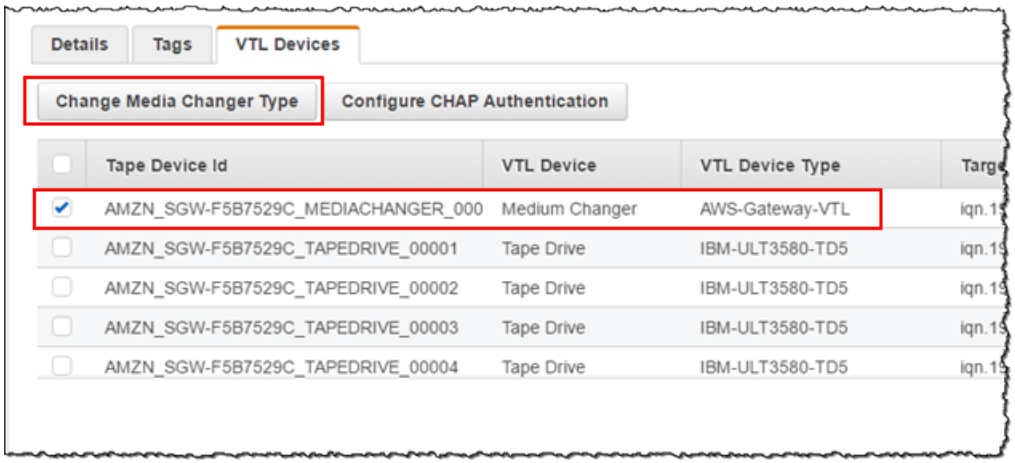
Selezione di un'unità di sostituzione dei supporti dopo l'attivazione del gateway

Una volta attivato il gateway, si può scegliere un'unità di sostituzione dei supporti diversa.

Come selezionare un'unità di sostituzione dei supporti diversa dopo l'attivazione del gateway

1. Interrompere eventuali attività correlate in esecuzione nel software di backup.
2. Aprire la finestra con le proprietà dell'iniziatore iSCSI sul server Windows.
3. Selezionare la scheda Targets (Destinazioni) per visualizzare le destinazioni trovate.
4. Nel riquadro delle destinazioni disponibili, scegliere l'unità di sostituzione dei supporti da modificare, poi selezionare prima Disconnect (Disconnetti) e poi OK (OK).

5. Nella console Storage Gateway, scegliere Gateway dal riquadro di navigazione e poi selezionare il gateway con l'unità di sostituzione dei supporti da modificare.
6. Scegliere la scheda VTL Devices (Dispositivi VTL), selezionare l'unità di sostituzione dei supporti da modificare e poi premere il pulsante Change Media Changer (Modifica unità di sostituzione dei supporti).



7. Nella finestra di dialogo che viene visualizzata, Modifica tipo di unità di sostituzione dei supporti, scegliere l'unità desiderata dall'elenco a discesa e, infine, selezionare Save (Salva).

Aggiornamento del driver del dispositivo per l'unità di sostituzione dei supporti

1. Aprire Gestione dispositivi nel server Windows ed espandere la struttura ad albero Medium Changer devices (Dispositivi di unità di sostituzione dei supporti).
2. Aprire il menu contestuale (clic con il pulsante destro) Unknown Medium Changer (Unità di sostituzione dei supporti sconosciuta) e scegliere Update Driver Software (Aggiorna software driver) per aprire la finestra Update Driver Software-unknown Medium Changer (Aggiorna software del driver per unità di sostituzione dei supporti sconosciuta).
3. Nella sezione How do you want to search for driver software? (Modalità di ricerca software driver?), scegliere Browse my computer for driver software (Cerca driver nel computer).
4. Scegliere Let me pick from a list of device drivers on my computer (Selezione manuale da un elenco di driver di dispositivo sul computer).

> **Note**
>
> È consigliabile utilizzare il driver Sony TSL-A500C Autoloader con i software di backup Veeam Backup & Replication 11A e Microsoft System Center Data Protection Manager.

> Questo driver Sony è stato testato con questi tipi di software di backup fino a Windows Server 2019 incluso.

5. Nella sezione Select the device driver you want to install for this hardware (Seleziona il driver di dispositivo da installare per questo hardware), deselezionare la casella di controllo Show compatible hardware (Mostra hardware compatibile), scegliere Sony nell'elenco Manufacturer (Produttore), selezionare Sony - TSL-A500C Autoloader dall'elenco Model (Modello) e, infine, selezionare Next (Avanti).
6. Nella finestra di avviso che appare, scegliere Yes (Sì). Una volta installato il driver, chiudere la finestra Update drive software (Aggiorna software driver).

Visualizzazione di codici a barre per nastri in Microsoft System Center DPM

Se si utilizza il media changer driver per l'Autoloader Sony TSL-A500C, Microsoft System Center Data Protection Manager non visualizza automaticamente i codici a barre per i nastri virtuali creati in Storage Gateway. Per visualizzare correttamente i codici a barre dei nastri, impostate il driver del media changer su Sun/ Library. StorageTek

Per visualizzare i codici a barre

1. Verificare che tutte le operazioni di backup siano state completate e che non ci sono attività in attesa o in corso.
2. Espellere e spostare i nastri nello spazio di archiviazione offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) e uscire dalla console di amministrazione DPM. Per informazioni su come estrarre un nastro in DPM, consulta Archiviazione di un nastro utilizzando DPM.
3. In Administrative Tools (Strumenti di amministrazione), selezionare Services (Servizi) e aprire il menu contestuale (clic sul tasto destro del mouse) per DPM Service (Servizio DPM) nel pannello Detail (Dettaglio), quindi scegliere Properties (Proprietà).
4. Nella scheda General (Domande generali), assicurarsi che il Startup type (Tipo di avvio) sia impostato su Automatic (Automatico), quindi scegliere Stop (Arresta) per arrestare il servizio DPM.
5. Scarica i StorageTek driver dal catalogo di Microsoft Update sul sito Web Microsoft.

> **Note**
>
> Annotare i diversi driver per le dimensioni diverse.

In Size (Dimensione) 18K, selezionare x86 drivers (driver x86).

In Size (Dimensione) 19K, selezionare x64 drivers (driver x64).

6. Nel server Windows, aprire Gestione dispositivi ed espandere la struttura ad albero Medium Changer devices (Dispositivi di unità di sostituzione dei supporti).
7. Aprire il menu contestuale (clic con il pulsante destro) Unknown Medium Changer (Unità di sostituzione dei supporti sconosciuta) e scegliere Update Driver Software (Aggiorna software driver) per aprire la finestra Update Driver Software-unknown Medium Changer (Aggiorna software del driver per unità di sostituzione dei supporti sconosciuta).
8. Individuare il percorso della nuova posizione del driver e installarlo. Il driver viene visualizzato come Sun/ StorageTek Library. Le unità nastro rimangono come dispositivo sequenziale IBM ULT3580-TD5 SCSI.
9. Riavviare il server DPM.
10. Nella console Storage Gateway, crea nuovi nastri.
11. Aprire la console di amministrazione DPM, scegliere Management (Gestione), quindi scegliere Rescan for new tape libraries (Eseguire nuovamente la scansione per nuove librerie a nastro). Dovresti vedere la libreria Sun/ StorageTek .
12. Scegliere la libreria, quindi selezionare Inventory (Inventario).
13. Scegliere Add Tapes (Aggiungi nastri) per aggiungere i nuovi nastri in DPM. I nuovi nastri devono ora visualizzare i codici a barre.

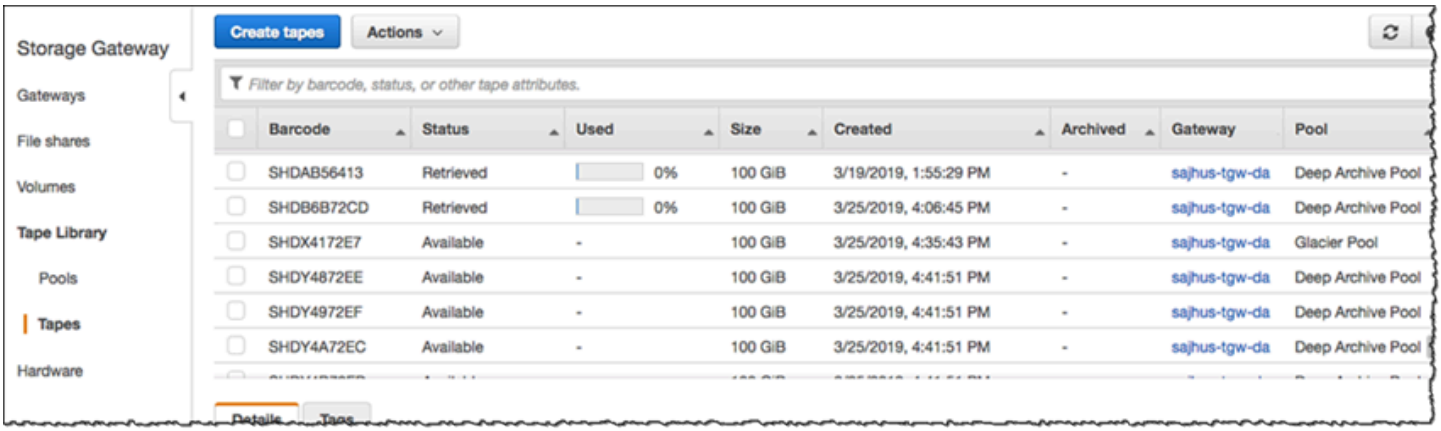
Utilizzo dei nastri

Storage gateway fornisce una libreria di nastri virtuali (VTL) per ogni gateway di nastri virtuali attivato. Inizialmente, la libreria è vuota, ma puoi creare nastri in qualunque momento ti occorrano. La tua applicazione può leggere e scrivere su qualsiasi nastro disponibile nel gateway di nastri virtuali. Perché vi si possa scrivere, il nastro deve presentare lo stato AVAILABLE (DISPONIBILE). Questi nastri sono supportati da Amazon Simple Storage Service (Amazon S3), ovvero, quando scrivi su questi nastri, il gateway di nastri virtuali archivia i dati in Amazon S3. Per ulteriori informazioni, consulta Comprendere le informazioni sullo stato del nastro in una VTL.

Argomenti

- Archiviazione di nastri
- Annullamento dell'archiviazione di un nastro

La libreria dei nastri mostra i nastri inclusi nel gateway di nastri virtuali. con i relativi codici a barre, gli stati e le dimensioni, nonché la quantità di nastro utilizzato e il gateway al quale ciascun nastro è associato.



Nelle librerie con molti nastri, la console consente di cercare un nastro in particolare per codice a barre, per stato o per entrambi. La ricerca per codice a barre permette di filtrare i risultati in base allo stato e al gateway.

Per eseguire la ricerca in base al codice a barre, lo stato e il gateway

1. Apri la console Storage Gateway all'indirizzo https://console.aws.amazon.com/storagegateway/home.
2. Nel riquadro di navigazione, selezionare Tapes (Nastri) e digitare un valore nella casella di ricerca. Il valore può essere il codice a barre, lo stato o il gateway. Per impostazione predefinita, Storage Gateway effettua la ricerca tra tutti i nastri virtuali. Tuttavia, è possibile filtrare la ricerca in base allo stato.

   Se si filtra per lo stato, nella libreria della console Storage Gateway vengono visualizzati i nastri che soddisfano i criteri.

   Se si filtra in base a un gateway, nella libreria della console Storage Gateway vengono visualizzati i nastri associati a tale gateway.

   > **Note**
   >
   > Per impostazione predefinita, Storage Gateway mostra tutti i nastri, indipendentemente dal loro stato.

Archiviazione di nastri

Puoi archiviare i nastri virtuali inclusi nel gateway di nastri virtuali. Quando archivi un nastro, Storage Gateway sposta il nastro nell'archivio.

Per archiviare un nastro, devi usare il software di backup. Il processo di archiviazione dei nastri è costituito da tre fasi, rappresentate dagli stati dei nastri IN TRANSIT TO VTS (IN TRANSITO VERSO VTS), ARCHIVING (ARCHIVIAZIONE)e ARCHIVED (ARCHIVIATO):

- Per archiviare un nastro, usa il comando fornito dall'applicazione di backup. All'inizio del processo di archiviazione, lo stato del nastro passa a IN TRANSIT TO VTS (IN TRANSITO VERSO VTS) e l'applicazione di backup non può più accedere al nastro. In questa fase, il Tape Gateway sta caricando i dati su. AWS Se necessario, puoi annullare l'archiviazione in corso. Per ulteriori informazioni sull'annullamento dell'archiviazione, consulta Annullamento dell'archiviazione di un nastro.

  > **Note**
  >
  > La procedura per l'archiviazione di un nastro dipende dall'applicazione di backup. Per istruzioni dettagliate, consulta la documentazione dell'applicazione di backup.

- Una volta AWS completato il caricamento dei dati, lo stato del nastro passa a ARCHIVING e Storage Gateway inizia a spostare il nastro nell'archivio. A questo punto, non puoi più annullare il processo di archiviazione.
- Dopo che il nastro viene spostato nell'archivio, il suo stato passa a ARCHIVED (ARCHIVIATO) e puoi recuperarlo in uno qualsiasi dei gateway. Per ulteriori informazioni sul recupero di nastri, consulta Recupero di nastri archiviati.

La procedura per l'archiviazione di un nastro dipende dal software di backup. Per istruzioni su come archiviare un nastro utilizzando il NetBackup software Symantec, vedere Archiviazione del nastro.

Annullamento dell'archiviazione di un nastro

Nel caso in cui decidessi di annullare l'archiviazione di un nastro già in corso per vari motivi, ad esempio perché la procedura ti sta sottraendo troppo tempo o per leggere i dati dal nastro, tieni presente che l'archiviazione di un nastro si sviluppa in tre fasi contraddistinte da tre stati:

- IN TRANSITO VERSO VTS: il gateway di nastri virtuali sta caricando i dati su AWS.

- ARCHIVIAZIONE: il caricamento dei dati è completo e il gateway di nastri virtuali sta trasferendo il nastro in archivio.
- ARCHIVIATO: il nastro è nell'archivio, da cui può essere recuperato.

L'archiviazione può essere annullata solo se il nastro è nello stato IN TRANSITO VERSO VTS. Tale stato potrebbe essere visibile nella console Storage Gateway o meno, in base a fattori quali la larghezza di banda del caricamento e la quantità di dati caricati. Per annullare l'archiviazione di un nastro, utilizza l'CancelRetrievalazione nel riferimento all'API.

Ottenimento di una chiave di attivazione per il gateway

Per ricevere una chiave di attivazione per il gateway, effettua una richiesta Web alla macchina virtuale (VM) del gateway. La macchina virtuale restituisce un reindirizzamento che contiene la chiave di attivazione, che viene passata come uno dei parametri dell'azione `ActivateGateway` API per specificare la configurazione del gateway. Per ulteriori informazioni, vedere ActivateGatewaylo Storage Gateway API Reference.

> **Note**
>
> Le chiavi di attivazione del gateway scadono dopo 30 minuti se non vengono utilizzate.

La richiesta effettuata alla macchina virtuale gateway include la AWS regione in cui avviene l'attivazione. L'URL restituito dal reindirizzamento nella risposta contiene un parametro della stringa di query denominato `activationkey`. Questo parametro della stringa di query è la chiave di attivazione. Il formato della stringa di query ha un aspetto simile a questo: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. L'output di questa query restituisce sia la regione che la chiave di attivazione.

L'URL include `vpcEndpoint` anche l'ID dell'endpoint VPC per i gateway che si connettono utilizzando il tipo di endpoint VPC.

> **Note**
>
> L'appliance hardware Storage Gateway, i modelli di immagini VM e le Amazon Machine Images (AMI) di Amazon EC2 sono preconfigurati con i servizi HTTP necessari per ricevere

e rispondere alle richieste Web descritte in questa pagina. Non è richiesta né consigliata l'installazione di servizi aggiuntivi sul gateway.

Argomenti

Linux (curl)

Gli esempi seguenti mostrano come recuperare una chiave di attivazione utilizzando Linux (curl).

> **Note**
>
> Sostituisci le variabili evidenziate con i valori effettivi per il gateway. I valori accettabili sono i seguenti:
>
> - *`gateway_ip_address - L'indirizzo`* IPv4 del gateway, ad esempio `172.31.29.201`
> - *`gateway_type`*: il tipo di gateway che desideri attivare, ad esempio, `STOREDCACHED`, `VTL` o. `FILE_S3` `FILE_FSX_SMB`
> - *`region_code`* - La regione in cui desideri attivare il gateway. Vedi Endpoint regionali nella Guida di riferimento generale.AWS
> - *`vpc_endpoint -`* Il nome dell'endpoint VPC per il gateway, ad esempio. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Per ottenere la chiave di attivazione per un endpoint pubblico:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Per ottenere la chiave di attivazione per un endpoint VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

L'esempio seguente mostra come usare Linux (bash/zsh) per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

L'esempio seguente mostra come utilizzare Microsoft Windows PowerShell per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
```

```
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Utilizzando la console locale

Nell'esempio seguente viene illustrato come utilizzare la console locale per generare e visualizzare una chiave di attivazione.

Per ottenere una chiave di attivazione per il gateway dalla console locale

1. Accedere alla tua console locale. Se ci si connette all'istanza Amazon EC2 da un computer Windows, accedere come amministratore.
2. Dopo aver effettuato l'accesso e aver visualizzato il menu principale Attivazione dell'AWS appliance - Configurazione, seleziona `0` Ottieni chiave di attivazione.
3. Seleziona l'opzione Storage Gateway for gateway family.
4. Quando richiesto, inserisci la AWS regione in cui desideri attivare il gateway.
5. Immettere 1 per pubblico oppure 2 per endpoint VPC come tipo di rete.
6. Inserire 1 Standard o 2 Federal Information Processing Standard (FIPS) come Tipo di endpoint.

Connessione di iniziatori iSCSI

Quando gestisci il gateway, lavori con volumi o dispositivi della libreria di nastri virtuali (VTL) esposti come destinazioni iSCSI (Internet Small Computer System Interface). Per i gateway di volumi, le destinazioni iSCSI sono volumi. Per i gateway di nastri virtuali, le destinazioni sono dispositivi VTL. Nell'ambito della gestione, svolgi attività come la connessione a queste destinazioni, la personalizzazione delle impostazioni iSCSI, la connessione da un client Red Hat Linux e la configurazione di CHAP (Challenge-Handshake Authentication Protocol).

Argomenti

- Connessione dei dispositivi VTL a un client Windows
- Connessione dei volumi o dei dispositivi VTL a un client Linux
- Personalizzazione delle impostazioni iSCSI
- Configurazione dell'autenticazione CHAP per le destinazioni iSCSI

Lo standard iSCSI è uno standard di rete di storage basato su IP per l'avvio e la gestione di connessioni tra client e dispositivi di storage basati su IP. L'elenco seguente definisce alcuni dei termini usati per descrivere la connessione iSCSI e i componenti coinvolti.

Iniziatore iSCSI

Il componente client di una rete iSCSI. L'iniziatore invia le richieste alla destinazione iSCSI. Gli iniziatori possono essere implementati nel software o nell'hardware. Storage Gateway supporta solo gli iniziatori software.

