



Guida per l'utente per gateway di volumi

# AWS Storage Gateway



Versione API 2013-06-30

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Storage Gateway: Guida per l'utente per gateway di volumi

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

---

# Table of Contents

.....	x
Cos'è un gateway di volumi? .....	1
Gateway di volumi .....	1
È la prima volta che utilizzi Storage Gateway? .....	2
Come funziona il gateway di volumi .....	2
Gateway di volumi .....	2
Prezzi .....	7
Pianificare l'implementazione del gateway .....	7
Iniziare con AWS Storage Gateway .....	9
Registrati per AWS Storage Gateway .....	9
Regioni AWS che supportano Storage Gateway .....	10
Requisiti .....	10
Requisiti storage e hardware .....	10
Requisiti di rete e firewall .....	13
Hypervisor supportati e requisiti di hosting .....	24
Iniziatori i SCSI supportati .....	25
Accedendo AWS Storage Gateway .....	26
Utilizzo dell'appliance hardware .....	27
Regioni supportate AWS .....	27
Configurazione dell'appliance hardware .....	28
Installazione fisica del dispositivo hardware .....	29
Dimensioni dell'appliance hardware .....	30
Configurazione dei parametri di rete .....	34
Attivazione dell'appliance hardware .....	37
Creazione di un gateway .....	39
Configurazione di un indirizzo IP per il gateway .....	39
Configurazione del gateway .....	41
Rimozione di un gateway .....	42
Eliminazione dell'appliance hardware .....	42
Creazione del gateway .....	44
Panoramica: attivazione del gateway .....	44
Configurazione di un gateway .....	44
Connect a AWS .....	44
Rivedi e attiva .....	44

Panoramica: configurazione del gateway .....	45
Panoramica: risorse di archiviazione .....	45
Creazione di un gateway di volumi .....	45
Creazione di un gateway .....	45
Creazione di un volume .....	51
Uso del volume .....	55
Backup dei volumi .....	64
Attivazione di un gateway in un cloud privato virtuale .....	70
Creazione di un VPC endpoint per Storage Gateway .....	70
Gestione del gateway .....	72
Gestione del gateway di volumi .....	72
Modifica delle informazioni sul gateway .....	73
Aggiunta di un volume .....	74
Espansione delle dimensioni di un volume .....	74
Clonazione di un volume .....	75
Visualizzazione dell'utilizzo del volume .....	79
Riduzione dell'importo addebitato per lo storage in un volume .....	79
Eliminazione di un volume .....	80
Spostamento dei volumi su un gateway differente .....	80
Creazione di uno snapshot una tantum .....	83
Modifica di una pianificazione degli snapshot .....	83
Eliminazione di snapshot .....	84
Informazioni su stati e transizioni dei volumi .....	97
Spostamento dei dati su un nuovo gateway .....	109
Spostamento dei volumi archiviati su un nuovo gateway di volumi archiviato .....	109
Spostamento dei volumi memorizzati nella cache su una nuova macchina virtuale del gateway di volumi memorizzata nella cache .....	112
Monitoraggio di Storage Gateway .....	116
Comprendere i parametri del gateway .....	116
Dimensioni per i parametri di Storage Gateway .....	122
Monitoraggio del buffer di caricamento .....	123
Monitoraggio dello storage della cache .....	126
Comprendere CloudWatch gli allarmi .....	128
Creazione di allarmi consigliati CloudWatch .....	129
Creazione di un CloudWatch allarme personalizzato .....	130
Monitoraggio del gateway di volumi .....	132

Ottenere i log dello stato del gateway di volumi .....	133
Utilizzo di Amazon CloudWatch Metrics .....	134
Misurazione delle prestazioni tra l'applicazione il gateway .....	136
Misurazione delle prestazioni tra il gateway e AWS .....	139
Informazioni sui parametri dei volumi .....	142
Gestione del gateway .....	150
Spegnimento della macchina virtuale gateway .....	150
Avvio e arresto di un gateway di volumi .....	151
Gestione dei dischi locali .....	152
Determinazione della quantità di archiviazione su disco locale .....	152
Dimensionamento del buffer di caricamento .....	154
Dimensionamento dell'archiviazione della cache .....	156
Aggiunta di un buffer di caricamento o di archiviazione della cache .....	156
Gestione della larghezza di banda .....	157
Per modificare la limitazione della larghezza di banda usando la console Storage Gateway .....	158
Pianificazione della limitazione della larghezza di banda .....	159
Utilizzando il AWS SDK for Java .....	161
Utilizzando il AWS SDK for .NET .....	163
Utilizzando il AWS Tools for Windows PowerShell .....	165
Gestione degli aggiornamenti del gateway .....	166
Frequenza di aggiornamento e comportamento previsto .....	166
Attiva o disattiva gli aggiornamenti di manutenzione .....	167
Modifica la pianificazione della finestra di manutenzione del gateway .....	168
Esecuzione di attività di manutenzione utilizzando la console locale .....	169
Esecuzione delle operazioni sulla console locale della VM di .....	169
Esecuzione di attività sulla console EC2 locale .....	189
Accesso alla console locale del gateway .....	195
Configurazione delle schede di rete per il gateway .....	201
Eliminazione del gateway e rimozione delle risorse .....	205
Eliminazione del gateway tramite la console Storage Gateway .....	206
Rimozione di risorse da un gateway distribuito in locale .....	207
Rimozione di risorse da un gateway distribuito su un'istanza Amazon EC2 .....	207
Prestazioni e ottimizzazione per Volume Gateway .....	209
Ottimizzazione delle prestazioni del gateway .....	209
Configurazione consigliata .....	209

Aggiungere risorse al gateway .....	210
Ottimizza le impostazioni SCSI .....	213
Aggiungere risorse per l'ambiente applicativo .....	213
Utilizzo dell'VMware alta disponibilità con Storage Gateway .....	214
Configura il tuo cluster vSphere VMware HA .....	215
Scarica l'immagine .ova dalla console Storage Gateway .....	217
Distribuzione del gateway .....	217
(Facoltativo) Aggiungi opzioni di sovrascrittura per altri utenti del tuo cluster VMs .....	218
Attivazione del gateway .....	218
Testa la tua configurazione VMware ad alta disponibilità .....	219
Sicurezza .....	220
Protezione dei dati .....	221
Crittografia dei dati .....	222
Configurazione dell'autenticazione CHAP .....	223
Identity and Access Management .....	225
Destinatari .....	226
Autenticazione con identità .....	227
Gestione dell'accesso con policy .....	230
Come funziona AWS Storage Gateway con IAM .....	233
Esempi di policy basate su identità .....	239
Risoluzione dei problemi .....	243
Registrazione e monitoraggio .....	245
Informazioni sullo Storage Gateway in CloudTrail .....	245
Comprensione delle voci dei file di log di Storage Gateway .....	246
Convalida della conformità .....	248
Resilienza .....	249
Sicurezza dell'infrastruttura .....	249
AWS Best practice per la sicurezza .....	250
Come risolvere i problemi del gateway .....	251
Risoluzione dei problemi: problemi relativi al gateway offline .....	251
Controlla il firewall o il proxy associato .....	252
Verifica la presenza di un'ispezione continua SSL o approfondita del traffico del gateway ....	252
Verificare la presenza di un'interruzione dell'alimentazione o di un guasto hardware sull'host dell'hypervisor .....	252
Verifica la presenza di problemi con un disco di cache associato .....	252
Risoluzione dei problemi: problemi di attivazione del gateway .....	253

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico .....	254
Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint Amazon VPC .....	257
Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico e nello stesso è presente un VPC endpoint Storage Gateway VPC .....	261
Come risolvere i problemi di gateway on-premise .....	261
Attivazione per facilitare la risoluzione dei problemi AWS Support del gateway .....	266
Come risolvere i problemi di configurazione di Microsoft Hyper-V .....	267
Risoluzione dei problemi relativi al EC2 gateway Amazon .....	272
Dopo qualche secondo, il gateway ancora non si attiva .....	272
Impossibile trovare l'istanza del EC2 gateway nell'elenco delle istanze .....	273
Impossibile collegare un EBS volume Amazon all'istanza del EC2 gateway .....	273
Impossibile collegare un iniziatore a una destinazione di volume del gateway EC2 .....	273
Messaggio di indisponibilità di dischi quando si tenta di aggiungere volumi di archiviazione .....	273
Come rimuovere un disco allocato per ridurre lo spazio del buffer di caricamento .....	274
La velocità effettiva da o verso il EC2 gateway scende a zero .....	274
Attivazione AWS Support per facilitare la risoluzione dei problemi relativi al gateway .....	274
Connect al EC2 gateway Amazon tramite la console seriale .....	276
Risoluzione dei problemi dell'appliance hardware .....	276
Come determinare l'indirizzo IP del servizio .....	276
Come si esegue una reimpostazione ai valori di fabbrica .....	277
Come eseguire il riavvio a distanza .....	277
Come ottenere il DRAC supporto Dell i .....	277
Come trovare il numero di serie dell'appliance hardware .....	277
Come ottenere supporto per il dispositivo hardware .....	278
Come risolvere i problemi dei volumi .....	279
Secondo la console il volume non è configurato .....	279
Secondo la console il volume è irrecuperabile .....	279
Il gateway nella cache è irraggiungibile e occorre recuperare i dati .....	280
Secondo la console il volume è nello stato TRANSITO .....	280
Occorre controllare l'integrità del volume e correggere possibili errori .....	281
La destinazione iSCSI del volume non compare nella console di gestione del disco Windows .....	281
Occorre modificare il nome della destinazione iSCSI del volume .....	282
Lo snapshot programmato per un volume non viene eseguito .....	282
È necessario rimuovere o sostituire un disco non riuscito .....	282

Il throughput dall'applicazione a un volume si è azzerato .....	282
Un disco della cache nel gateway rileva un errore .....	283
Lo snapshot di un volume resta allo stato IN ATTESA più del previsto .....	284
Notifiche di stato della disponibilità elevata .....	284
Risoluzione dei problemi relativi alla disponibilità elevata .....	284
Notifiche di stato .....	284
Metriche .....	286
Ripristino dei dati: best practice .....	286
Ripristino da un arresto imprevisto della macchina virtuale .....	287
Ripristino dei dati da un gateway o una macchina virtuale malfunzionante .....	287
Ripristino dei dati da un volume irrecuperabile .....	288
Ripristino dei dati da un disco della cache malfunzionante .....	288
Ripristino dei dati da un file system danneggiato .....	289
Ripristino dei dati da un data center inaccessibile .....	290
Risorse aggiuntive .....	291
Implementazione e configurazione dell'host VM gateway .....	291
Configurazione VMware per Storage Gateway .....	291
Sincronizzazione dell'ora della VM associata al gateway .....	299
Implementa un EC2 host Amazon per Volume Gateway .....	301
Implementazione di Amazon EC2 con impostazioni predefinite .....	305
Modifica le opzioni dei metadati delle EC2 istanze Amazon .....	308
Gateway di volumi .....	308
Rimozione di dischi dal gateway .....	308
EBSVolumi per gateway EC2 .....	313
Ottenere una chiave di attivazione .....	314
Linux (curl) .....	315
Linux (bash/zsh) .....	316
Microsoft Windows PowerShell .....	317
Utilizzo della console locale .....	317
Connessione degli SCSI iniziatori .....	318
Connessione ai volumi in un client Windows .....	319
Connessione di volumi o VTL dispositivi a un client Linux .....	324
Personalizzazione delle impostazioni SCSI .....	327
Configurazione dell'autenticazione CHAP .....	335
Utilizzo AWS Direct Connect con Storage Gateway .....	344
Requisiti delle porte di rete per Volume Gateway .....	344