Destinazione iSCSI

Il componente server della rete iSCSI che riceve le richieste dagli iniziatori e risponde. Ogni volume è esposto come destinazione iSCSI. Connetti un solo iniziatore iSCSI a ogni destinazione iSCSI.

Iniziatore iSCSI Microsoft

Il programma software nei computer Microsoft Windows che permette la connessione di un computer client (ovvero il computer che esegue l'applicazione i cui dati devono essere scritti nel gateway) a un array basato su iSCSI esterno (ovvero il gateway). La connessione viene effettuata usando la scheda di rete Ethernet del computer host. L'iniziatore Microsoft iSCSI è stato convalidato con Storage Gateway su Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019. L'iniziatore è integrato in questi sistemi operativi.

Iniziatore iSCSI Red Hat

Il pacchetto`iscsi-initiator-utils` RPM (Resource Package Manager) fornisce un iniziatore iSCSI implementato nel software per Red Hat Linux. Il pacchetto include un daemon del server per il protocollo iSCSI.

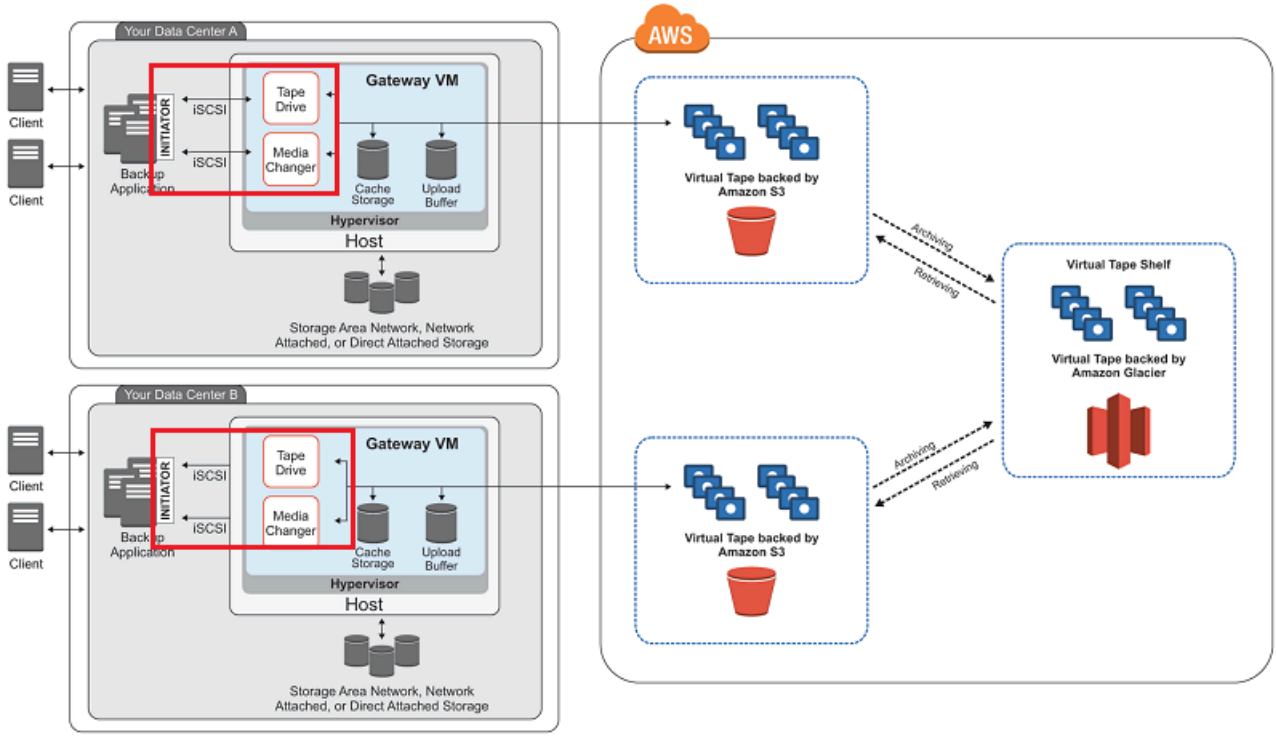
Ogni tipo di gateway è in grado di connettersi ai dispositivi iSCSI ed è possibile personalizzare queste connessioni, come descritto di seguito.

Connessione dei dispositivi VTL a un client Windows

Un gateway di nastri virtuali espone diverse unità nastro e un'unità di sostituzione dei supporti, definite collettivamente dispositivi VTL, come destinazioni iSCSI. Per ulteriori informazioni, consulta Requisiti.

> **Note**
>
> È possibile connettere una sola applicazione a ogni destinazione iSCSI.

Il diagramma seguente evidenzia la destinazione iSCSI nell'immagine più grande dell'architettura Storage Gateway. Per ulteriori informazioni sull'architettura di Storage Gateway, consulta Come funziona il gateway di nastri virtuali (architettura).

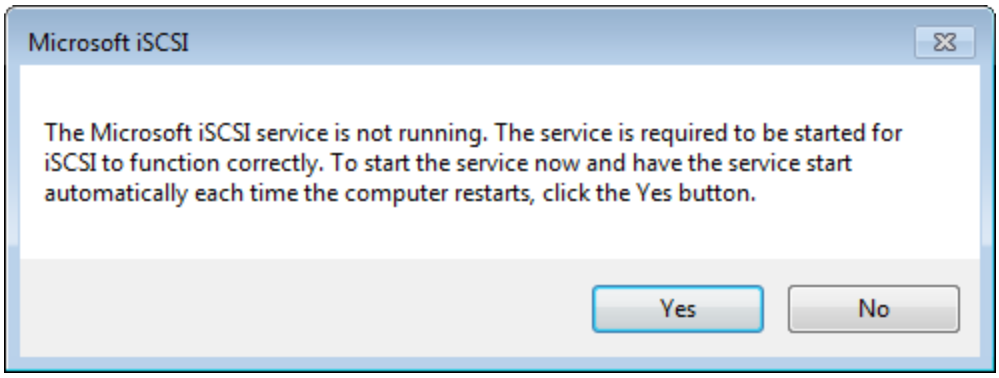


Per connettere il client Windows ai dispositivi VTL

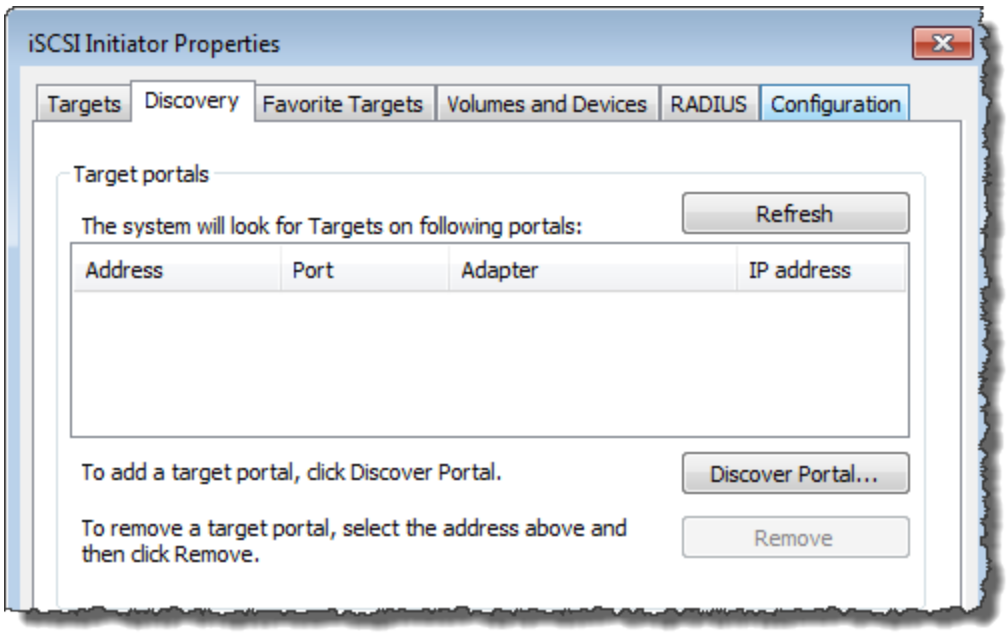
1. Nel menu Start del computer client Windows, digitare **`iscsicpl.exe`** nella casella Cerca programmi e file, individuare il programma dell'iniziatore iSCSI ed eseguirlo.

> **Note**
>
> Per eseguire l'iniziatore iSCSI, è necessario disporre di diritti di amministratore nel computer client.

2. Se viene richiesto, scegliere Sì per avviare l'iniziatore Microsoft iSCSI.

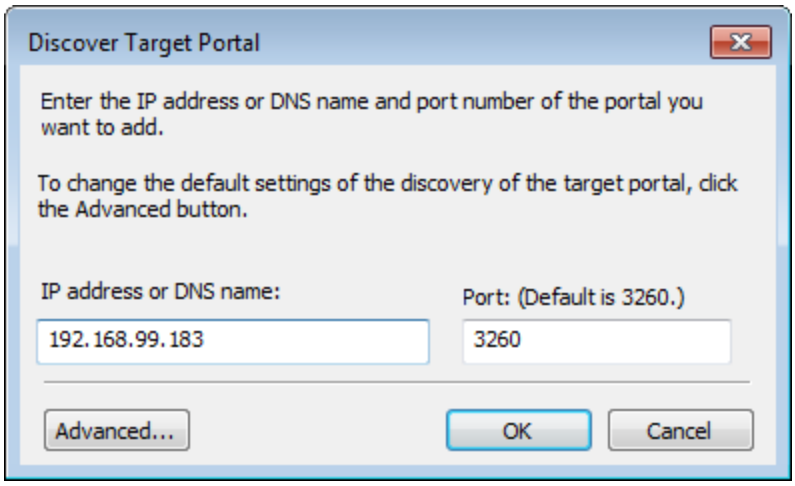


3. Nella finestra di dialogo iSCSI Initiator Properties (Proprietà iniziatore iSCSI) scegliere la scheda Discovery (Individuazione) e quindi scegliere Discover Portal (Individua portale).



4. Nella finestra di dialogo Individua portale destinazione digitare l'indirizzo IP del gateway di nastri virtuali in Indirizzo IP o nome DNS e quindi fare clic su OK. Per ottenere l'indirizzo IP del gateway, fare riferimento alla scheda Gateway nella console Storage Gateway. Se il gateway è

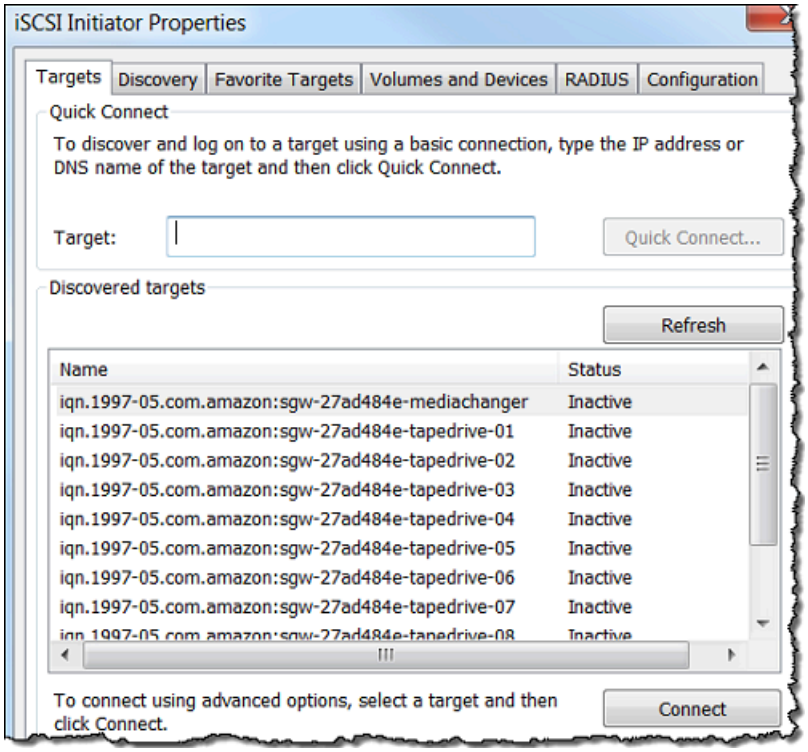
stato distribuito in un'istanza Amazon EC2, l'indirizzo DNS o IP pubblico è indicato nella scheda Description (Descrizione) della console Amazon EC2.



> **Warning**
>
> Per i gateway distribuiti in un'istanza Amazon EC2, l'accesso al gateway tramite una connessione Internet pubblica non è supportato. Non è possibile usare l'indirizzo IP elastico dell'istanza Amazon EC2; come indirizzo di destinazione.

5. Scegliere la scheda Targets (Destinazioni) e quindi scegliere Refresh (Aggiorna). Le 10 unità nastro e l'unità di sostituzione dei supporti verranno visualizzate nella casella Discovered targets (Destinazioni individuate). Lo stato della destinazione è Inactive (Inattivo).

   Lo screenshot seguente mostra le destinazioni individuate.

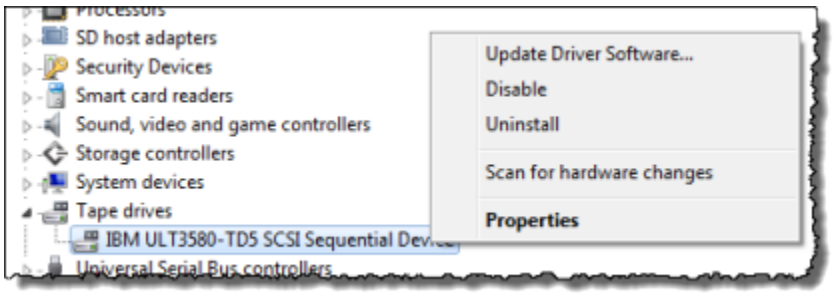


6. Selezionare il primo dispositivo e scegliere Connect (Connetti). I dispositivi devono essere connessi uno per volta.
7. Nella finestra di dialogo Connect To Target (Connetti a destinazione) scegliere OK.
8. Ripetere le fasi 6 e 7 per ciascuno dei dispositivi fino a connetterli tutti e quindi scegliere OK nella finestra di dialogo iSCSI Initiator Properties (Proprietà iniziatore iSCSI).

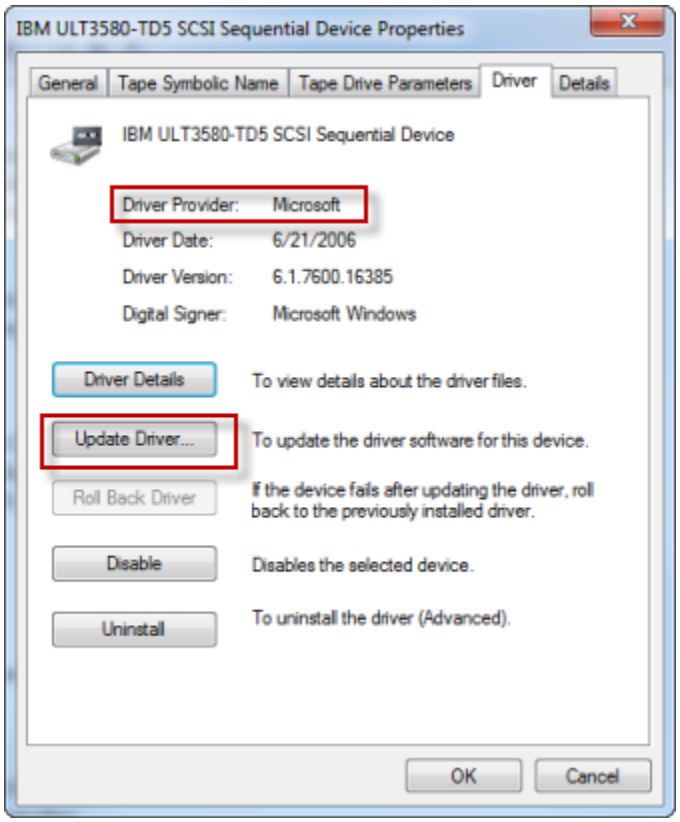
In un client Windows il fornitore di driver per l'unità nastro deve essere Microsoft. Usare la procedura seguente per verificare il fornitore di driver e aggiornare il driver e il fornitore, se necessario.

Per verificare il fornitore di driver e, se necessario, aggiornare il driver e il fornitore in un client Windows

1. Nel client Windows avviare Gestione dispositivi.
2. Espandere Tape drives (Unità nastro), visualizzare il menu contestuale (con il pulsante destro del mouse) per un'unità nastro e scegliere Properties (Proprietà).



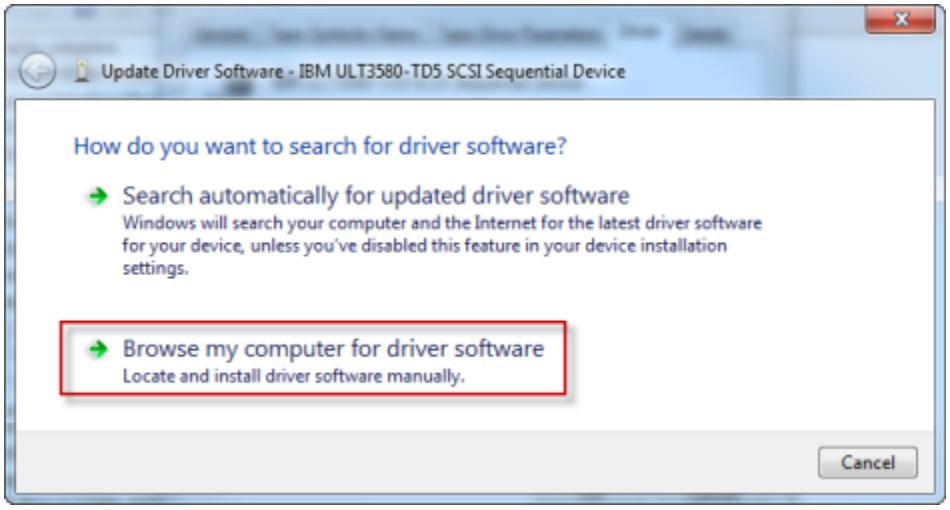
3. Nella scheda Driver della finestra di dialogo Device Properties (Proprietà dispositivo) verificare che per Driver Provider (Fornitore driver) sia indicato Microsoft.