---

Connessione al gateway .....	351
Ottenere un indirizzo IP da un EC2 host Amazon .....	352
Comprensione delle risorse e delle risorse IDs .....	353
Lavorare con Resource IDs .....	354
Tagging delle risorse .....	354
Lavorare con i tag .....	355
Componenti open source .....	356
Quote Storage Gateway .....	356
Quote per i volumi .....	357
Dimensioni disco locale consigliate per il gateway .....	357
API Riferimento .....	359
Intestazioni obbligatorie delle richieste .....	359
Firmare le richieste .....	362
Esempio di calcolo di firma .....	363
Risposte agli errori .....	364
Eccezioni .....	365
Codici di errore delle operazioni .....	367
Risposte agli errori .....	387
Operazioni .....	389
Cronologia dei documenti .....	390
Aggiornamenti precedenti .....	408
Note di rilascio .....	429

La documentazione del gateway di file Amazon S3 è stata spostata in [Cos'è un gateway di file Amazon S3?](#)

La documentazione di Amazon FSx File Gateway è stata spostata in [Cos'è Amazon FSx File Gateway?](#)

La documentazione del gateway di nastri virtuali è stata spostata in [Cos'è un gateway di nastri virtuali?](#)

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 volumi?

AWS Storage Gateway collega un'appliance software locale con storage basato su 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 File Gateway basati su file (Amazon S3 File e FSx Amazon File), soluzioni di storage basate su volume (memorizzate nella cache e archiviate) e su nastro.

## Argomenti

- [Gateway di volumi](#)
- [È la prima volta che utilizzi Storage Gateway?](#)
- [Come funziona il gateway di volumi \(architettura\)](#)
- [Prezzi di Storage Gateway](#)
- [Pianifica l'implementazione di Storage Gateway](#)

## Gateway di volumi

Volume Gateway: un Volume Gateway fornisce volumi di archiviazione basati sul cloud che puoi montare come dispositivi Internet Small Computer System Interface (iSCSI) dai tuoi server di applicazioni locali.

Puoi implementare un Volume Gateway in locale come appliance VM in esecuzione su VMware ESXi, KVM o hypervisor Microsoft Hyper-V, come appliance hardware o come istanza Amazon. AWS EC2

Il gateway supporta le configurazioni di volumi seguenti:

- Volumi nella cache: puoi archiviare i dati in Amazon Simple Storage Service (Amazon S3) e conservare in locale una copia dei sottoinsiemi di dati con accesso frequente. I volumi nella cache offrono un notevole risparmio sui costi dello storage principale e riducono al minimo la necessità di dimensionare lo storage in locale. Inoltre, è possibile mantenere accesso a bassa latenza ai dati utilizzati frequentemente.
- Volumi archiviati: se necessiti di accesso a bassa latenza all'intero set di dati, per prima cosa configura il gateway on-premise in modo che archivi tutti i dati a livello locale. Quindi esegui il

backup asincrono point-in-time degli snapshot di questi dati su Amazon S3. Questa configurazione fornisce backup offsite durevoli ed economici che puoi ripristinare nel tuo data center locale o in Amazon Elastic Compute Cloud (Amazon) EC2. Ad esempio, se hai bisogno di capacità sostitutiva per il disaster recovery, puoi ripristinare i backup su Amazon EC2.

Documentazione: per la documentazione del gateway di volumi, consulta [Creazione di un gateway di volumi](#).

## 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 volumi](#) descrive come creare e usare un gateway di volumi. Mostra come creare volumi di storage ed eseguire il backup dei dati sui volumi.
- [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 a livello di codice, consulta la Guida di riferimento AWS Storage Gateway API](#)

## Come funziona il gateway di volumi (architettura)

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

### Gateway di volumi

Per i gateway di volumi, è possibile utilizzare i volumi nella cache o i volumi archiviati.