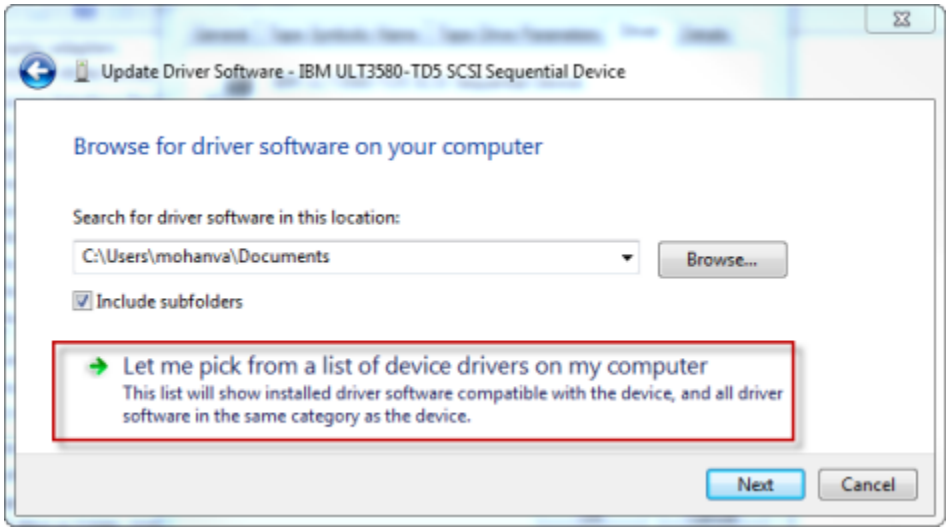
4. Se in Driver Provider (Fornitore driver) non è indicato Microsoft, impostare il valore come illustrato di seguito:

   a. Scegliere Update Driver (Aggiorna driver).

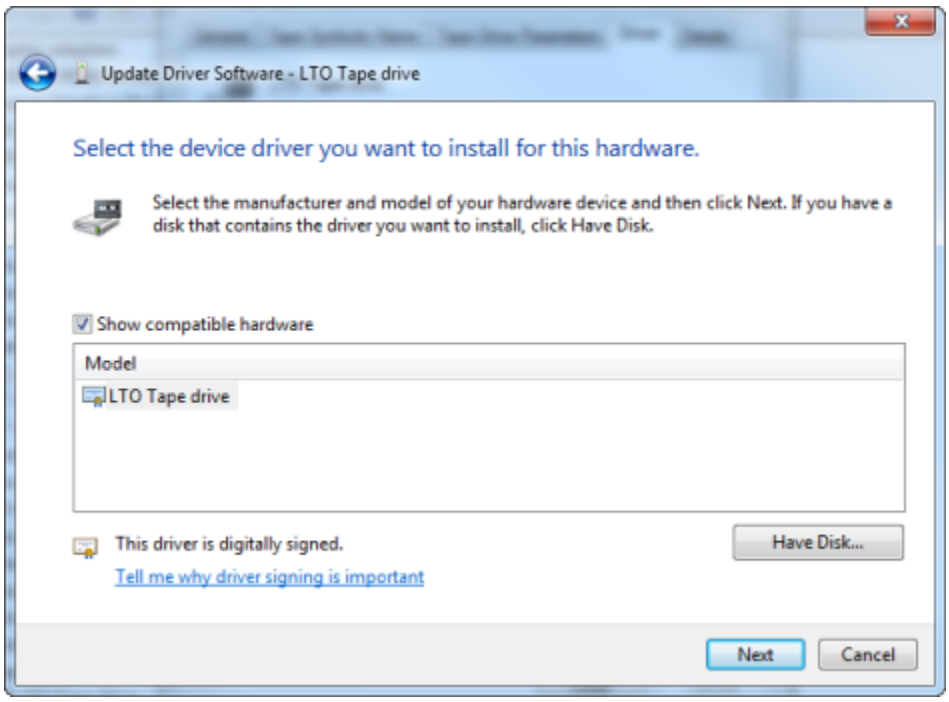
   b. Nella finestra di dialogo Update Driver Software (Aggiornamento software driver) scegliere Browse my computer for driver software (Cerca software driver nel computer).



c. Nella finestra di dialogo Update Driver Software (Aggiornamento software driver) scegliere Let me pick from a list of device drivers on my computer (Seleziona da un elenco di driver di dispositivo nel computer).



d. Selezionare LTO Tape drive (unità nastro LTO) e quindi Next (Avanti).



e. Scegliere Close (Chiudi) per chiudere la finestra Update Driver Software (Aggiornamento software driver) e verificare che il valore di Driver Provider (Fornitore driver) sia ora impostato su Microsoft.

5. Ripetere le fasi da 4.1 a 4.5 per aggiornare tutte le unità nastro.

Connessione dei volumi o dei dispositivi VTL a un client Linux

Quando usi Red Hat Enterprise Linux (RHEL), puoi usare il pacchetto `iscsi-initiator-utils`RPM per connetterti alle destinazioni iSCSI del gateway (volumi o dispositivi VTL).

Per connettere un client Linux alle destinazioni iSCSI

1. Installare il pacchetto `iscsi-initiator-utils`RPM, se non è già installato nel client.

   Puoi utilizzare il seguente comando per installare il pacchetto.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Verificare che il daemon iSCSI sia in esecuzione.

   a. Per verificare che il daemon iSCSI sia in esecuzione, usare uno dei comandi seguenti.

      Per RHEL 5 o 6, utilizzare il seguente comando.

```
sudo /etc/init.d/iscsi status
```

Per RHEL 7, utilizzare il seguente comando.

```
sudo service iscsid status
```

b. Se il comando status non restituisce uno stato running (in esecuzione), avviare il daemon usando uno dei comandi seguenti.

Per RHEL 5 o 6, utilizzare il seguente comando.

```
sudo /etc/init.d/iscsi start
```

Per RHEL 7, utilizzare il seguente comando. Per RHEL 7 in genere non è necessario avviare in modo esplicito il servizio `iscsid`.

```
sudo service iscsid start
```

3. Per individuare i volumi o il dispositivo VTL di destinazione definito per un gateway, usare il comando di individuazione seguente.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

Specificare l'indirizzo IP del gateway al posto della variabile *[GATEWAY_IP]* nel comando precedente. L'indirizzo IP del gateway è indicato nelle proprietà Informazioni destinazione iSCSI di un volume nella console Storage Gateway.

L'output del comando di individuazione sarà simile all'output di esempio seguente.

Per i gateway di volumi: *[GATEWAY_IP]*`:3260, 1 iqn.1997-05.com.amazon:myvolume`

Per i gateway di nastri virtuali: `iqn.1997-05.com.amazon:`*[GATEWAY_IP]*`-tapedrive-01`

Il nome completo iSCSI (IQN) sarà diverso da quello mostrato in precedenza, perché i valori dei nomi IQN sono univoci per un'organizzazione. Il nome della destinazione è il nome specificato quando viene creato il volume. È anche possibile trovare il nome della destinazione nel riquadro delle proprietà iSCSI Target Info (Informazioni destinazione iSCSI) quando si seleziona un volume nella console Storage Gateway.

4. Per connettersi a una destinazione, utilizzare il seguente comando.

   Nel comando di connessione, è necessario specificare i valori corretti per *[GATEWAY_IP]* e IQN.

   > **Warning**
   >
   > Per i gateway distribuiti in un'istanza Amazon EC2, l'accesso al gateway tramite una connessione Internet pubblica non è supportato. Non è possibile usare l'indirizzo IP elastico dell'istanza Amazon EC2; come indirizzo di destinazione.

   ```
   sudo /sbin/iscsiadm --mode node --targetname
    iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
   ```

5. Per verificare che il volume sia collegato al computer client (iniziatore), utilizzare il seguente comando.

   ```
   ls -l /dev/disk/by-path
   ```

   L'output del comando sarà simile all'output di esempio seguente.

   ```
   lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
   iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
   ```

   È consigliabile personalizzare le impostazioni iSCSI dopo aver configurato l'iniziatore, come illustrato in Personalizzazione delle impostazioni iSCSI di Linux.

Personalizzazione delle impostazioni iSCSI

Dopo aver configurato l'iniziatore, ti consigliamo di personalizzare le impostazioni iSCSI per impedire all'iniziatore di disconnettersi dalle destinazioni.

Aumentando i valori di timeout iSCSI come mostrato nella procedura seguente, l'applicazione sarà in grado di gestire meglio le operazioni di scrittura che richiedono molto tempo e altri problemi temporanei, come le interruzioni di rete.

> **Note**
>
> Prima di apportare modifiche al Registro di sistema, devi eseguirne una copia di backup. Per informazioni sulla creazione di una copia di backup e altre procedure consigliate da seguire quando si lavora con il Registro di sistema, vedere Procedure consigliate per il Registro di sistema nella Microsoft TechNet Library.

Argomenti

Personalizzazione delle impostazioni iSCSI di Windows

Per una configurazione del gateway di nastri virtuali, la connessione ai dispositivi VTL tramite un iniziatore iSCSI Microsoft è un processo in due fasi:

1. Connettere i dispositivi gateway di nastri virtuali al client Windows.
2. Se si usa un'applicazione di backup, configurare l'applicazione per l'uso dei dispositivi.

La configurazione mostrata nell'esempio sulle operazioni iniziali offre le istruzioni per entrambe le fasi. Utilizza l'applicazione di NetBackup backup Symantec. Per ulteriori informazioni, consultare Connessione dei dispositivi VTL e Configurazione dei dispositivi di storage NetBackup .

Per personalizzare le impostazioni iSCSI di Windows

1. Aumentare il tempo massimo durante il quale lasciare in coda le richieste.

   a. Avviare l'editor del Registro di sistema (`Regedit.exe`).

   b. Passare alla chiave del GUID (identificatore univoco globale) per la classe del dispositivo che contiene le impostazioni del controller iSCSI, mostrata di seguito.

> **Warning**
>
> Assicurati di lavorare sulla CurrentControlSetsottochiave e non su un altro set di controlli, come ControlSet001 o 002. ControlSet

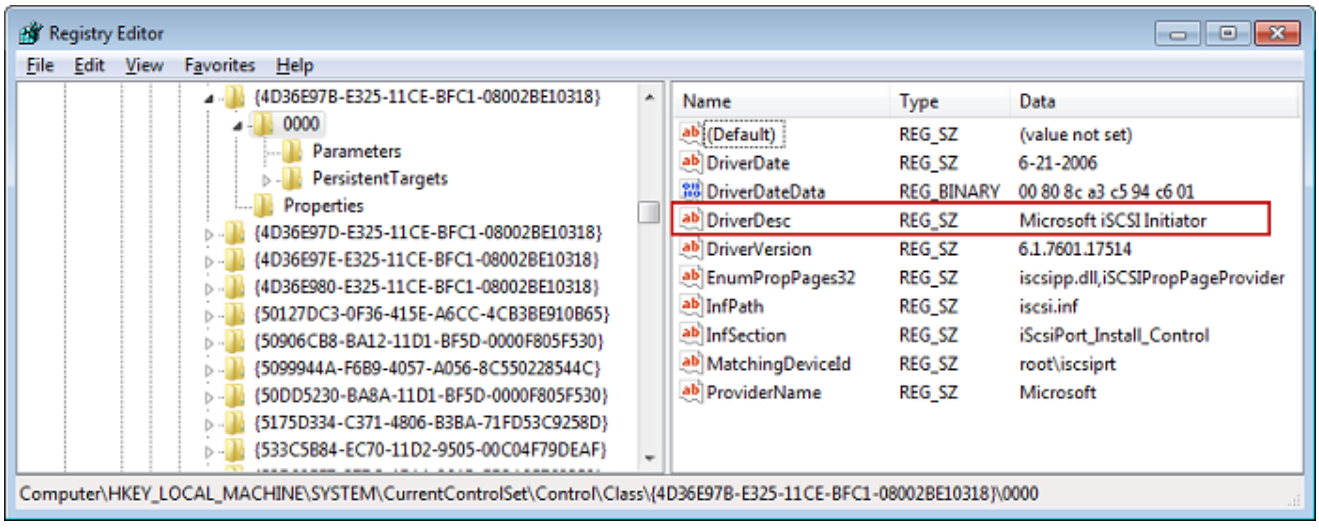
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. Individuare la sottochiave per l'iniziatore iSCSI Microsoft, mostrata di seguito come *`[<Instance Number]`*.

   La chiave è rappresentata da un numero a quattro cifre, ad esempio `0000`.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

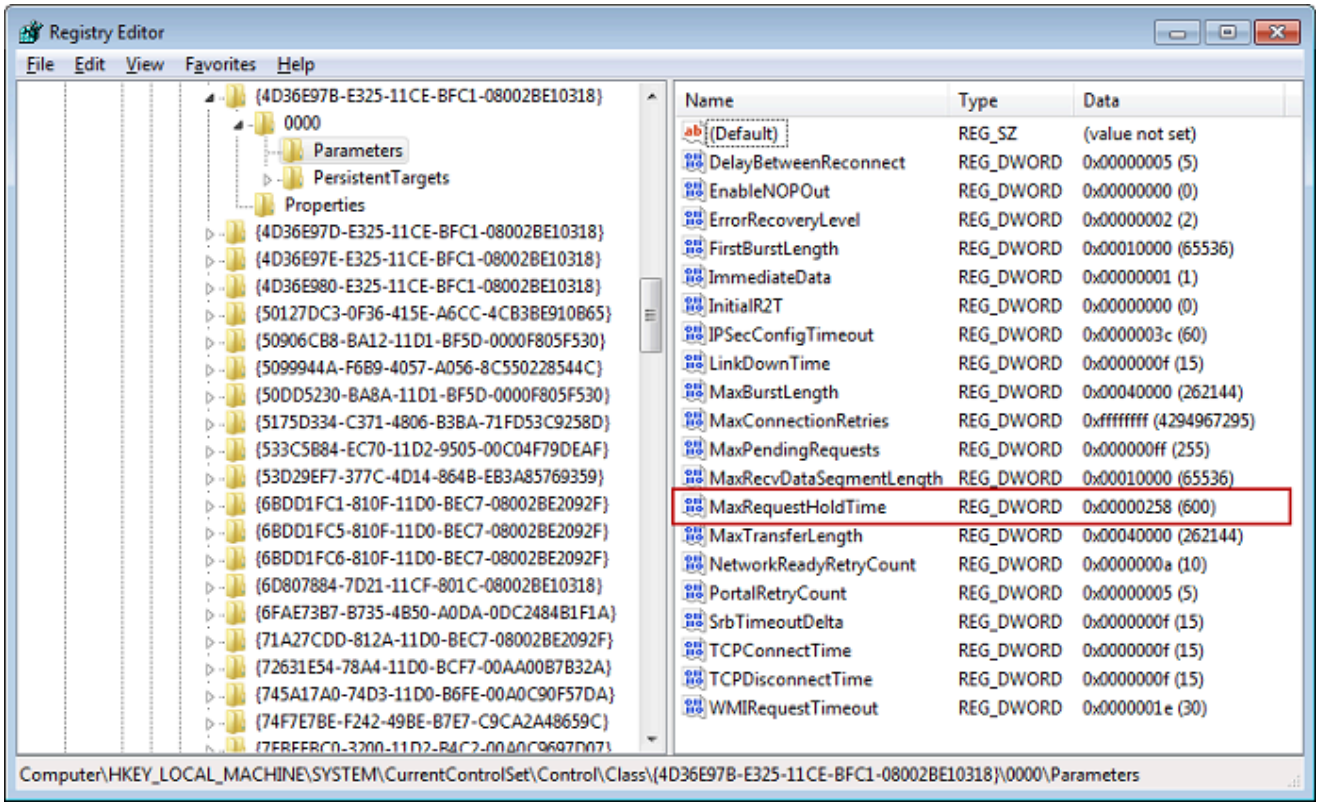
   A seconda di cosa è installato nel computer, l'iniziatore iSCSI Microsoft può non corrispondere alla sottochiave `0000`. È possibile controllare di aver selezionato la sottochiave corretta verificando che la stringa `DriverDesc` abbia il valore `Microsoft iSCSI Initiator`, come mostrato nell'esempio seguente.



d. Per visualizzare le impostazioni iSCSI, scegliere la sottochiave Parameters (Parametri).

e. Aprite il menu contestuale (con il pulsante destro del mouse) per il valore MaxRequestHoldTimeDWORD (32 bit), scegliete Modifica, quindi modificate il valore in. **`600`**

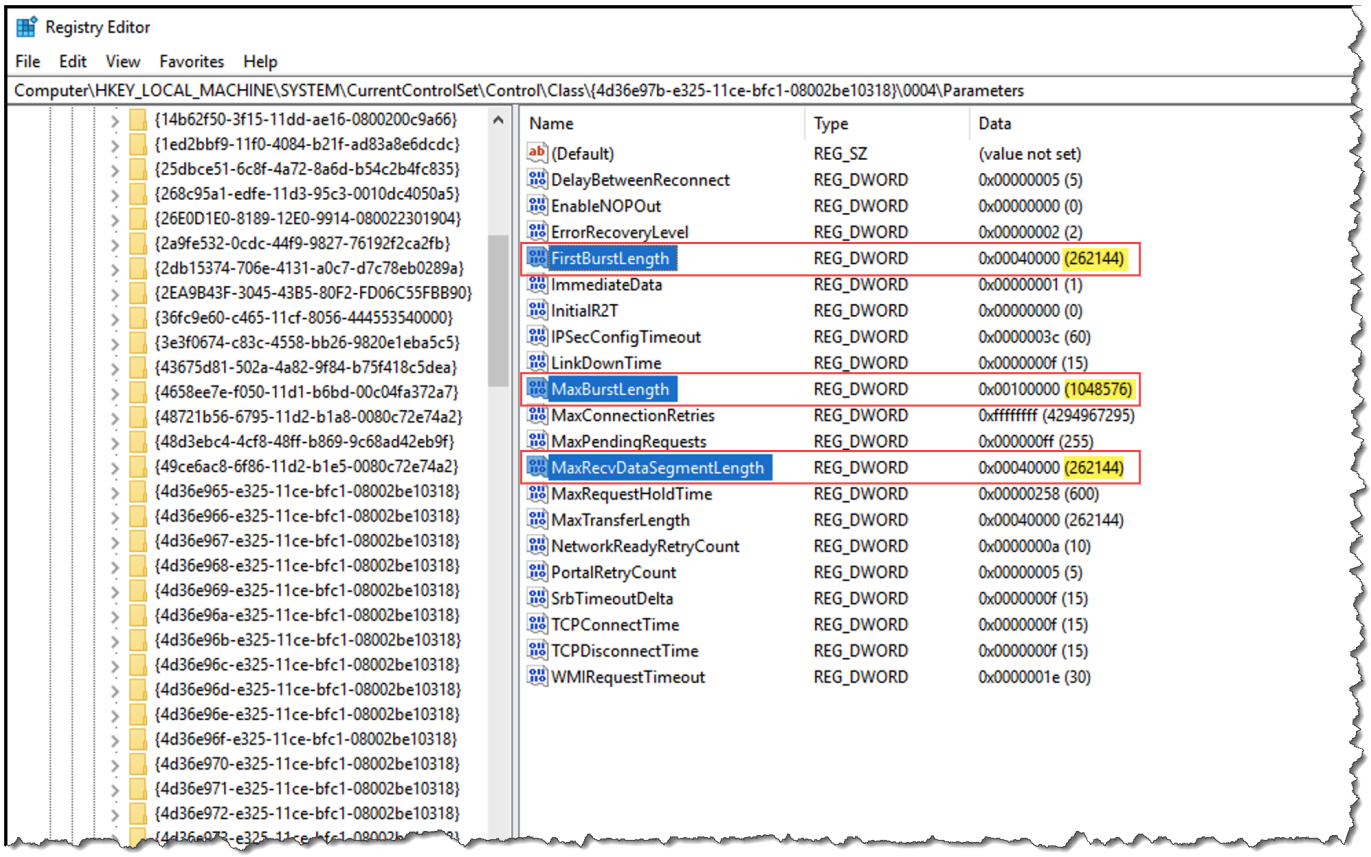
   MaxRequestHoldTimespecifica per quanti secondi l'iniziatore Microsoft iSCSI deve trattenere e riprovare i comandi in sospeso prima di notificare un evento al livello superiore. `Device Removal` Questo valore rappresenta un tempo di attesa di 600 secondi, come illustrato nell'esempio seguente.



2. È possibile aumentare la quantità massima di dati che è possibile inviare nei pacchetti iSCSI modificando i seguenti parametri:

   - FirstBurstLengthcontrolla la quantità massima di dati che possono essere trasmessi in una richiesta di scrittura non richiesta. Imposta questo valore su **`262144`** o sul valore predefinito del sistema operativo Windows, a seconda di quale sia il più alto.
   - MaxBurstLengthè simile a FirstBurstLength, ma imposta la quantità massima di dati che possono essere trasmessi in sequenze di scrittura richieste. Imposta questo valore su **`1048576`** o sul valore predefinito del sistema operativo Windows, a seconda di quale sia il più alto.

- MaxRecvDataSegmentLengthcontrolla la dimensione massima del segmento di dati associato a una singola unità di dati di protocollo (PDU). Imposta questo valore su **262144** o sul valore predefinito del sistema operativo Windows, a seconda di quale sia il più alto.



> **Note**
>
> È possibile ottimizzare diversi software di backup per funzionare al meglio utilizzando diverse impostazioni iSCSI. Per verificare quali valori per questi parametri offriranno le migliori prestazioni, vedere la documentazione relativa al software di backup.

3. Aumentare il valore di timeout del disco, come mostrato di seguito:

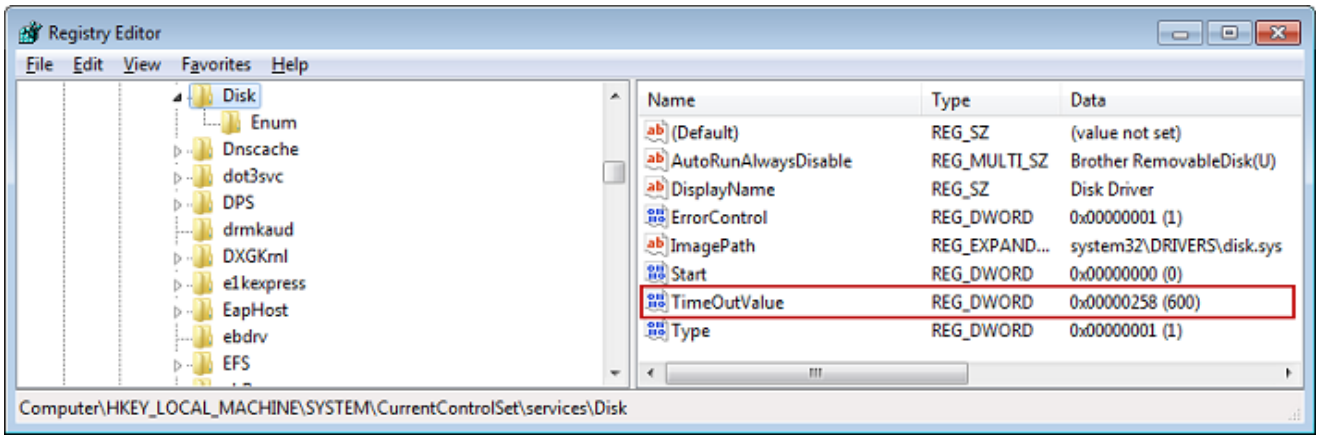
   a. Se non è già stato fatto, avviare l'editor del Registro di sistema (`Regedit.exe`).

   b. Accedere alla sottochiave Disk nella sottochiave Services di CurrentControlSet, illustrata di seguito.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

c. Aprite il menu contestuale (con il pulsante destro del mouse) per il valore TimeOutValueDWORD (32 bit), scegliete Modifica, quindi modificate il valore in. **`600`**

   TimeOutValuespecifica per quanti secondi l'iniziatore iSCSI aspetterà una risposta dalla destinazione prima di tentare il ripristino della sessione interrompendo e ristabilendo la connessione. Questo valore rappresenta un periodo di timeout di 600 secondi, come illustrato nell'esempio seguente.



4. Perché i nuovi valori di configurazione vengano applicati, riavviare il sistema.

   Prima di riavviare, è necessario accertarsi che i risultati di tutte le operazioni di scrittura nei volumi vengano scaricate. A questo scopo, portare offline tutti i dischi del volume di storage mappati prima di riavviare.

Personalizzazione delle impostazioni iSCSI di Linux

Dopo aver configurato l'iniziatore del tuo gateway, ti consigliamo di personalizzare le impostazioni iSCSI per impedire all'iniziatore di disconnettersi dalle destinazioni. Aumentando i valori di timeout iSCSI come mostrato di seguito, l'applicazione sarà in grado di gestire meglio le operazioni di scrittura che richiedono molto tempo e altri problemi temporanei, come le interruzioni di rete.

> **Note**
>
> I comandi possono essere leggermente diversi per altri tipi di Linux. Gli esempi seguenti sono basati su Red Hat Linux.

Per personalizzare le impostazioni iSCSI di Linux

1. Aumentare il tempo massimo durante il quale lasciare in coda le richieste.

   a. Aprire il file `/etc/iscsi/iscsid.conf` e individuare le righe seguenti.

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. Impostare il valore *[replacement_timeout_value]* su **600**.

   Impostare il valore *[noop_out_interval_value]* su **60**.

   Impostare il valore *[noop_out_timeout_value]* su **600**.

   Tutti e tre i valori sono espressi in secondi.

   > **Note**
   >
   > Le impostazioni di `iscsid.conf` devono essere configurate prima di individuare il gateway. Se hai già individuato il gateway o hai effettuato l'accesso alla destinazione (o hai eseguito entrambe le operazioni), puoi eliminare la voce dal database di individuazione tramite il comando seguente. Puoi quindi individuare di nuovo il gateway o riaccedere per recuperare la nuova configurazione.
   >
   > ```
   > iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
   > ```

2. Aumentare i valori massimi per la quantità di dati che è possibile trasmettere in ogni risposta.

   a. Aprire il file `/etc/iscsi/iscsid.conf` e individuare le righe seguenti.