#### Argomenti

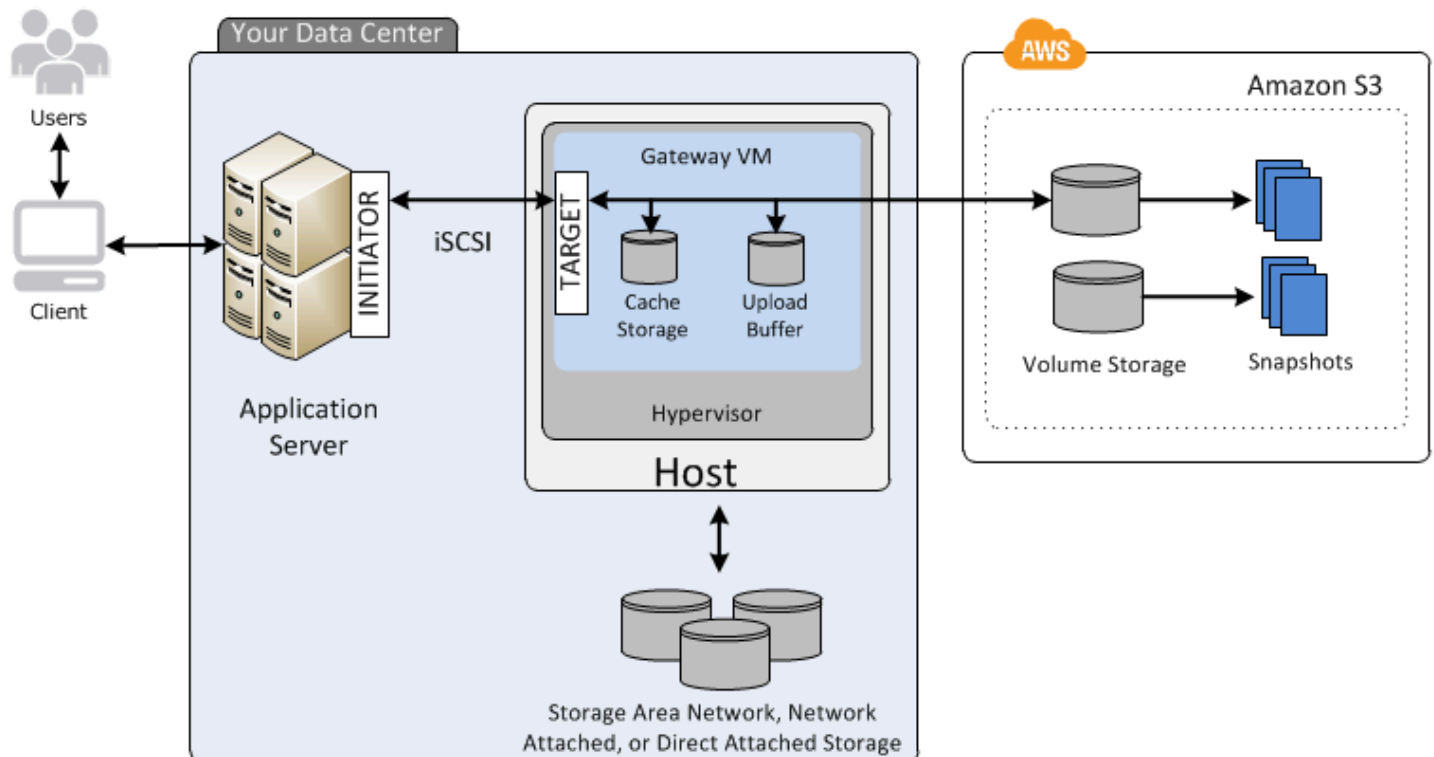
- [Architettura dei volumi nella cache](#)
- [Architettura dei volumi archiviati](#)

## Architettura dei volumi nella cache

Con i volumi nella cache, è possibile utilizzare Amazon S3 come spazio di archiviazione di dati principale, mantenendo i dati con accesso frequente in locale, in Storage Gateway. I volumi nella cache riducono al minimo l'esigenza di dimensionare l'infrastruttura di storage locale, fornendo comunque alle applicazioni accesso a bassa latenza ai dati utilizzati di frequente. È possibile creare volumi di storage di dimensioni fino a 32 TiB e collegarli come SCSI dispositivi i dai server delle applicazioni locali. Il gateway archivia i dati che scrivi su questi volumi in Amazon S3 e conserva i dati letti di recente nella cache di Storage Gateway on-premise e nell'archiviazione del buffer di caricamento.

I volumi nella cache possono avere dimensioni che variano da 1 GiB a 32 TiB e devono essere arrotondati al GiB più vicino. Ciascun gateway configurato per i volumi nella cache può supportare fino a 32 volumi per un volume di storage massimo totale di 1.024 TiB (1 PiB).

Nella soluzione con volumi nella cache, Storage Gateway archivia tutti i dati delle applicazioni on-premise in un volume di archiviazione in Amazon S3. Il diagramma seguente fornisce una panoramica della distribuzione dei volumi nella cache.



Dopo aver installato l'appliance software Storage Gateway, la macchina virtuale, su un host del data center e averla attivata, la usi per effettuare il provisioning dei volumi di storage supportati

AWS Management Console da Amazon S3. È inoltre possibile effettuare il provisioning dei volumi di storage in modo programmatico utilizzando lo Storage Gateway API o le AWS SDK librerie. Questi volumi di storage vengono quindi montati sui server delle applicazioni locali come dispositivi i. SCSI

È inoltre possibile allocare dischi locali per la macchina virtuale. Questi dischi locali servono per i seguenti scopi:

- Dischi utilizzati dal gateway come storage cache: quando le applicazioni scrivono i dati nei volumi di storage in esso contenuti AWS, il gateway archivia innanzitutto i dati sui dischi locali utilizzati per l'archiviazione della cache. Il gateway carica quindi i dati su Amazon S3. L'archiviazione della cache funge da archiviazione durevole on-premise per i dati che aspettano di essere caricati in Amazon S3 dal buffer di caricamento.

Lo storage della cache consente inoltre al gateway di archiviare in locale i dati delle applicazioni utilizzati recentemente per un accesso a bassa latenza. Se l'applicazione richiede i dati, il gateway controlla dapprima l'archiviazione della cache per rilevare i dati prima di controllare Amazon S3.