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   node.conn[0].iscsi.MaxRecvDataSegmentLength
    = [replacement_segment_length_value]
   ```

   b. Consigliamo i seguenti valori per ottenere prestazioni migliori. Il software di backup potrebbe essere ottimizzato per utilizzare valori diversi, quindi consultare la documentazione del software di backup per ottenere risultati ottimali.

Imposta il valore *[replacement_first_burst_length_value] su o sul valore predefinito del sistema* operativo Linux, a seconda di quale sia il più alto. **262144**

Imposta il valore *[replacement_max_burst_length_value]* su o sul valore predefinito del sistema operativo Linux, a seconda di quale sia il più alto. **1048576**

Imposta il valore *[replacement_segment_length_value]* su o sul valore predefinito del sistema operativo Linux, a seconda di quale sia il più alto. **262144**

> **Note**
>
> È possibile ottimizzare diversi software di backup per funzionare al meglio utilizzando diverse impostazioni iSCSI. Per verificare quali valori per questi parametri offriranno le migliori prestazioni, vedere la documentazione relativa al software di backup.

3. Riavviare il sistema perché i nuovi valori di configurazione vengano applicati.

   Prima di riavviare, è necessario accertarsi che i risultati di tutte le operazioni di scrittura nei volumi vengano scaricate. A tale scopo, smonta i nastri prima di riavviarli.

Personalizzazione delle impostazioni di Linux Disk Timeout per gateway di volumi

Se si utilizza un gateway di volumi, è possibile personalizzare le seguenti impostazioni di timeout del disco di Linux oltre alle impostazioni iSCSI descritte nella sezione precedente.

Per personalizzare le impostazioni di timeout di Linux

1. Aumentare il valore di timeout del disco nel file delle regole.

   a. Se si usa l'iniziatore RHEL 5, aprire il file `/etc/udev/rules.d/50-udev.rules` e individuare la riga seguente.

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   Poiché questo file delle regole non esiste negli iniziatori RHEL 6 o 7, è necessario crearlo usando la regola seguente.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Per modificare il valore di timeout in RHEL 6, utilizzare il seguente comando e quindi aggiungere le righe di codice mostrate sopra.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Per modificare il valore di timeout in RHEL 7, utilizzare il seguente comando e quindi aggiungere le righe di codice mostrate sopra.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. Impostare il valore *[timeout]* su **600**.

Questo valore rappresenta un timeout di 600 secondi.

2. Riavviare il sistema perché i nuovi valori di configurazione vengano applicati.

Prima di riavviare, è necessario accertarsi che i risultati di tutte le operazioni di scrittura nei volumi vengano scaricate. A questo scopo, smontare i volumi di storage prima di riavviare.

3. È possibile testare la configurazione usando il comando seguente.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

Questo comando mostra le regole udev applicate al dispositivo iSCSI.

Configurazione dell'autenticazione CHAP per le destinazioni iSCSI

Storage Gateway supporta l'autenticazione tra il gateway e gli iniziatori iSCSI utilizzando Challenge-Handshake Authentication Protocol (CHAP). CHAP fornisce protezione dagli attacchi di riproduzione verificando periodicamente l'identità di un iniziatore iSCSI autenticato per accedere a un volume e a un dispositivo di destinazione VTL.

> **Note**
>
> La configurazione CHAP è facoltativa, ma fortemente consigliata.

Per configurare l'autenticazione CHAP, è necessario eseguire l'operazione sia nella console Storage Gateway che nel software dell'iniziatore iSCSI usato per la connessione alla destinazione. Storage Gateway usa l'autenticazione CHAP reciproca, ovvero l'iniziatore autentica la destinazione e la destinazione autentica l'iniziatore.

Per configurare l'autenticazione CHAP reciproca per le destinazioni

1. Configurare l'autenticazione CHAP nella console Storage Gateway come illustrato in Per configurare il protocollo CHAP per un dispositivo VTL nella console Storage Gateway.
2. Nel software dell'iniziatore client completare la configurazione dell'autenticazione CHAP:
   - Per configurare l'autenticazione CHAP reciproca in un client Windows, consulta Per configurare l'autenticazione CHAP reciproca in un client Windows.
   - Per configurare l'autenticazione CHAP reciproca in un client Red Hat Linux, consulta Per configurare l'autenticazione CHAP reciproca in un client Red Hat Linux.

Per configurare il protocollo CHAP per un dispositivo VTL nella console Storage Gateway

In questa procedura è necessario specificare due chiavi segrete che vengono usate per leggere e scrivere in un nastro virtuale. Le stesse chiavi vengono usate nella procedura per configurare l'iniziatore client.

1. Nel riquadro di navigazione, scegliere Gateways.
2. Scegliere il gateway e quindi scegliere la scheda VTL Devices (Dispositivi VTL) per visualizzare tutti i dispositivi VTL.
3. Scegliere il dispositivo per il quale si desidera configurare CHAP.
4. Fornire le informazioni richieste nella finestra di dialogo Configure CHAP Authentication (Configura autenticazione CHAP).
   a. Per Initiator Name (Nome iniziatore) digitare il nome dell'iniziatore iSCSI. Questo nome è un nome qualificato Amazon iSCSI (IQN) preceduto da `iqn.1997-05.com.amazon:` un nome di destinazione. Di seguito è riportato un esempio.

      `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

      È possibile trovare il nome dell'iniziatore usando il software dell'iniziatore iSCSI. Per i client Windows, ad esempio, il nome è il valore nella scheda Configuration (Configurazione)

dell'iniziatore iSCSI. Per ulteriori informazioni, consulta Per configurare l'autenticazione CHAP reciproca in un client Windows.

> **Note**
>
> Per modificare il nome di un iniziatore, è prima necessario disabilitare CHAP, modificare il nome dell'iniziatore nel software dell'iniziatore iSCSI e quindi abilitare CHAP con il nuovo nome.

b. Per Secret used to Authenticate Initiator (Segreto utilizzato per autenticare l'iniziatore), digitare il segreto richiesto.

   Questo segreto deve essere composto da un minimo di 12 caratteri e un massimo di 16 caratteri. Questo valore è la chiave segreta che l'iniziatore, ovvero il client Windows, deve conoscere per partecipare all'autenticazione CHAP con la destinazione.

c. Per Secret used to Authenticate Target (Mutual CHAP) (Segreto utilizzato per autenticare la destinazione - Autenticazione CHAP reciproca), digitare il segreto richiesto.

   Questo segreto deve essere composto da un minimo di 12 caratteri e un massimo di 16 caratteri. Questo valore è la chiave segreta che la destinazione deve conoscere per partecipare all'autenticazione CHAP con l'iniziatore.

> **Note**
>
> Il segreto usato per autenticare la destinazione deve essere diverso dal segreto usato per autenticare l'iniziatore.

d. Selezionare Salva.

5. Nella scheda VTL Devices (Dispositivi VTL) verificare che il campo relativo all'autenticazione CHAP iSCSI sia impostato su true.

Per configurare l'autenticazione CHAP reciproca in un client Windows

In questa procedura configuri l'autenticazione CHAP nell'iniziatore iSCSI Microsoft usando le stesse chiavi usate per configurare l'autenticazione CHAP per il volume nella console.

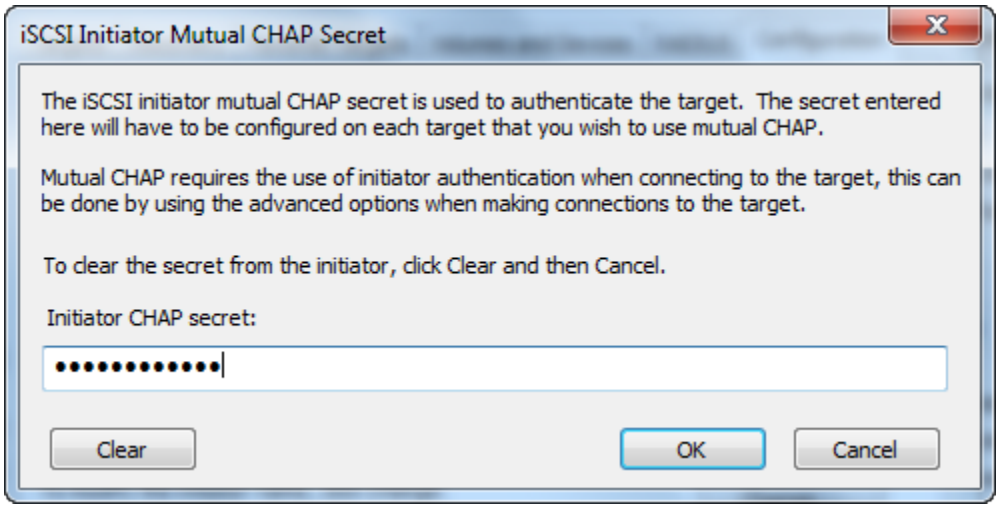
1. Se l'iniziatore iSCSI non è già stato avviato, nel menu Start del computer client Windows scegliere Run (Esegui), digitare **`iscsicpl.exe`** e quindi scegliere OK per eseguire il programma.
2. Configurare l'autenticazione CHAP reciproca per l'iniziatore (client Windows):

   a. Scegli la scheda Configurazione.

   > **Note**
   >
   > Il valore in Initiator Name (Nome iniziatore) è univoco per l'iniziatore e l'azienda. Il nome mostrato in precedenza corrisponde al valore usato nella finestra di dialogo Configure CHAP Authentication (Configura autenticazione CHAP) della console Storage Gateway.
   > Il nome visualizzato nell'immagine di esempio è solo per scopo dimostrativo.

   b. Scegli CHAP.

   c. Nella finestra di dialogo iSCSI Initiator Mutual Chap Secret (Segreto autenticazione CHAP reciproca iniziatore iSCSI) digitare il valore del segreto per l'autenticazione CHAP reciproca.

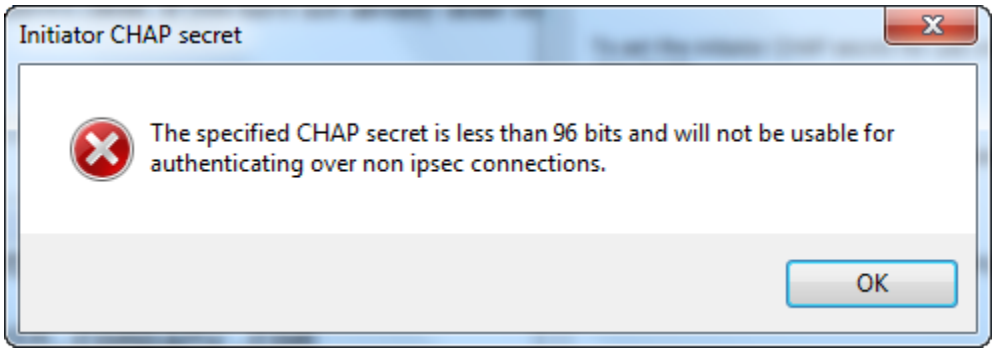


   In questa finestra di dialogo è necessario immettere il segreto che l'iniziatore (client Windows) usa per autenticare la destinazione (volume di storage). Questo segreto permette al target di leggere e scrivere nell'iniziatore. Questo segreto corrisponde al segreto digitato nella casella Secret used to Authenticate Target (Mutual CHAP) (Segreto utilizzato per autenticare la destinazione - Autenticazione CHAP reciproca) nella finestra di dialogo

Configure CHAP Authentication (Configura autenticazione CHAP). Per ulteriori informazioni, consulta Configurazione dell'autenticazione CHAP per le destinazioni iSCSI.

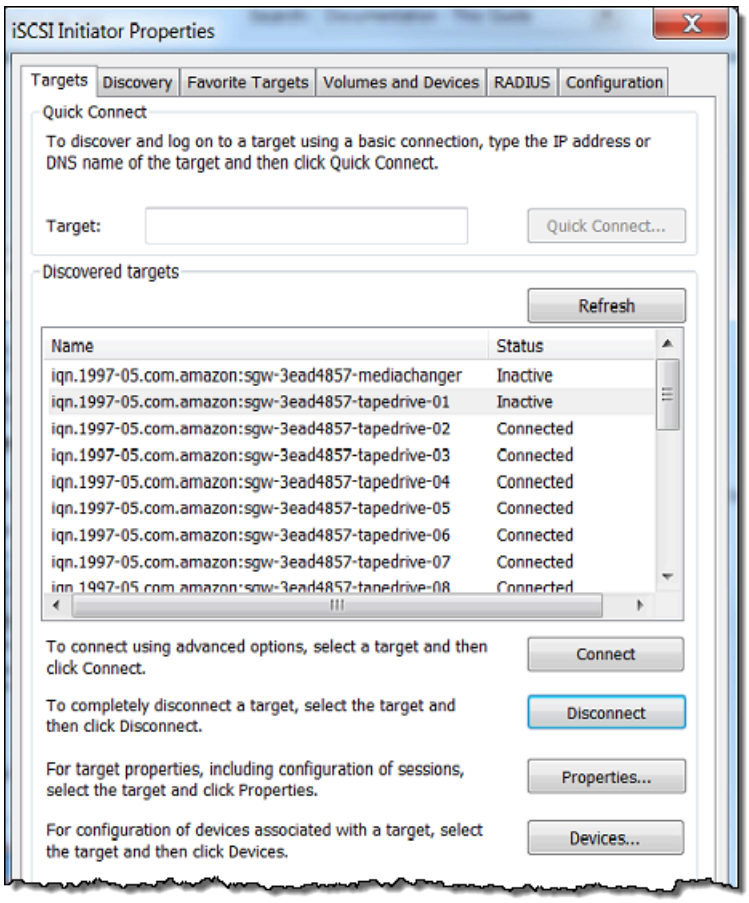
d. Se la chiave digitata è costituita da meno di 12 caratteri o più di 16 caratteri, viene visualizzata una finestra di dialogo di errore Initiator CHAP secret (Segreto CHAP iniziatore).

   Scegliere OK e quindi digitare di nuovo la chiave.



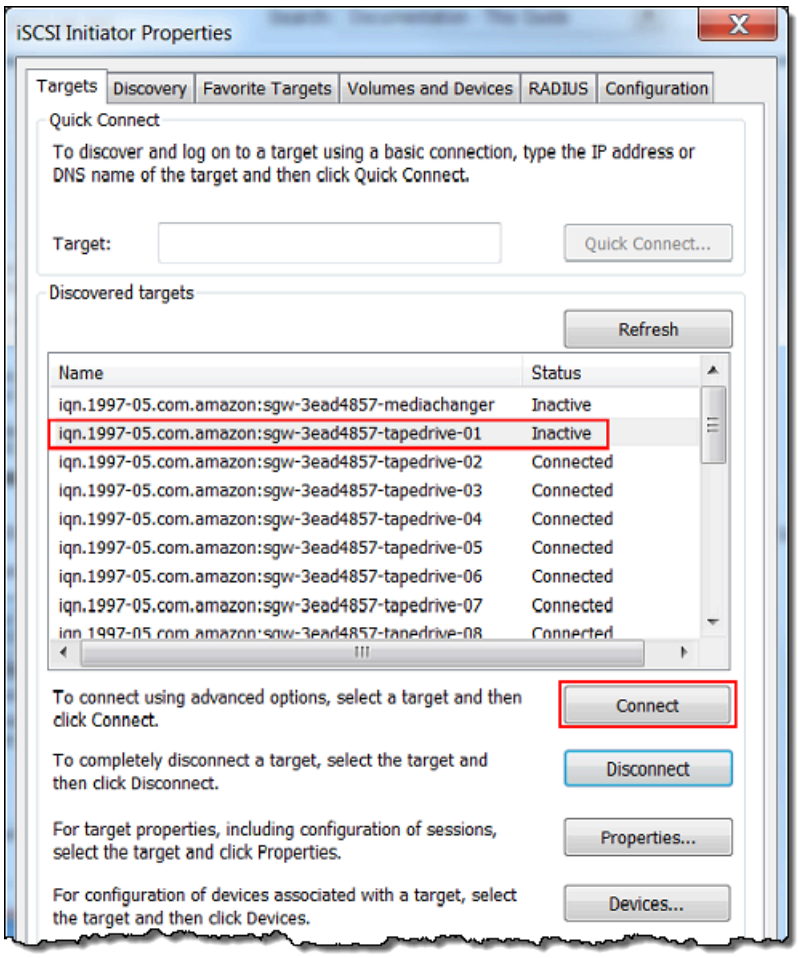
3. Configurare la destinazione con il segreto dell'iniziatore per completare la configurazione dell'autenticazione CHAP reciproca.

   a. Scegliere la scheda Destinazioni.

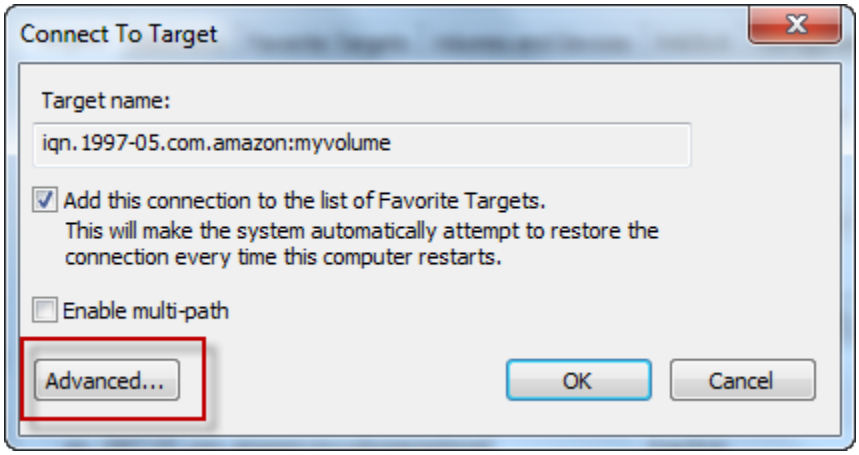


b. Se la destinazione che si desidera configurare per l'autenticazione CHAP è attualmente connessa, disconnetterla selezionandola e scegliendo Disconnect (Disconnetti).

c. Selezionare la destinazione da configurare per l'autenticazione CHAP e quindi scegliere Connect (Connetti).



d. Nella finestra di dialogo Connect to Target (Connetti a destinazione) scegliere Advanced (Avanzate).



e. Nella finestra di dialogo Advanced Settings (Impostazioni avanzate) configurare l'autenticazione CHAP.

i. Seleziona Attiva accesso CHAP.

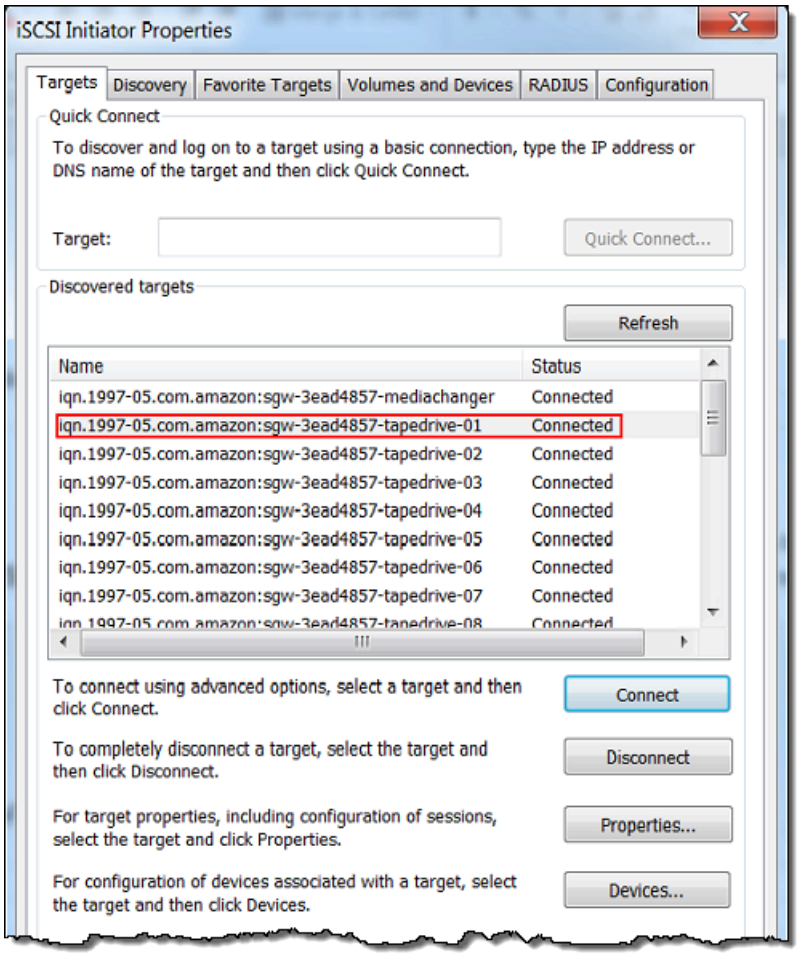
ii. Digitare il segreto necessario per autenticare l'iniziatore. Questo segreto corrisponde al segreto digitato nella casella Secret used to Authenticate Initiator (Segreto utilizzato per autenticare l'iniziatore) nella finestra di dialogo Configure CHAP Authentication (Configura autenticazione CHAP). Per ulteriori informazioni, consulta Configurazione dell'autenticazione CHAP per le destinazioni iSCSI.

iii. Selezionare Perform mutual authentication (Esegui autenticazione reciproca).

iv. Per applicare le modifiche, scegliere OK.

f. Nella finestra di dialogo Connect To Target (Connetti a destinazione) scegliere OK.

4. Se è stata fornita la chiave segreta corretta, lo stato della destinazione è Connected (Connesso).



Per configurare l'autenticazione CHAP reciproca in un client Red Hat Linux

In questa procedura configuri l'autenticazione CHAP nell'iniziatore iSCSI Linux usando le stesse chiavi usate per configurare l'autenticazione CHAP per il volume nella console Storage Gateway.

1. Verificare che il daemon iSCSI sia in esecuzione e di essere già connessi a una destinazione. Se non avete completato queste due attività, consultate Linux.
2. Disconnettere e rimuovere eventuali configurazioni esistenti per la destinazione per la quale si sta per configurare l'autenticazione CHAP.

   a. Per trovare il nome della destinazione e verificare che si tratti di una configurazione definita, visualizzare l'elenco delle configurazioni salvate usando il comando seguente.

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. Disconnettersi dalla destinazione.

   Il comando seguente permette di disconnettersi dalla destinazione denominata **myvolume** definita nel nome completo iSCSI (IQN) Amazon. Modificare il nome della destinazione e il nome IQN in base alla situazione specifica.

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. Rimuovere la configurazione per la destinazione.

   Il comando seguente rimuove la configurazione per la destinazione **myvolume**.

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. Modificare il file di configurazione iSCSI per abilitare CHAP.

   a. Ottenere il nome dell'iniziatore, ovvero il client in uso.

   Il comando seguente ottiene il nome dell'iniziatore dal file `/etc/iscsi/initiatorname.iscsi`.

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   L'output di questo comando è simile al seguente:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. Apri il file `/etc/iscsi/iscsid.conf`.

c. Rimuovere il commento dalle righe seguenti nel file e specificare i valori corretti per *username*, *password*, *username_in* e *password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Per informazioni sui valori da specificare, consulta la tabella seguente.

Impostazione di configurazione	Valore
username	Nome dell'iniziatore individuato in una fase precedente in questa procedura. Il valore inizia con iqn. Ad esempio, **iqn.1994-05.com.redhat:8e89b27b5b8** è un valore *username* valido.
password	Chiave segreta usata per autenticare l'iniziatore (il client in uso) quando comunica con il volume.
username_in	Nome IQN del volume di destinazione. Il valore inizia con iqn e termina con il nome della destinazione. Ad esempio, **iqn.1997-05.com.amazon:myvolume** è un valore *username_in* valido.
password_in	Chiave segreta usata per autenticare la destinazione (il volume) quando comunica con l'iniziatore.

d. Salvare le modifiche nel file di configurazione e quindi chiudere il file.

4. Individuare la destinazione e accedervi. Per farlo, seguite i passaggi descritti in Connessione a un client Linux.

Utilizzo AWS Direct Connect con Storage Gateway

AWS Direct Connect collega la tua rete interna ad Amazon Web Services Cloud. Utilizzando AWS Direct Connect Storage Gateway, è possibile creare una connessione per esigenze di carichi di lavoro ad alta velocità, fornendo una connessione di rete dedicata tra il gateway locale e. AWS

Storage Gateway utilizza endpoint pubblici. Una volta AWS Direct Connect stabilita una connessione, è possibile creare un'interfaccia virtuale pubblica per consentire il routing del traffico verso gli endpoint Storage Gateway. L'interfaccia virtuale pubblica ignora i provider di servizi Internet nel percorso di rete. L'endpoint pubblico del servizio Storage Gateway può trovarsi nella stessa AWS regione della AWS Direct Connect posizione o in una AWS regione diversa.

La figura seguente mostra un esempio di come AWS Direct Connect funziona con Storage Gateway. architettura di rete che mostra Storage Gateway connesso al cloud tramite connessione AWS diretta.

La procedura seguente presuppone che è stato creato un funzionamento gateway.

Da utilizzare AWS Direct Connect con Storage Gateway

1. Crea e stabilisci una AWS Direct Connect connessione tra il data center locale e l'endpoint Storage Gateway. Per ulteriori informazioni su come creare una connessione, consulta Nozioni di base su AWS Direct Connect nella Guida per l'utente di AWS Direct Connect .
2. Connect l'appliance Storage Gateway locale al AWS Direct Connect router.
3. Creare un'interfaccia virtuale pubblica e configurare il router locale di conseguenza. Anche con Direct Connect, gli endpoint VPC devono essere creati con HAProxy. Per ulteriori informazioni, consulta Creazione di un'interfaccia virtuale nella Guida per l'utente di AWS Direct Connect .

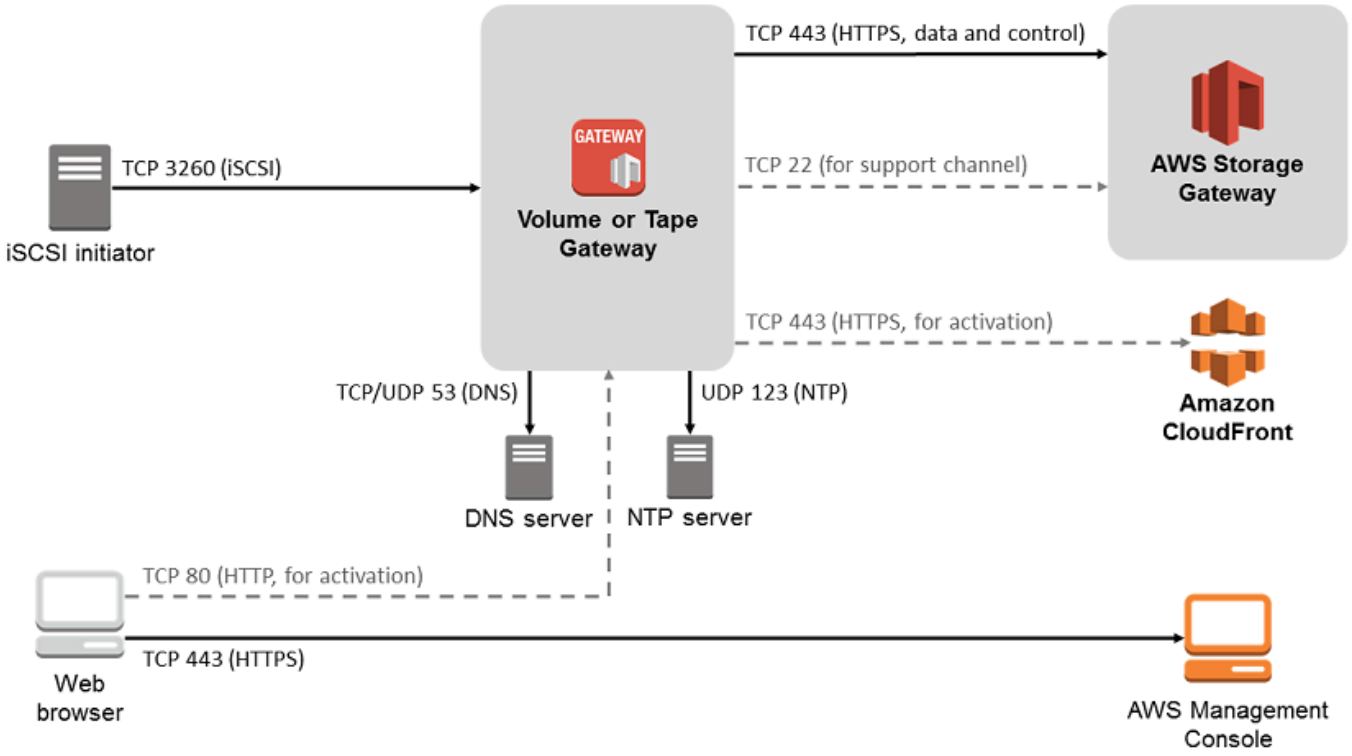
Per ulteriori informazioni AWS Direct Connect, consulta What is? AWS Direct Connect nella Guida AWS Direct Connect per l'utente.

Requisiti porta

Per il corretto funzionamento di Storage Gateway, sono necessarie le porte seguenti. Alcune porte sono comuni e necessarie per tutti i tipi di gateway. Altre porte sono necessarie per determinati tipi di gateway. In questa sezione, puoi trovare un'illustrazione e un elenco delle porte richieste per il gateway di nastri virtuali.

Gateway di nastri virtuali

La figura seguente mostra tutte le porte che devi aprire per il funzionamento dei gateway di nastri virtuali.



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

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Macchina virtuale Storage Gateway	AWS	TCP (Transmission Control Protocol)	443 (HTTPS)	Per la comunicazione da una macchina virtuale in uscita dello Storage Gateway a un endpoint di AWS servizio. Per informazioni	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
				sugli endpoint del servizio, consulta Consentire AWS Storage Gateway l'accesso tramite firewall e router.	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Browser	Macchina virtuale Storage Gateway	TCP	80 (HTTP)	Dai sistemi locali per ottenere la chiave di attivazione di Storage Gateway. La porta 80 viene usata durante l'attivazione di un'applia nce Storage Gateway. Per una macchina virtuale Storage Gateway la porta 80 non deve essere accessibile pubblicam ente. Il livello di accesso richiesto alla porta 80 dipende dalla configura zione di rete. Se attivi il gateway dalla console di	

Da	Per	Protocollo	Porta	Modalità di utilizzo	
				gestione Storage Gateway, l'host da cui ti colleghi alla console deve avere accesso alla porta 80 del gateway.	
Macchina virtuale 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	
Macchina virtuale Storage Gateway	AWS	TCP	22 (Canale di supporto)	Consente di accedere AWS Support al gateway per facilitare la risoluzione dei 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	
Macchina virtuale 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.	

Oltre alle porte comuni, i gateway di nastri virtuali richiedono le seguenti porte.

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Iniziatori iSCSI	Macchina virtuale Storage Gateway	TCP	3260 (iSCSI)	Da sistemi locali per connettersi alle destinazioni iSCSI esposte da un gateway.	

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: Ottenere un indirizzo IP da un host Amazon EC2

Quando individui l'indirizzo IP, annotalo. Quindi torna alla console Storage Gateway e digita l'indirizzo IP nella console.

Ottenere un indirizzo IP da un host Amazon EC2

Per ottenere l'indirizzo IP dell'istanza Amazon EC2 su cui il gateway viene distribuito, collegarsi alla console locale dell'istanza EC2. Quindi ottenere l'indirizzo IP nella parte superiore della pagina della console. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.

È possibile anche recuperare l'indirizzo IP dalla console di gestione Amazon EC2. Consigliamo di usare l'indirizzo IP pubblico per l'attivazione. Per ottenere l'indirizzo IP pubblico, utilizzare la procedura 1. Se si sceglie invece di utilizzare l'indirizzo IP elastico, consulta la procedura 2.

Procedura 1: per connettersi al gateway utilizzando l'indirizzo IP pubblico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza EC2 sulla quale è distribuito il gateway.
3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare l'indirizzo IP pubblico. Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP.

Per utilizzare l'indirizzo IP elastico per l'attivazione, procedere nel modo seguente.

Procedura 2: per connettersi al gateway utilizzando l'indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza EC2 sulla quale è distribuito il gateway.
3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare il valore Elastic IP (IP elastico). Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP elastico.

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.

Informazioni sulle risorse e sugli ID delle risorse di Storage Gateway

In Storage Gateway, la risorsa principale è un gateway ma altri tipi di risorse includono: volume, nastro virtuale, destinazione iSCSI e dispositivo vtl. In questo caso, si parla di risorse secondarie, che non esistono a meno che non siano state associate a un gateway.