È possibile utilizzare le seguenti linee guida per determinare la quantità di spazio su disco da allocare allo storage della cache. Generalmente, si dovrebbe allocare almeno il 20% della dimensione dello storage di file esistente come storage della cache. Lo storage della cache dovrebbe inoltre essere maggiore del buffer di caricamento. Questa linea guida aiuta a garantire che l'archiviazione della cache sia sufficiente per contenere in modo persistente nel buffer di caricamento tutti i dati che non sono stati ancora caricati su Amazon S3.

- Dischi che il gateway utilizza come buffer di caricamento: per predisporre il caricamento su Amazon S3, il gateway archivia inoltre i dati in entrata in un'area di gestione temporanea, chiamata buffer di caricamento. Il gateway carica questi dati del buffer tramite una connessione crittografata Secure Sockets Layer (SSL) AWS, dove vengono archiviati crittografati in Amazon S3.

È possibile effettuare backup incrementali, detti snapshot, dei volumi di archiviazione in Amazon S3. Queste point-in-time istantanee vengono inoltre archiviate in Amazon S3 come istantanee AmazonEBS. Quando esegui una nuova snapshot, vengono archiviati solo i dati che sono stati modificati rispetto all'ultima snapshot. Quando viene scattata l'istantanea, il gateway carica le modifiche fino al punto dell'istantanea, quindi crea la nuova istantanea utilizzando Amazon. EBS Puoi avviare le snapshot su base pianificata o una tantum. Un singolo volume supporta l'accodamento di più istantanee in rapida successione, ma ogni snapshot deve finire di essere creato prima di poter scattare il successivo. Quando elimini una snapshot, vengono rimossi solo i dati non necessari ad

altre eventuali snapshot. Per informazioni sugli EBS snapshot di Amazon, consulta [Amazon EBS snapshots](#).

Puoi ripristinare uno EBS snapshot Amazon su un volume di storage gateway se devi ripristinare un backup dei tuoi dati. In alternativa, per le istantanee di dimensioni fino a 16 TiB, puoi utilizzare l'istantanea come punto di partenza per un nuovo volume Amazon. EBS Puoi quindi collegare questo nuovo EBS volume Amazon a un'EC2istanza Amazon.

Tutti i dati del gateway e i dati degli snapshot per i volumi memorizzati nella cache vengono archiviati in Amazon S3 e crittografati a riposo utilizzando la crittografia lato server (). SSE Tuttavia, non puoi accedere a questi dati con Amazon S3 API o altri strumenti come la console di gestione Amazon S3.