Alle risorse e alle 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 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`*

Tipo di risorsa	Formato ARN
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 delle risorse di Storage Gateway sono in lettere maiuscole. Tuttavia, quando si utilizzano questi ID risorsa con l'API Amazon EC2, Amazon 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.

Tagging per 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.

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 all' AWS uso.
- I caratteri validi per la proprietà di chiave sono lettere e numeri UTF-8, spazi e i caratteri speciali + - = . _ : / e @.

Lavorare con i tag

È possibile lavorare con i tag utilizzando la console Storage Gateway, l'API di Storage Gateway o l'interfaccia a riga di comando (CLI) Storage Gateway. Le procedure seguenti illustrano come aggiungere, modificare ed eliminare un tag dalla console.

Per aggiungere un tag

1. Apri la console Storage Gateway all'indirizzo https://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. Apri la console Storage Gateway all'indirizzo https://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. Apri la console Storage Gateway all'indirizzo https://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).

Uso di componenti open source per AWS Storage Gateway

Questa sezione descrive gli strumenti e le licenze di terze parti da cui dipendiamo per fornire la funzionalità Storage Gateway.

Il codice sorgente per determinati componenti software open source inclusi con il software AWS Storage Gateway è disponibile per il download agli indirizzi seguenti:

- Per i gateway distribuiti su VMware ESXi, scarica sources.tar
- Per i gateway distribuiti su Microsoft Hyper-V, scaricare sources_hyperv.tar
- Per i gateway distribuiti su macchina virtuale basata su kernel (KVM) Linux, scaricare Sources_kvm.tar

Questo prodotto include il software sviluppato da OpenSSL Project per l'uso nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consultare Licenze di terze parti.

AWS Storage Gateway quote

In questa sezione puoi trovare informazioni sulle quote di volume e nastro, configurazione e prestazioni per Storage Gateway.

Argomenti

- Quote per nastri
- Dimensioni disco locale consigliate per il gateway

Quote per nastri

La tabella seguente elenca le quote per i nastri.

Descrizione	Gateway di nastri virtuali
La dimensione minima di un nastro virtuale	100 GiB
La dimensione massima di un nastro virtuale	15 TiB
Numero massimo di nastri virtuali assegnati a un gateway	1.500
Dimensione totale di tutti i nastri virtuali assegnati a un gateway	1 PiB
Il numero massimo di nastri virtuali in archivio	Nessun limite
Dimensioni totali di tutti i nastri in un archivio	Nessun limite

Dimensioni disco locale 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)	Buffer di caricamento (minimo)	Buffer di caricamento (minimo)	Altri dischi locali richiesti
Gateway di nastri virtuali	150 GiB	64 TiB	150 GiB	2 TiB	—

Note

È possibile configurare una o più unità locali per la cache e il buffer di caricamento, fino alla capacità massima.

Quando aggiungi la cache o il buffer di caricamento 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 o come buffer di caricamento.

Riferimento API per Storage Gateway

Oltre a utilizzare la console, puoi utilizzare l' AWS Storage Gateway API per configurare e gestire i gateway in modo programmatico. Questa sezione descrive AWS Storage Gateway le operazioni, la richiesta di firma per l'autenticazione e la gestione degli errori. Per ulteriori informazioni sulle regioni e sugli endpoint disponibili per Storage Gateway, consulta AWS Storage Gateway Endpoint e quote nella Riferimenti generali di AWS.

> **Note**
>
> Puoi anche utilizzare gli AWS SDK per sviluppare applicazioni con AWS Storage Gateway. Gli AWS SDK per Java, .NET e PHP racchiudono l' AWS Storage Gateway API sottostante, semplificando le attività di programmazione. Per ulteriori informazioni sul download delle librerie SDK, consulta Librerie e codice di esempio.

Argomenti

Intestazioni obbligatorie delle richieste in Storage Gateway

Questa sezione descrive le intestazioni obbligatorie che devi inviare con ogni richiesta POST a 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 utilizzate 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 a Storage Gateway. Le intestazioni mostrate di seguito che iniziano con «x-amz» sono intestazioni specifiche. AWS Tutte le altre intestazioni elencate sono intestazioni comuni usate in transazioni HTTP.

Header	Descrizione
`Authorization`	L'intestazione di autorizzazione contiene diverse informazioni sulla richiesta, che permettono a Storage Gateway di 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, si YourAccessKeyspecificano l'anno, il mese e il giorno (aaaammgg), la regione e il. CalculatedSignature Il formato dell'intestazione di autorizzazione è dettato dai requisiti del processo di firma V4. AWS I dettagli sulla firma vengono approfonditi nell'argomento Firmare le richieste.
`Content-Type`	Usa `application/x-amz-json-1.1` come tipo di contenuto per tutte le richieste a Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Header	Descrizione
`Host`	Usa l'intestazione host per specificare l'endpoint Storage Gateway in cui invii la richiesta. Ad esempio, `storagegateway.us-east-2.amazonaws.com` è l'endpoint per la regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili per Storage Gateway, consulta Endpoint e quote AWS Storage Gateway nella Riferimenti generali di AWS. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	È necessario fornire il timestamp nell'intestazione HTTP o nell'`Date`intestazione. AWS `x-amz-date` (Alcune librerie client HTTP non consentono di impostare l'intestazione `Date`) Quando è presente un'intestazione `x-amz-date` , lo Storage Gateway ignora qualsiasi intestazione `Date` 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 OperationName (ad esempio ActivateGateway "«) può essere trovato dall'elenco delle API,. Riferimento API per Storage Gateway

Firmare le richieste

Storage Gateway richiede l'autenticazione con firma di ogni richiesta inviata. Per firmare una richiesta, è necessario calcolare una firma digitale utilizzando una funzione hash crittografica. Una funzione hash crittografica è una funzione che restituisce un valore hash univoco basato sull'input. L'input alla funzione hash include il testo della richiesta e la tua chiave di accesso segreta. La funzione hash restituisce un valore hash che includi nella richiesta come firma. La firma è parte dell'intestazione `Authorization` della richiesta.

Dopo aver ricevuto la richiesta, Storage Gateway ricalcola la firma utilizzando la stessa funzione hash e lo stesso input utilizzati per firmare la richiesta. Se la firma risultante corrisponde alla firma nella richiesta, Storage Gateway elabora la richiesta. In caso contrario, la richiesta viene respinta.

Storage Gateway supporta l'autenticazione con AWS Signature Version 4. La procedura per il calcolo di una firma può essere suddivisa in tre fasi:

- Fase 1. Creazione di una richiesta canonica

  Riorganizza la richiesta HTTP in un formato canonico. L'utilizzo di un formato canonico è necessario in quanto Storage Gateway utilizza quel formato quando ricalcola una firma da confrontare con quella che hai inviato.

- Fase 2: creazione di una stringa di firma

  Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata stringa di firma, è una concatenazione del nome dell'algoritmo hash, della data della richiesta, di una stringa di ambito credenziali e della richiesta in formato canonico creata nella fase precedente. La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

- Fase 3. Creazione di una firma

  Crea una firma per la tua richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input: la tua stringa di firma e una chiave derivata. La chiave derivata viene calcolata 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 Fase 1. Creazione di una richiesta canonica è:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

L'ultima riga della richiesta canonica è l'hash del corpo della richiesta. Nota inoltre la terza riga vuota nella richiesta canonica. Ciò è dovuto alla mancanza di parametri di query per questa API (o qualsiasi API di Storage Gateway).

La stringa di firma per Fase 2: creazione di una stringa di firma è:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La prima riga della stringa di firma è l'algoritmo, la seconda è il timestamp, la terza è l'ambito credenziali e l'ultima è un hash del formato della richiesta canonica in Fase 1.

Per Fase 3. Creazione di una firma, la chiave derivata può essere rappresentata come segue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Se viene utilizzata la chiave di accesso segreta, wjalrxutnfeMI/k7mdeng/ bPxRfi CYEXAMPLEKEY, la firma calcolata è:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

La fase finale consiste nel creare l'intestazione `Authorization`. Per la chiave di accesso di dimostrazione 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 AWS Storage Gateway fornisce informazioni di riferimento sugli errori. Questi errori sono rappresentati da un'eccezione di errore e da un codice di errore dell'operazione. L'eccezione

di errore `InvalidSignatureException`, ad esempio, viene restituita da qualsiasi risposta API in caso di problema con la firma della richiesta. Tuttavia, il codice di errore dell'operazione `ActivationKeyInvalid` viene restituito solo per l'ActivateGatewayAPI.

A seconda del tipo di errore, Storage Gateway può restituire solo un'eccezione oppure sia un'eccezione che un codice di errore dell'operazione. In Risposte agli errori vengono forniti esempi di risposte di errore.

Eccezioni

La tabella seguente elenca le eccezioni AWS Storage Gateway API. Quando un' AWS Storage Gateway operazione restituisce una risposta di errore, il corpo della risposta contiene una di queste eccezioni. `InternalServerError` e `InvalidGatewayRequestException` restituiscono uno dei messaggi Codici di errore delle operazioni dei codici di errore delle operazioni che forniscono il codice di errore dell'operazione specifico.

Eccezione	Messaggio	Codice di stato HTTP
`IncompleteSignatureException`	La firma specificata non è completa.	400 Richiesta non valida
`InternalFailure`	L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto sconosciuto.	500 - Errore interno del server
`InternalServerError`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	500 - Errore interno del server
`InvalidAction`	L'azione o l'operazione richiesta non è valida.	400 Richiesta non valida
`InvalidClientTokenId`	Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.	403 Non consentito

Eccezione	Messaggio	Codice di stato HTTP
`InvalidGatewayRequestException`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	400 Richiesta non valida
`InvalidSignatureException`	La firma di richiesta che abbiamo calcolato non corrisponde alla firma che hai fornito. Controlla la tua chiave di AWS accesso e il metodo di firma.	400 Richiesta non valida
`MissingAction`	Nella richiesta manca un parametro di un'azione o un'operazione.	400 Richiesta non valida
`MissingAuthenticationToken`	La richiesta deve contenere un ID chiave di AWS accesso valido (registrato) o un certificato X.509.	403 Non consentito
`RequestExpired`	La richiesta ha superato la data di scadenza o la data della richiesta (con margine di 15 minuti) oppure la data della richiesta è oltre 15 minuti nel futuro.	400 Richiesta non valida
`SerializationException`	Si è verificato un errore durante la serializzazione. Controllare che il formato del payload JSON sia corretto.	400 Richiesta non valida
`ServiceUnavailable`	La richiesta non è riuscita a causa di un errore temporaneo del server.	503 Service Unavailable (503 Servizio non disponibile)
`SubscriptionRequiredException`	L' AWS Access Key Id richiede un abbonamento per il servizio.	400 Richiesta non valida

Eccezione	Messaggio	Codice di stato HTTP
`ThrottlingException`	Velocità superata.	400 Richiesta non valida
`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 AWS Storage Gateway operativi 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.	CreateCachediVolume SCSI CreateStorediVolume SCSI
`InitiatorNotFound`	L'iniziatore specificato non è stato trovato.	DeleteChapCredentials
`DiskAlreadyAllocated`	Il disco specificato è già allocato.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediVolume SCSI
`DiskDoesNotExist`	Il disco specificato non esiste.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediVolume SCSI
`DiskSizeNotGigAligned`	Il disco specificato non è allineato ai gigabyte.	CreateStorediVolume SCSI
`DiskSizeGreaterThanVolumeMaxSize`	La dimensione del disco specificata è superiore alla dimensione massima del volume.	CreateStorediVolume SCSI

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.	CreateStorediVolume SCSI
`DuplicateCertificateInfo`	Le informazioni sul certificato specificate sono duplicate.	ActivateGateway

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 CreateCachediVolume SCSI CreateSnapshot CreateStorediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI 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 CreateCachediVolume SCSI CreateSnapshot CreateStorediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI 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 CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI 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 CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI 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 CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI

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 corretti.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI

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 corretto.	CreateStorediVolume SCSI

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`MaximumVolumeCountExceeded`	Il numero massimo di volumi è stato superato.	CreateCachediVolume SCSI CreateStorediVolume SCSI DescribeCachediVolumi SCSI DescribeStorediVolumi SCSI
`NetworkConfigurationChanged`	La configurazione di rete del gateway è stata modificata.	CreateCachediVolume SCSI CreateStorediVolume SCSI

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 CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumi SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumi SCSI

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Il gateway specificato non è aggiornato.	ActivateGateway
`SnapshotInProgressException`	Lo snapshot specificato è in corso.	DeleteVolume
`SnapshotIdInvalid`	Lo snapshot specificato non è valido.	CreateCachediVolume SCSI CreateStorediVolume SCSI
`StagingAreaFull`	L'area di gestione temporanea è piena.	CreateCachediVolume SCSI CreateStorediVolume SCSI

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`TargetAlreadyExists`	La destinazione specificata esiste già.	CreateCachediVolume SCSI CreateStorediVolume SCSI
`TargetInvalid`	La destinazione specificata non è valida.	CreateCachediVolume SCSI CreateStorediVolume SCSI DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	La destinazione specificata non è stata trovata.	CreateCachediVolume SCSI CreateStorediVolume SCSI 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 CreateCachediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteSnapshotSchedule DescribeCache DescribeCachediVolumi SCSI DescribeStorediVolumi SCSI DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Il volume specificato esiste già.	CreateCachediVolume SCSI CreateStorediVolume SCSI
`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 DescribeCachediVolumi SCSI DescribeSnapshotSchedule DescribeStorediVolumi SCSI UpdateSnapshotSchedule
`VolumeNotReady`	Il volume specificato non è pronto.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Risposte agli errori

Quando si verifica un errore, le informazioni dell'intestazione della risposta contengono:

- Tipo di contenuto: application/ -1.1 x-amz-json
- Un codice di stato HTTP `4xx` o `5xx` appropriato

Il corpo di una risposta di errore contiene informazioni relative all'errore. La risposta di errore di esempio seguente mostra la sintassi di output degli elementi della risposta comuni a tutte le risposte di errore.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

La tabella seguente illustra i campi della risposta di errore JSON mostrata nella sintassi precedente.

__type

Una delle eccezioni elencate in Eccezioni.

Tipo: stringa

error

Contiene dettagli dell'errore specifici dell'API. Negli errori generali, ovvero non specifici di un'API, queste informazioni sull'errore non vengono visualizzate.

Tipo: raccolta

errorCode

Uno dei codici di errore delle operazioni .

Tipo: stringa

errorDetails

Questo campo non viene usato nella versione corrente dell'API.

Tipo: stringa

message

Uno dei messaggi dei codici di errore delle operazioni.

Tipo: stringa

Esempi di risposta di errore

Il seguente corpo JSON viene restituito se si utilizza l'API DescribeStoredi SCSIVolumes 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 API di Storage Gateway, consulta Operazioni nel Riferimento API AWS Storage Gateway .

Cronologia dei documenti della Guida per l'utente per Gateway di nastri virtuali

- Versione API: 30-06-2013
- Ultimo aggiornamento della documentazione: 24 novembre 2020

La tabella seguente descrive le modifiche importanti introdotte in ogni versione della Guida per l'utente di AWS Storage Gateway dopo aprile 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Supporto obsoleto per Tape Gateway su Snowball Edge	Non è più possibile ospitare Tape Gateway su dispositivi Snowball Edge.	14 marzo 2024
Istruzioni aggiornate per testare la configurazione del gateway utilizzando applicazioni di terze parti	Le istruzioni per testare la configurazione del gateway utilizzando applicazioni di terze parti ora descrivono il comportamento previsto se il gateway si riavvia durante un processo di backup in corso. Per ulteriori informazioni, consulta Utilizzo del software di backup per testare la configurazione del gateway.	24 ottobre 2023
Allarmi consigliati CloudWatch aggiornati	L' CloudWatch `HealthNotifications` allarme ora si applica ed è consigliato per tutti i tipi di gateway e piattaforme host. Le impostazioni di configurazione consigliate sono state aggiornat	2 ottobre 2023

	e anche per `HealthNotifications` e `AvailabilityNotifications`. Per ulteriori informazioni, vedere Comprensione degli CloudWatch allarmi Comprendere .	
Dimensione massima del nastro aumentata a 15 TiB per i gateway di nastri virtuali	Inoltre, per i gateway di nastri virtuali, la dimensione massima di un nastro virtuale è ora aumentata da 5 TiB a 15 TiB. Per ulteriori informazioni, consulta Quote per i nastri virtuali nella Guida per l'utente di Storage Gateway.	4 ottobre 2022
Guide utente separate per gateway di nastri virtuali e di volumi	La Guida per gli utenti di Storage Gateway, che in precedenza conteneva informazioni sui tipi di gateway di nastri virtuali e di volumi, è stata suddivisa in Guida per gli utenti di gateway di nastri virtuali e Guida per gli utenti di gateway di volumi, ognuna contenente informazioni su un solo tipo di gateway. Per ulteriori informazioni, vedere la Guida per l'utente di gateway di nastri virtuali e la Guida per l'utente di gateway di volumi.	23 marzo 2022

Procedure di creazione del gateway aggiornate	Le procedure per la creazione di tutti i tipi di gateway utilizzando la console Storage Gateway sono state aggiornate. Per ulteriori informazioni, consulta Creazione del gateway.	18 gennaio 2022