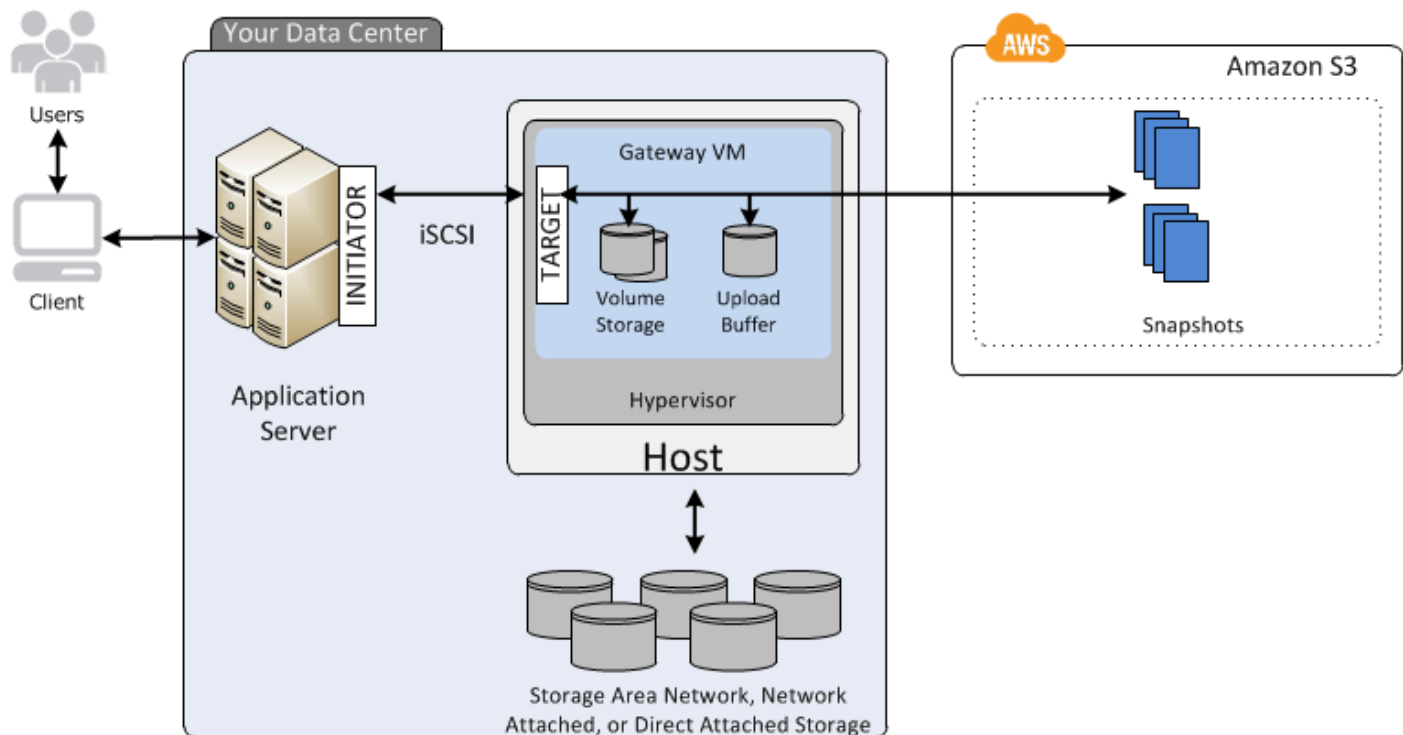
## Architettura dei volumi archiviati

Utilizzando i volumi archiviati, puoi archiviare i dati primari localmente, eseguendo al contempo il backup asincrono di tali dati su. AWS I volumi archiviati forniscono alle applicazioni locali l'accesso a bassa latenza a tutti i relativi set di dati. Al contempo, forniscono backup offsite durevoli. È possibile creare volumi di storage e montarli come SCSI dispositivi i dai server delle applicazioni locali. I dati scritti sui volumi archiviati vengono memorizzati nell'hardware di storage locale. Il backup di questi dati viene eseguito in modo asincrono su Amazon S3 come snapshot di Amazon Elastic Block Store (Amazon). EBS

I volumi archiviati possono avere dimensioni che variano da 1 GiB a 16 TiB e devono essere arrotondati al GiB più vicino. Ciascun gateway configurato per i volumi archiviati può supportare fino a 32 volumi e uno storage di volumi totale di 512 TiB (0,5 PiB).

Con i volumi archiviati, puoi mantenere lo storage dei volumi in locale, nel data center. Ciò significa che è possibile archiviare tutti i dati delle applicazioni nell'hardware di storage locale. Successivamente, tramite funzionalità che contribuiscono a mantenere la sicurezza dei dati, il gateway carica i dati sul cloud Amazon Web Services per un backup a costi contenuti e un rapido ripristino di emergenza. Questa soluzione è ideale se desideri conservare i dati a livello locale on-premise poiché devi disporre di un accesso a bassa latenza a tutti i dati e devi inoltre mantenere i backup in AWS.

Il diagramma seguente fornisce una panoramica della distribuzione dei volumi archiviati.



Dopo aver installato e attivato l'appliance software Storage Gateway (la macchina virtuale) su un host nel data center, è possibile creare volumi di archiviazione del gateway. Quindi li mappi su dischi Direct Attached Storage (DAS) o Storage Area Network (SAN) locali. È possibile iniziare con nuovi dischi o dischi che già contengono dati. È quindi possibile montare questi volumi di archiviazione sui server delle applicazioni locali come dispositivi iSCSI. Man mano che le applicazioni locali scrivono dati e leggono dati su un volume di storage del gateway, tali dati vengono archiviati e recuperati dal disco assegnato al volume.

Per preparare i dati da caricare su Amazon S3, il gateway archivia inoltre i dati in entrata in un'area di gestione temporanea, chiamata buffer di caricamento. È possibile utilizzare dischi locali DAS o SAN dischi per lo storage di lavoro. Il gateway carica i dati dal buffer di caricamento tramite una connessione Secure Sockets Layer (SSL) crittografata al servizio Storage Gateway in esecuzione nel cloud Amazon Web Services. Il servizio archivia quindi i dati crittografati in Amazon S3.

È possibile richiedere backup incrementali, detti snapshot, dei volumi di storage. Il gateway archivia queste istantanee in Amazon S3 come istantanee AmazonEBS. Quando esegui una nuova snapshot, vengono archiviati solo i dati che sono stati modificati rispetto all'ultima snapshot. Quando viene scattata l'istantanea, il gateway carica le modifiche fino al punto dell'istantanea, quindi crea la nuova istantanea utilizzando Amazon EBS. Puoi avviare le snapshot su base pianificata o una tantum. Un singolo volume supporta l'accodamento di più istantanee in rapida successione, ma ogni snapshot



deve finire di essere creato prima di poter scattare il successivo. Quando elimini uno snapshot, vengono rimossi solo i dati che non sono necessari per altri snapshot.

Puoi ripristinare uno EBS snapshot Amazon su un volume di storage gateway locale se devi ripristinare un backup dei tuoi dati. Puoi anche utilizzare lo snapshot come punto di partenza per un nuovo EBS volume Amazon, che puoi quindi collegare a un'EC2istanza Amazon.

## Prezzi di Storage Gateway

Per informazioni aggiornate sui prezzi, consulta la sezione [Prezzi nella pagina dei](#) AWS Storage Gateway dettagli.

## 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 volumi: usando i gateway di volumi, è possibile creare volumi di archiviazione nel cloud Amazon Web Services. Le applicazioni locali possono accedervi come destinazioni Internet Small Computer System Interface (i). SCSI Sono disponibili due opzioni: volumi nella cache e volumi archiviati.
- Con i volumi memorizzati nella cache, i dati di volume vengono archiviati in una cache locale AWS, mentre una piccola parte dei dati a cui si accede di recente viene archiviata nella cache locale. Questo approccio permette l'accesso a bassa latenza ai set di dati usati di frequente. Fornisce inoltre un accesso senza interruzioni all'intero set di dati archiviato in. AWS Usando i volumi nella cache, è possibile dimensionare le risorse di storage senza dover effettuare il provisioning di hardware aggiuntivo.
- Con i volumi archiviati, è possibile archiviare l'intero set di dati di volume in locale e archiviare i point-in-time backup periodici (istantanee) in. AWS In questo modello, lo storage locale è primario e offre un accesso a bassa latenza all'intero set di dati. AWS lo storage è il backup che è possibile ripristinare in caso di emergenza nel data center.