Nuova interfaccia Tapes	La pagina di panoramica dei nastri nella AWS Storage Gateway console è stata aggiornata con nuove funzionalità di ricerca e filtro. Tutte le procedure pertinenti in questa guida sono state aggiornate per descrivere la nuova funzionalità. Per ulteriori informazioni, consulta Gestione del gateway di nastri virtuali.	23 settembre 2021
Supporto per Quest NetVault Backup 13 per Tape Gateway	I Tape Gateway ora supportano Quest NetVault Backup 13 in esecuzione su Microsoft Windows Server 2012 R2 o Microsoft Windows Server 2016. Per ulteriori informazioni, consulta Testare la configurazione utilizzando Quest NetVault Backup.	22 agosto 2021

Argomenti del gateway di file S3 rimossi dalle guide per gateway di nastri virtuali e gateway di volumi	Per aiutare a rendere le guide utente dei gateway di nastri virtuali e dei gateway di volumi più facili da seguire per i clienti che configurano i rispettiv i tipi di gateway, sono stati rimossi alcuni argomenti non necessari.	21 luglio 2021
Supporto per IBM Spectrum Protect 8.1.10 su Windows e Linux per gateway di nastri virtuali	I gateway di nastri virtuali ora supportano IBM Spectrum Protect versione 8.1.10 in esecuzione su Microsoft Windows Server e Linux. Per ulteriori informazioni, consulta Test della configura zione mediante IBM Spectrum Protect.	24 novembre 2020
Conformità agli standard FedRAMP	Storage Gateway è ora conforme a FedRAMP. Per ulteriori informazioni, vedere Convalida della conformità per Storage Gateway Gateway.	24 novembre 2020
Limitazione della larghezza di banda basata sulla pianifica zione	Storage Gateway ora supporta la limitazione della larghezza di banda basata sulla pianifica zione per i gateway di nastri virtuali e di volumi. Per ulteriori informazioni, vedere Pianifica zione della limitazione della larghezza di banda utilizzando la console Storage Gateway.	9 novembre 2020

Aumento di 4 volte dello storage della cache locale del volume e dei gateway di nastri virtuali	Storage Gateway ora supporta una cache locale fino a 64 TB per i gateway di volumi e per i gateway di nastri virtuali memorizzati nella cache, migliorando le prestazioni per le applicazioni on-premis e fornendo un accesso a bassa latenza a set di dati di lavoro più grandi. Per ulteriori informazioni, vedere Dimensioni dei dischi locali consigliate per il gateway.	9 novembre 2020
Migrazione del gateway	Storage Gateway ora supporta la migrazione dei gateway di volumi memorizzati nella cache verso nuove macchine virtuali. Per ulteriori informazi oni, consulta Spostamento dei volumi memorizzati nella cache su una nuova macchina virtuale del gateway di volumi memorizzato nella cache.	10 settembre 2020

Support per il blocco della conservazione del nastro e la protezione del nastro write-once-read-many (WORM)	Storage Gateway supporta il blocco della conservazione dei nastri su nastri virtuali e la funzionalità WORM (Write Once Read Many). Tape Retention Lock consente di specificare la modalità e il periodo di conservazione sui nastri virtuali archiviati, evitando che vengano eliminati per un periodo di tempo fisso fino a 100 anni. Include controlli di autorizzazione su chi può eliminare i nastri o modificare le impostazioni di conservazione. Per ulteriori informazioni, consulta l'argomento relativo all'utilizzo di Tape Retention Lock. I nastri virtuali attivati da worm aiutano a garantire che i dati sui nastri attivi nella libreria di nastri virtuali non possano essere sovrascritti o cancellati. Per ulteriori informazioni, vedere Write Once, Read Many (WORM) Tape Protection.	19 agosto 2020
Ordinare l'appliance hardware tramite la console	È ora possibile ordinare l'appliance hardware tramite la AWS Storage Gateway console. Per ulteriori informazioni, consulta Utilizzo dell'appliance hardware Storage Gateway.	12 agosto 2020

Supporto per gli endpoint Federal Information Processing Standard (FIPS) in nuove regioni AWS	È ora possibile attivare un gateway con endpoint FIPS nelle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon) e Canada (Centrale). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway nella Riferimenti generali di AWS.	31 luglio 2020
Migrazione del gateway	Storage Gateway ora supporta la migrazione dei gateway di nastri virtuali e di volumi archiviati verso nuove macchine virtuali. Per ulteriori informazioni, vedere Spostamento dei dati su un nuovo gateway gateway.	31 luglio 2020
Visualizza gli CloudWatch allarmi Amazon nella console Storage Gateway	È ora possibile visualizzare gli CloudWatch allarmi nella console Storage Gateway.	29 maggio 2020

Supporto per gli endpoint Federal Information Processing Standard (FIPS)	Puoi ora attivare un gateway con endpoint FIPS nelle regioni AWS GovCloud (US) . Per scegliere un endpoint FIPS per un gateway di volumi, consulta Scelta di un endpoint di servizio. Per scegliere un endpoint FIPS per un gateway di nastri virtuali, consulta Connessione del gateway di nastri virtuali a AWS.	22 maggio 2020
Nuove regioni AWS	Storage Gateway è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway nella Riferimenti generali di AWS.	7 maggio 2020

Supporto per classe di storage S3 Intelligent-Tiering	Storage Gateway ora supporta la classe di archiviazione S3 Intelligent-Tiering. La classe di storage S3 Intelligent-Tiering è progettata per ottimizzare i costi dello storage spostando automaticamente i dati sul livello di accesso di storage più conveniente, senza impatto sulle prestazioni o sovraccarico operativo. Per ulteriori informazioni, consulta Classe di archiviazione per l'ottimizzazione automatica degli oggetti a cui si accede frequentemente e raramente nella Guida per l'utente di Amazon Simple Storage Service.	30 aprile 2020
Raddoppio delle prestazioni di scrittura e lettura del gateway di nastri virtuali	Storage Gateway migliora le prestazioni di lettura e scrittura da nastri virtuali sul gateway di nastri virtuali, raddoppiandone la velocità e consentendoti così di accelerare l'esecuzione di backup e ripristino. Per ulteriori informazioni, consulta Guida alle prestazioni dei gateway di nastri virtuali nella Guida per l'utente di Storage Gateway.	23 aprile 2020

Supporto per la creazione automatica di nastri	Storage Gateway offre ora la possibilità di creare automaticamente nuovi nastri virtuali. Il gateway di nastri virtuali crea automaticamente nuovi nastri virtuali per mantenere il numero minimo di nastri disponibili da te configurati e rende quindi questi nuovi nastri disponibili per l'importazione da parte dell'applicazione di backup, agevolando l'esecuzione dei processi di backup senza interruzioni. Per ulteriori informazioni, consulta Creazione automatica di nastri nella Guida per l'utente di Storage Gateway.	23 aprile 2020
Nuova AWS regione	Storage Gateway è ora disponibile nella regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway in Riferimenti generali di AWS.	12 marzo 2020

Supporto per hypervisor macchina virtuale basata su kernel (KVM) Linux	Storage Gateway offre ora la possibilità di distribuire un gateway on-premise nella piattaforma di virtualizzazione KVM. I gateway distribuiti in KVM hanno tutte le stesse funzionalità e caratteristiche dei gateway on-premise esistenti. Per ulteriori informazioni, consulta l'argomento relativo agli Hypervisor supportati e requisiti host nella Guida per l'utente di Storage Gateway.	4 febbraio 2020
Supporto per VMware vSphere High Availability	Storage Gateway ora fornisce il supporto per la disponibilità elevata su VMware per proteggere i carichi di lavoro di archiviazione da errori di hardware, hypervisor o rete. Per ulteriori informazioni, consulta l'argomento relativo all'Utilizzo di VMware vSphere High Availability con Storage Gateway nella Guida per l'utente di Storage Gateway. Questa versione include inoltre i miglioramenti delle prestazioni. Per ulteriori informazioni, consulta Prestazioni nella Guida per l'utente di Storage Gateway.	20 novembre 2019

Nuova AWS regione per Tape Gateway	Il gateway di nastri virtuali è ora disponibile nella regione Sud America (San Paolo). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway in Riferimenti generali di AWS.	24 settembre 2019
Supporto per IBM Spectrum Protect versione 7.1.9 su Linux e una dimensione massima del nastro aumentata a 5 TiB per i gateway di nastri virtuali	I gateway di nastri virtuali ora supportano IBM Spectrum Protect (Tivoli Storage Manager) versione 7.1.9 in esecuzione su Linux, oltre all'esecuzione su Microsoft Windows. Per ulteriori informazioni, consulta Test della configurazione mediante IBM Spectrum Protect nella Guida per l'utente di Storage Gateway. Inoltre, per i gateway di nastri virtuali, la dimensione massima di un nastro virtuale è ora aumentata da 2,5 TiB a 5 TiB. Per ulteriori informazioni, consulta Quote per i nastri virtuali nella Guida per l'utente di Storage Gateway.	10 settembre 2019

Support per Amazon CloudWatch Logs	Ora puoi configurare File Gateway con Amazon CloudWatch Log Groups per ricevere notifiche sugli errori e sullo stato del gateway e delle sue risorse. Per ulteriori informazioni, consulta la sezione Getting Notified About Gateway Health and Errors with Amazon CloudWatch Log Groups nella Storage Gateway User Guide.	4 settembre 2019
Nuova AWS regione	Storage Gateway è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway in Riferimenti generali di AWS.	14 agosto 2019
Nuova AWS regione	Storage Gateway è ora disponibile nella regione Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Endpoint e quote AWS Storage Gateway in Riferimenti generali di AWS.	29 luglio 2019

Supporto per attivare un gateway in un cloud privato virtuale (VPC, Virtual Private Cloud)	È ora possibile attivare un gateway in un cloud privato virtuale. È possibile creare una connessione privata tra l'applicazione software locale e l'infrastruttura di storage basato sul cloud. Per ulteriori informazioni, vedere Activating a Gateway in a Virtual Private Cloud.	20 giugno 2019
Supporto per lo spostamento di nastri virtuali da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive	È ora possibile spostare i nastri virtuali che sono archiviati nella classe di archiviazione S3 Glacier Flexible Retrieval nella classe di archiviazione S3 Glacier Deep Archive per una conservazione dei dati conveniente e a lungo termine. Per ulteriori informazioni, consulta Spostamento di un nastro da S3 Glacier Flexible Retrieval a S3 Glacier Deep Archive.	28 maggio 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
Integrazione con S3 Glacier Deep Archive	Il gateway di nastri virtuali si integra con S3 Glacier Deep Archive. È ora possibile archiviare nastri virtuali in S3 Glacier Deep Archive per la conservazione dei dati a lungo termine. Per ulteriori informazioni, consulta Archiving Virtual Tapes.	27 marzo 2019

Disponibilità dell'appliance hardware Storage Gateway in Europa	L'appliance hardware Storage Gateway è ora disponibile in Europa. Per ulteriori informazioni, consulta Regioni hardware appliance AWS Storage Gateway in Riferimenti generali di AWS. Inoltre, ora è possibile aumentare lo storage utilizzabile sullo Storage Gateway 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
Integrazione con AWS Backup	Storage Gateway si integra con AWS Backup. Ora puoi utilizzarlo AWS Backup per eseguire il backup di applicazioni aziendali locali che utilizzano volumi Storage Gateway per lo storage basato sul cloud. Per ulteriori informazioni, consulta Backup dei volumi.	16 gennaio 2019

Supporto per Bacula Enterprise e IBM Spectrum Protect	I gateway di nastri virtuali ora supportano Bacula Enterprise e IBM Spectrum Protect. Storage Gateway ora supporta anche le versioni più recenti di Veritas NetBackup, Veritas Backup Exec e Quest backup. NetVault È ora possibile utilizzare queste applicazioni di backup per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Utilizzo del software di backup per testare la configurazione del gateway.	13 novembre 2018
Supporto per l'appliance hardware Storage Gateway	L'appliance hardware Storage Gateway 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, di nastri virtuali e di volumi. Per ulteriori informazioni, consulta Utilizzo dell'appliance hardware Storage Gateway.	18 settembre 2018

Compatibilità con Microsoft System Center 2016 Data Protection Manager (DPM)	I gateway di nastri virtuali sono ora compatibili con Microsoft System Center 2016 Data Protection Manager (DPM). È ora possibile utilizzare Microsoft DPM per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Test della configurazione utilizzando Microsoft System Center Data Protection Manager.	18 luglio 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 condivisioni file. Per ulteriori informazioni, consulta Creazione di una condivisione file.	20 giugno 2018

Supporto per la crittografia di condivisioni file, volumi nella cache e nastri virtuali	È ora possibile utilizzare AWS Key Management Service (AWS KMS) per crittografare i dati scritti su una condivisione di file, un volume memorizzato nella cache o un nastro virtuale. Al momento, questa operazione è possibile utilizzando l'API AWS Storage Gateway . Per maggiori informazioni, consulta Crittografia dei dati tramite AWS KMS.	12 giugno 2018
Support per NovaStor DataCenter /Network	I Tape Gateway ora supportano /Network. NovaStor DataCenter Ora puoi utilizzare NovaStor DataCenter / Network versione 6.4 o 7.1 per eseguire il backup dei dati su Amazon S3 e archiviarli direttamente nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Verifica della configurazione utilizzando / Network. NovaStor DataCenter	24 maggio 2018

Aggiornamenti precedenti

La tabella che segue descrive le modifiche importanti apportate a ogni versione della AWS Storage Gateway Guida per l'utente prima di maggio 2018.

Modifica	Descrizione	Data della modifica
Supporto per la classe di storage S3 One Zone_IA	Per i gateway di file puoi ora scegliere One Zone_IA in S3 come classe di storage predefinita per le condivisioni file. Usando questa classe di storage, puoi archiviare i dati degli oggetti in un'unica zona di disponibilità in Amazon S3. Per ulteriori informazioni, consulta Creazione di una condivisione file.	4 aprile 2018
Nuova regione	Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Singapore). Per informazioni dettagliate, consulta AWS Regioni.	3 Aprile 2018
Supporto per la notifica dell'aggiornamento della cache, i pagamenti a carico del richiedente e le liste di controllo degli accessi predefinite per bucket Amazon S3.	Con i gateway di file puoi ora ricevere notifiche quando il gateway completa l'aggiornamento della cache per il bucket Amazon S3. Per ulteriori informazioni, vedere RefreshCache.html nello Storage Gateway API Reference. I gateway di file permettono ora al richiedente o al lettore di pagare le tariffe di accesso al posto del proprietario del bucket. I gateway di file permettono ora di concedere il controllo completo al proprietario del bucket S3 mappato alla condivisione file NFS. Per ulteriori informazioni, consulta Creazione di una condivisione file.	1 marzo 2018
Support per Dell EMC NetWorker V9.x	I Tape Gateway ora supportano Dell EMC V9.x. NetWorker Ora puoi utilizzare Dell EMC NetWorker V9.x per eseguire il backup dei dati su Amazon S3 e archiviarli direttamente su storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Dell EMC. NetWorker	27 febbraio 2018

Modifica	Descrizione	Data della modifica
Nuova regione	Storage Gateway è ora disponibile nella regione Europa (Parigi). Per informazioni dettagliate, consulta AWS Regioni.	18 dicembre 2017
Supporto per la notifica di caricamento dei file e il rilevamento del tipo MIME	I gateway di file ora possono inviare una notifica quando tutti i file scritti nella condivisione file NFS sono stati caricati in Amazon S3. Per ulteriori informazioni, vedere NotifyWhenUploadedlo Storage Gateway API Reference. I gateway di file permettono ora il rilevamento del tipo MIME per gli oggetti caricati in base alle estensioni dei file. Per ulteriori informazioni, consulta Creazione di una condivisione file.	21 Novembre 2017
Supporto per VMware ESXi Hypervisor versione 6.5	AWS Storage Gateway ora supporta 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, consulta Hypervisor supportati e requisiti di hosting.	13 settembre 2017
Compatibilità con Commvault 11	I gateway di nastri virtuali sono ora compatibili con Commvault 11. È ora possibile utilizzare Commvault per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Commvault.	12 settembre 2017
Supporto del gateway di file per l'hypervisor Microsoft Hyper-V	Puoi ora distribuire un gateway di file in un hyperviso r Microsoft Hyper-V. Per informazioni, consulta Hypervisor supportati e requisiti di hosting.	22 giugno 2017

Modifica	Descrizione	Data della modifica
Supporto per il recupero dei nastri in tre-cinque ore dall'archivio	Per un gateway di nastri virtuali puoi ora recuperare i nastri dall'archivio in tre-cinque ore. Puoi anche determinare la quantità di dati scritti nel nastro dall'applicazione di backup o dalla libreria di nastri virtuali (VTL). Per ulteriori informazioni, consulta Visualizzazione dell'utilizzo del nastro.	23 maggio 2017
Nuova regione	Storage Gateway è ora disponibile nella regione Asia Pacifico (Mumbai). Per informazioni dettagliate, consulta AWS Regioni.	02 maggio 2017
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, consulta 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 l'API Reference. RefreshCache	28 marzo 2017
Supporto per la clonazione di un volume	Per i Volume Gateway memorizzati nella cache, AWS Storage Gateway ora supporta la possibilità di clonare un volume da un volume esistente. Per ulteriori informazioni, consulta Clonazione di un volume.	16 marzo 2017

Modifica	Descrizione	Data della modifica
Supporto per i gateway di file in Amazon EC2	AWS Storage Gateway ora offre la possibilità di implementare un File Gateway in Amazon EC2. Puoi avviare un gateway di file in Amazon EC2 usando l'Amazon Machine Image (AMI) Storage Gateway ora disponibile come AMI della community. Per informazioni su come creare un gateway di file e distribuirlo su un'istanza EC2, consulta Creare e attivare un gateway di file Amazon S3 o Creare e attivare un gateway di file Amazon FSx. Per informazioni su come avviare un gateway di file AMI, consulta Implementazione di un gateway di file S3 su un host Amazon EC2 o Implementazione di un gateway di file FSx su un host Amazon EC2.	08 febbraio 2017
Compatibilità con Arcserve 17	Il gateway di nastri virtuali è ora compatibile con Arcserve 17. Ora puoi usare Arcserve per eseguire il backup dei dati in Amazon S3 e archiviarli direttamente in S3 Glacier Flexible Retrieval. Per ulteriori informazioni, vedere Test della configurazione utilizzando Arcserve Backup r17.0.	17 gennaio 2017
Nuova regione	Storage Gateway è ora disponibile nella regione Europa (Londra). Per informazioni dettagliate, consulta AWS Regioni.	13 dicembre 2016
Nuova regione	Storage Gateway è ora disponibile nella regione Canada (Centrale). Per informazioni dettagliate, consulta AWS Regioni.	08 dicembre 2016

Modifica	Descrizione	Data della modifica
Supporto per il gateway di file	Oltre ai gateway di volumi e ai gateway di nastri virtuali, Storage Gateway offre ora gateway di file. Un gateway di file combina un servizio e un'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 permette l'accesso a oggetti in Amazon S3 come file in un punto di montaggio NFS.	29 Novembre 2016
Backup Exec 16	Il gateway di nastri virtuali è ora compatibile con Backup Exec 16. È ora possibile utilizzare Backup Exec 16 per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Veritas Backup Exec.	7 Novembre 2016