Sia per i volumi memorizzati nella cache che per quelli archiviati, puoi scattare point-in-time istantanee dei tuoi volumi Volume Gateway sotto forma di istantanee AmazonEBS. Puoi

utilizzare un'istantanea del tuo volume come punto di partenza per un nuovo EBS volume Amazon, che puoi quindi collegare a un'EC2istanza Amazon. Utilizzando questo approccio, puoi fornire dati dalle tue applicazioni locali alle tue applicazioni in esecuzione su Amazon EC2 se hai bisogno di capacità di calcolo su richiesta aggiuntiva per l'elaborazione dei dati o capacità sostitutiva per scopi di disaster recovery. Ciò consente di creare copie con versione ed efficienti in termini di spazio dei volumi per la protezione, il ripristino, la migrazione e varie altre esigenze di trasferimento dei dati.

Per informazioni sulla creazione di un volume basato su uno EBS snapshot Amazon, consulta [Creazione di un volume](#).

Per una panoramica dell'architettura dei gateway di volumi, consulta [Architettura dei volumi memorizzati nella cache](#) e [Architettura dei volumi archiviati](#).

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

- 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 Linux Kernel-based Virtual Machine (). KVM Se distribuisce il gateway protetto un firewall, assicurati che le porte siano accessibili alla macchina virtuale del gateway. Per ulteriori informazioni, consulta [Requisiti per la configurazione di Volume Gateway](#).

# Iniziare con AWS Storage Gateway

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](#)
- [Regioni AWS che supportano Storage Gateway](#)
- [Requisiti per la configurazione di Volume Gateway](#)
- [Accedendo AWS Storage Gateway](#)

## 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 di un account Amazon Web Services

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
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 AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Per informazioni sui prezzi, consulta la pagina [Prezzi](#) nella pagina dei dettagli di Storage Gateway.

## Regioni AWS che supportano Storage Gateway

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 per la configurazione di Volume Gateway

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](#)
- [SCSISupportato negli iniziatori](#)

## 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 VMs

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 Volume Gateway , l'hardware deve dedicare le seguenti quantità diRAM:

- 16 GiB di spazio riservato RAM per gateway con dimensioni della cache fino a 16 TiB
- 32 GiB di spazio RAM riservato ai gateway con dimensioni della cache da 16 TiB a 32 TiB
- 48 GiB di spazio RAM riservato ai 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 EC2 istanze Amazon

Quando distribuisce il gateway su Amazon Elastic Compute Cloud EC2 (Amazon), la dimensione dell'istanza deve essere almeno troppo grande per il funzionamento del gateway. Tuttavia, per la famiglia di istanze ottimizzate per il calcolo, le dimensioni devono essere almeno 2xlarge.

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

- 16 GiB di spazio riservato RAM per gateway con dimensioni della cache fino a 16 TiB
- 32 GiB di spazio RAM riservato ai gateway con dimensioni della cache da 16 TiB a 32 TiB
- 48 GiB di spazio RAM riservato ai 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. Scegli la dimensione dell'istanza 2xlarge o superiore per soddisfare i requisiti richiesti. 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 (massimo)	Altri dischi locali richiesti
Gateway di volumi memorizzato nella cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway di volumi archiviato	—	—	150 GiB	2 TiB	1 o più per il volume o i volumi archiviati

### Note

È possibile configurare una o più unità locali per la cache e il buffer di caricamento, fino alla capacità massima.

Quando si aggiunge cache o buffer di caricamento a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza AmazonEC2). 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 l'accesso a Internet, alle reti locali, ai server Domain Name Service (DNS), ai firewall, ai router e così via. 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 limitano gli intervalli di indirizzi AWS 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, potresti implementare Storage Gateway su Amazon EC2 o utilizzare altri tipi di implementazione.

### Argomenti

- [Requisiti porta](#)
- [Requisiti di rete e di firewall per l'appliance hardware Storage Gateway](#)
- [Consentire AWS Storage Gateway l'accesso tramite firewall e router](#)
- [Configurazione dei gruppi di sicurezza per la tua istanza Amazon EC2 Gateway](#)

### 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 delle porte di rete per Volume Gateway](#).

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	43 (3) HTTPS	In uscita	Storage Gateway	AWS	Per la comunicazione dallo Storage Gateway all'endpoint del AWS servizio. Per informazioni sugli endpoint del servizio, consulta <a href="#">Consentire l'accesso tramite firewall e router</a> .
TCP	80 () HTTP	In entrata	L'host da cui si connette alla console AWS di gestione.	Storage Gateway	Dai sistemi locali per ottenere la chiave di attivazione di Storage Gateway.