Compatibilità con Micro Focus (HPE) Data Protector 9.x	Il gateway di nastri virtuali è ora compatibile con Micro Focus (HPE) Data Protector 9.x. Ora puoi usare HPE Data Protector per eseguire il backup dei dati in Amazon S3 e archiviarli direttamente in S3 Glacier Flexible Retrieval. Per ulteriori informazioni, consulta Test della configurazione tramite Micro Focus (HPE) Data Protector.	2 Novembre 2016
Nuova regione	Storage Gateway ora è disponibile nella regione Stati Uniti orientali (Ohio). Per informazioni dettagliate, consulta AWS Regioni.	17 ottobre 2016

Modifica	Descrizione	Data della modifica
Riprogettazione della console Storage Gateway	La Console di gestione Storage Gateway è stata riprogettata per semplificare la configurazione, la gestione e il monitoraggio di gateway, volumi e nastri virtuali. L'interfaccia utente ora fornisce visualizzazioni che possono essere filtrate e fornisce collegame nti diretti a AWS servizi integrati come CloudWatc h Amazon EBS. Per ulteriori informazioni, consulta Registrati per AWS Storage Gateway.	30 agosto 2016
Compatibilità con Veeam Backup & Replication V9 Update 2 o versioni successiv e	Il gateway di nastri virtuali è ora compatibile con Veeam Backup & Replication V9 Update 2 o versioni successive, ovvero le versioni 9.0.0.1715 e successiv e. È ora possibile utilizzare Veeam Backup Replicati on V9 Update 2 o versione successiva per eseguire il backup dei dati in Amazon S3 e archiviare direttame nte nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Test della configura zione utilizzando Veeam Backup & Replication.	15 agosto 2016
ID volume e snapshot più lunghi	Storage Gateway sta introducendo ID più lunghi per i volumi e gli snapshot. Puoi attivare il formato ID più lungo per i tuoi volumi, istantanee e altre risorse supportate. AWS Per ulteriori informazioni, consulta Informazioni sulle risorse e sugli ID delle risorse di Storage Gateway.	25 Aprile 2016

Modifica	Descrizione	Data della modifica
Nuova regione Supporto per storage di dimensioni fino a 512 TiB per i volumi archiviati Altri aggiornamenti e miglioramenti del gateway per la console locale Storage Gateway	Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Seoul). Per ulteriori informazioni, consulta AWS Regioni. Per i volumi archiviati, puoi ora creare fino a 32 volumi di storage ciascuno di dimensioni fino a 16 TiB, per un massimo di 512 TiB di storage. Per ulteriori informazioni, consulta Architettura dei volumi archiviati eAWS Storage Gateway quote. Le dimensioni totali di tutti i nastri in una libreria di nastri virtuali (VTL) sono state aumentate a 1 PiB. Per ulteriori informazioni, consulta AWS Storage Gateway quote. Puoi ora impostare la password per la console locale della macchina virtuale nella console Storage Gateway. Per informazioni, consulta Impostazione della password della console locale dalla console Storage Gateway.	21 marzo 2016
Compatibilità con Dell EMC 8.x NetWorker	Tape Gateway è ora compatibile con Dell EMC NetWorker 8.x. Ora puoi utilizzare Dell EMC NetWorker per eseguire il backup dei dati su Amazon S3 e archiviarli direttamente nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Dell EMC. NetWorker	29 febbraio 2016

Modifica	Descrizione	Data della modifica
Supporto per l'iniziatore iSCSI di VMware ESXi Hypervisor versione 6.0 e di Red Hat Enterprise Linux 7	AWS Storage Gateway ora supporta la versione 6.0 di VMware ESXi Hypervisor e l'iniziatore iSCSI Red Hat Enterprise Linux 7. Per ulteriori informazioni, consultare Hypervisor supportati e requisiti di hosting e Iniziatori iSCSI supportati.	20 Ottobre 2015
Nuova struttura dei contenuti	Questa versione include questo miglioramento: la documentazione include ora la sezione Gestione del gateway attivato, che riunisce attività di gestione comuni per tutte le soluzioni gateway. Seguono le istruzioni su come gestire il gateway dopo averlo distribuito e attivato. Per ulteriori informazioni, consulta Gestione del gateway.	

Modifica	Descrizione	Data della modifica
Supporto per storage di dimensioni fino a 1.024 TiB per i volumi nella cache Supporto per il tipo di scheda di rete VMXNET3 (10 GbE) nell'hypervisor VMware ESXi Miglioramenti per le prestazioni Miglioramenti e aggiornamenti vari per la console locale Storage Gateway	Per i volumi nella cache, puoi ora creare fino a 32 volumi di storage ciascuno di dimensioni fino a 32 TiB, per un massimo di 1.024 TiB di storage. Per ulteriori informazioni, consulta Architettura dei volumi in cache eAWS Storage Gateway quote. Se il gateway è ospitato in un hypervisor VMware ESXi, puoi riconfigurarlo per l'uso del tipo di scheda VMXNET3. Per ulteriori informazioni, consulta Configurazione delle schede di rete per il gateway. La velocità massima di caricamento per Storage Gateway è aumentata a 120 MB al secondo, mentre la velocità massima di download è aumentata a 20 MB al secondo. La console locale Storage Gateway è stata aggiornata e migliorata con caratteristiche aggiuntive per semplificare le attività di manutenzione. Per ulteriori informazioni, consulta Configurazione di rete del gateway.	16 settembre 2015
Supporto per il tagging	Storage Gateway ora supporta il tagging delle risorse. Puoi ora aggiungere tag a gateway, volumi e nastri virtuali per semplificarne la gestione. Per ulteriori informazioni, consulta Tagging per risorse Storage Gateway.	2 settembre 2015

Modifica	Descrizione	Data della modifica
Compatibilità con Quest (precedentemente Dell) Backup 10.0 NetVault	Tape Gateway è ora compatibile con Quest NetVault Backup 10.0. Ora puoi usare Quest NetVault Backup 10.0 per eseguire il backup dei dati su Amazon S3 e archiviarli direttamente nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Test della configurazione utilizzando Quest NetVault Backup.	22 giugno 2015

Modifica	Descrizione	Data della modifica
Supporto per volumi di storage da 16 TiB per le configurazioni dei gateway di volumi archiviati	Storage Gateway supporta ora volumi di archiviazione da 16 TiB per le configurazioni dei gateway di volumi archiviati. Puoi ora creare 12 volumi di storage da 16 TiB, per un massimo di 192 TiB di storage. Per ulteriori informazioni, consulta Architettura dei volumi archiviati.	3 giugno 2015
Supporto per controlli delle risorse di sistema nella console locale Storage Gateway	Puoi ora determinare se le risorse di sistema (core delle CPU virtuali, dimensioni del volume root e RAM) sono sufficienti per il corretto funzionamento del gateway. Per ulteriori informazioni, consulta Visualizzazione dello stato relativo alle risorse di sistema del gateway o Visualizzazione dello stato relativo alle risorse di sistema del gateway.	
Supporto per l'iniziatore iSCSI di Red Hat Enterprise Linux 6	Storage Gateway supporta ora l'iniziatore iSCSI di Red Hat Enterprise Linux 6. Per ulteriori informazioni, consulta Requisiti.	
	Questa versione include i miglioramenti e gli aggiornamenti per Storage Gateway seguenti: • Dalla console Storage Gateway puoi ora visualizzare la data e l'ora dell'applicazione dell'ultimo aggiornamento software al gateway. Per ulteriori informazioni, consulta Gestione degli aggiornamenti del gateway tramite la console AWS Storage Gateway. • Storage Gateway fornisce ora un'API che puoi usare per elencare gli iniziatori iSCSI connessi ai volumi di	

Modifica	Descrizione	Data della modifica
	archiviazione. Per ulteriori informazioni, ListVolumeInitiatorsconsulta il riferimento all'API.	
Supporto per l'hypervisor Microsoft Hyper-V versioni 2012 e 2012 R2	Storage Gateway supporta ora l'hypervisor Microsoft Hyper-V versioni 2012 e 2012 R2. Questa versione è in aggiunta al supporto per l'hypervisor Microsoft Hyper-V versione 2008 R2. Per ulteriori informazioni, consulta Hypervisor supportati e requisiti di hosting.	30 Aprile 2015
Compatibilità con Symantec Backup Exec 15	Il gateway di nastri virtuali è ora compatibile con Symantec Backup Exec 15. È ora possibile utilizzare Symantec Backup Exec 15 per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Veritas Backup Exec.	6 Aprile 2015
Supporto per l'autenticazione CHAP per i volumi di storage	Storage Gateway supporta ora la configurazione dell'autenticazione CHAP per i volumi di archiviazione. Per ulteriori informazioni, consulta Configurare l'autenticazione CHAP per i volumi.	2 Aprile 2015
Supporto per VMware ESXi Hypervisor versioni 5.1 e 5.5	Storage Gateway ora supporta VMware ESXi Hypervisor versioni 5.1 e 5.5. Queste si aggiungono al supporto per VMware ESXi Hypervisor versioni 4.1 e 5.0. Per ulteriori informazioni, consulta Hypervisor supportati e requisiti di hosting.	30 marzo 2015

Modifica	Descrizione	Data della modifica
Supporto per l'utilità Windows CHKDSK	Storage Gateway supporta ora l'utilità Windows CHKDSK. Puoi usare questa utilità per verificare l'integrità dei volumi e correggere gli errori nei volumi. Per ulteriori informazioni, consulta Risoluzione dei problemi dei volumi.	04 marzo 2015
Integrazione con AWS CloudTrail To Capture API	Storage Gateway è ora integrato con AWS CloudTrail. AWS CloudTrail acquisisce le chiamate API effettuate da o per conto di Storage Gateway nel tuo account Amazon Web Services e invia i file di log a un bucket Amazon S3 da te specificato. Per ulteriori informazioni, consulta Registrazione e monitoraggio AWS Storage Gateway. Questa versione include i miglioramenti e gli aggiornamenti per Storage Gateway seguenti: • I nastri virtuali con dati di scarsa qualità nello storage della cache, ovvero che includono contenuto che non è stato caricato in AWS, vengono ora ripristinati ogni volta che viene modificata un'unità nella cache del gateway. Per ulteriori informazioni, consulta Recupero di un nastro virtuale da un gateway compromesso.	16 dicembre 2014

Modifica	Descrizione	Data della modifica
Compatibilità con unità di sostituzione dei supporti e software di backup aggiuntivi	Il gateway di nastri virtuali è ora compatibile con i software di backup seguenti: • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 È ora possibile utilizzare questi quattro prodotti software di backup con la libreria di nastri virtuali (VTL) di Storage Gateway per eseguire il backup dei dati in Amazon S3 e archiviare direttamente sullo storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Utilizzo del software di backup per testare la configurazione del gateway. Storage Gateway fornisce ora un'unità di sostituzione dei supporti aggiuntiva compatibile con il nuovo software di backup. Questa versione include vari AWS Storage Gateway miglioramenti e aggiornamenti.	3 Novembre 2014
Regione Europa (Francoforte)	Storage Gateway è ora disponibile nella regione Europa (Francoforte). Per informazioni dettagliate, consulta AWS Regioni.	23 ottobre 2014

Modifica	Descrizione	Data della modifica
Nuova struttura dei contenuti	È stata creata una sezione introduttiva comune per tutte le soluzioni gateway. Seguono istruzioni per il download, la distribuzione e l'attivazione di un gateway. Dopo aver distribuito e attivato un gateway, puoi consulta ulteriori istruzioni specifiche per i volumi archiviati, i volumi nella cache e le configurazioni dei gateway di nastri virtuali. Per ulteriori informazioni, consulta Creazione di un gateway di nastri virtuali.	19 maggio 2014
Compatibilità con Symantec Backup Exec 2012	Il gateway di nastri virtuali è ora compatibile con Symantec Backup Exec 2012. È ora possibile utilizzar e Symantec Backup Exec 2012 per eseguire il backup dei dati in Amazon S3 e archiviare direttamente nello spazio di archiviazione offline (S3 Glacier Deep Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta Testare la configurazione utilizzando Veritas Backup Exec.	28 aprile 2014

Modifica	Descrizione	Data della modifica
Supporto per Windows Server Failover Clustering Supporto per l'iniziatore di VMware ESX Supporto per l'esecuzione di attività di configurazione nella console locale Storage Gateway	• Storage Gateway ora supporta la connessione di più host allo stesso volume se gli host coordinano l'accesso utilizzando Windows Server Failover Clustering (WSFC). Tuttavia, non puoi connettere più host allo stesso volume senza usare WSFC. • Storage Gateway ti permette ora di gestire la connettività di storage direttamente tramite l'host ESX. Questa è un'alternativa all'uso di iniziatori residenti nel sistema operativo guest delle macchine virtuali. • Storage Gateway offre ora il supporto per l'esecuzione di attività di configurazione nella console locale Storage Gateway. Per informazioni sull'esecuzione di attività di configurazione in gateway distribuiti in locale, consulta Esecuzione delle operazioni sulla console locale della VM di o Esecuzione delle operazioni sulla console locale della VM di . Per informazioni sull'esecuzione di attività di configurazione in gateway distribuiti in un'istanza EC2, consulta Esecuzione delle operazioni sulla console locale Amazon EC2 o Esecuzione delle operazioni sulla console locale Amazon EC2.	31 gennaio 2014

Modifica	Descrizione	Data della modifica
Supporto per la libreria di nastri virtuali (VTL) e introduzione della versione API del 30/06/2013	Storage Gateway collega un'appliance software locale con lo storage basato sul cloud per integrare l'ambient e IT locale con l'infrastruttura di storage. AWS Oltre ai gateway di volumi (volumi nella cache e volumi archiviati), Storage Gateway supporta ora la libreria di nastri virtuali (VTL) del gateway. Puoi configurare il gateway di nastri virtuali con un massimo di 10 unità nastro virtuali per gateway. Ogni unità nastro virtuale risponde al set di comandi SCSI, in modo da garantire il funzionamento delle applicazioni di backup locali esistenti senza alcuna modifica. Per ulteriori informazi oni, consulta gli argomenti seguenti nella Guida per l'utente AWS Storage Gateway . • Per una panoramica dell'architettura, vedi Come funziona un gateway di nastri virtuali (architettura). • Per iniziare a usare il gateway di nastri virtuali, consulta Creazione di un gateway di nastri virtuali.	5 Novembre 2013
Supporto per Microsoft Hyper-V	Storage Gateway offre ora la possibilità di distribuire un gateway on-premise nella piattaforma di virtualiz zazione Microsoft Hyper-V. I gateway distribuiti in Microsoft Hyper-V hanno tutti le stesse funzionalità e caratteristiche dello storage gateway on-premis e esistente. Per informazioni su come iniziare a distribuire un gateway con Microsoft Hyper-V, consulta Hypervisor supportati e requisiti di hosting.	10 Aprile 2013

Modifica	Descrizione	Data della modifica
Supporto per la distribuzione di un gateway in Amazon EC2	Storage Gateway ora offre la possibilità di implement are un gateway in Amazon Elastic Compute Cloud (Amazon EC2). Puoi avviare un'istanza gateway in Amazon EC2 utilizzando l'AMI Storage Gateway disponibile in Marketplace AWS. Per informazioni su come iniziare a distribuire un gateway usando l'AMI Storage Gateway, consulta Implementazione di un'istanza Amazon EC2 per ospitare il tuo gateway di nastri virtuali.	15 gennaio 2013

Modifica	Descrizione	Data della modifica
Supporto per volumi nella cache e introduzione della versione API del 30/06/2012	In questa versione Storage Gateway introduce il supporto per i volumi nella cache. I volumi nella cache riducono al minimo la necessità di dimensionare l'infrastruttura di storage locale, continuando a fornire alle applicazioni accesso a bassa latenza ai dati attivi. Puoi creare volumi di storage di dimensioni fino a 32 TiB e montarli come dispositivi iSCSI dai server applicazioni locali. I dati scritti nei volumi nella cache vengono archiviati in Amazon Simple Storage Service (Amazon S3), con una sola cache di dati scritti e letti di recente archiviata in locale nell'hardware di archiviazione on-premise. I volumi nella cache ti permettono di utilizzare Amazon S3 per dati per cui sono accettabili latenze di recupero maggiori, ad esempio per dati meno recenti ad accesso non frequente, mantenendo lo spazio di archiviazione on-premise per i casi in cui è necessario accesso a bassa latenza. In questa versione Storage Gateway introduce anche una nuova versione API che, oltre a supportare le operazioni attuali, offre nuove operazioni per supportare i volumi nella cache. Per ulteriori informazioni sulle due soluzioni Storage Gateway, consulta Come funziona il gateway di nastri virtuali (architettura). Puoi anche provare una configurazione di test. Per istruzioni, consulta Creazione di un gateway di nastri virtuali.	29 Ottobre 2012

Modifica	Descrizione	Data della modifica
Supporto per API e IAM	In questa versione, Storage Gateway introduce il supporto API e il supporto per AWS Identity and Access Management(IAM). • Supporto per l'API: puoi ora configurare e gestire le risorse Storage Gateway a livello di programma zione. Per ulteriori informazioni sull'API, consulta Riferimento API per Storage Gateway nella Guida per gli utenti AWS Storage Gateway . • Supporto per IAM: AWS Identity and Access Management ti permette di creare utenti e gestire l'accesso degli utenti alle risorse Storage Gateway tramite policy IAM. Per alcuni esempi di policy IAM, consultare Identity and Access Management per AWS Storage Gateway. Per ulteriori informazioni su IAM, consulta la pagina dei dettagli del prodotto AWS Identity and Access Management (IAM).	9 maggio 2012
Supporto per indirizzi IP statici	Puoi ora specificare un indirizzo IP statico per il gateway locale. Per ulteriori informazioni, consulta Configurazione di rete del gateway.	5 marzo 2012
Nuova guida	Questa è la prima versione della Guida per l'utente di AWS Storage Gateway .	24 gennaio 2012

Note di rilascio per il software Tape Gateway Appliance

Queste note di rilascio descrivono le funzionalità, i miglioramenti e le correzioni nuovi e aggiornati inclusi in ogni versione dell'appliance Tape Gateway . Ogni versione del software è identificata dalla data di rilascio e da un numero di versione univoco.

È possibile determinare il numero di versione del software di un gateway controllando la relativa pagina Dettagli nella console Storage Gateway o chiamando l'azione DescribeGatewayInformationAPI utilizzando un AWS CLI comando simile al seguente:

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

Il numero di versione viene restituito nel `SoftwareVersion` campo della risposta API.

> **Note**
>
> Un gateway non riporterà le informazioni sulla versione del software nelle seguenti circostanze:
>
> - Il gateway è offline.
> - Il gateway esegue un software precedente che non supporta la segnalazione delle versioni.
> - Il tipo di gateway è FSx File Gateway.

Per ulteriori informazioni sugli aggiornamenti di Tape Gateway , incluso come modificare la pianificazione automatica predefinita di manutenzione e aggiornamento per un gateway, vedere Gestione degli aggiornamenti del gateway tramite la console AWS Storage Gateway .

Data di rilascio	Versione del software	Note di rilascio
2024-04-10	28,1	• Risolto un problema di utilizzo della memoria introdotto nella versione 2.8.0 • Aggiornamenti delle patch di sicurezza

Data di rilascio	Versione del software	Note di rilascio
		• Processo di aggiornamento del software migliorato • Risolto il problema del componente NTP (Network Time Protocol) mancante per i nuovi gateway
2024-03-06	2.8.0	• Aggiornamenti del sistema operativo per nuovi gateway • Aggiornamenti delle patch di sicurezza • Prestazioni migliorate per carichi di lavoro di Backup e Ripristino simultanei
2023-12-19	2.7.0	• Aggiornamenti del sistema operativo per nuovi gateway
2023-12-14	2,6,6	• È stato risolto un problema con il posizionamento relativo su nastri di dimensioni superiori a 5 TiB
2023-10-19	2,6,5	• Sono state aggiunte misure di protezione contro la sovrascrittura del nastro da parte dei client dopo il riavvio del gateway