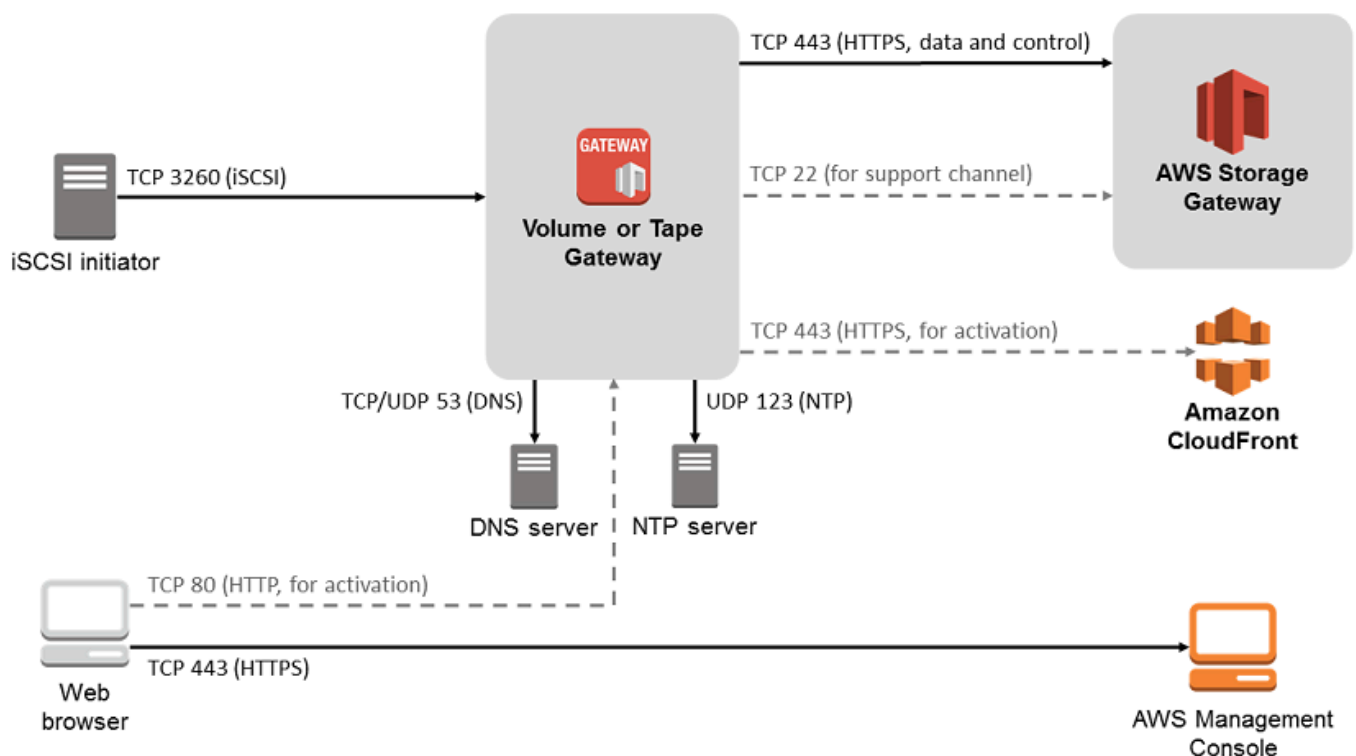
Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
					<p>La porta 80 viene usata solo durante l'attivazione dell'appliance Storage Gateway.</p> <p>Storage Gateway non richiede che la porta 80 sia accessibile pubblicamente. Il livello di accesso richiesto alla porta 80 dipende dalla 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.</p>

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

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
UDP	123 (NTP)	In uscita	NTPcliente	NTPserver	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 gateway di volumi e .



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

Protocollo	Porta	Direzione	Origine	Destinazione	Modalità di utilizzo
TCP	3260 (iSCSI)	In entrata	iSCSI) Iniziatori	Storage Gateway	Dai sistemi locali per connettersi ai SCSI target i esposti dal gateway.

Per informazioni dettagliate sui requisiti di porta, consulta [Requisiti delle porte di rete per Volume Gateway](#) nella sezione Risorse aggiuntive di Storage Gateway.

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

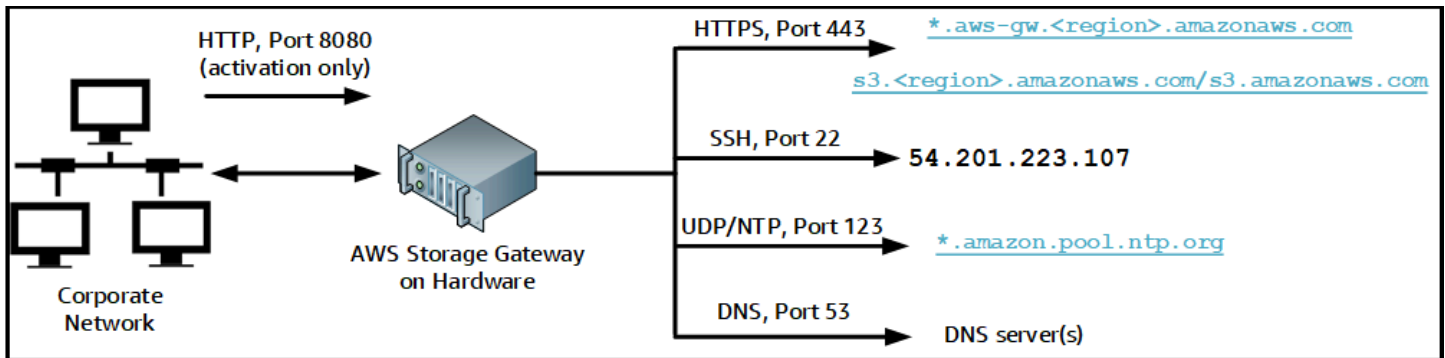
Ogni appliance hardware Storage Gateway richiede i seguenti servizi di rete:

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

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

1. i DRAC
2. em1
3. em2
4. em3
5. em4

È possibile utilizzare la DRAC porta i 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	DNSserver	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:

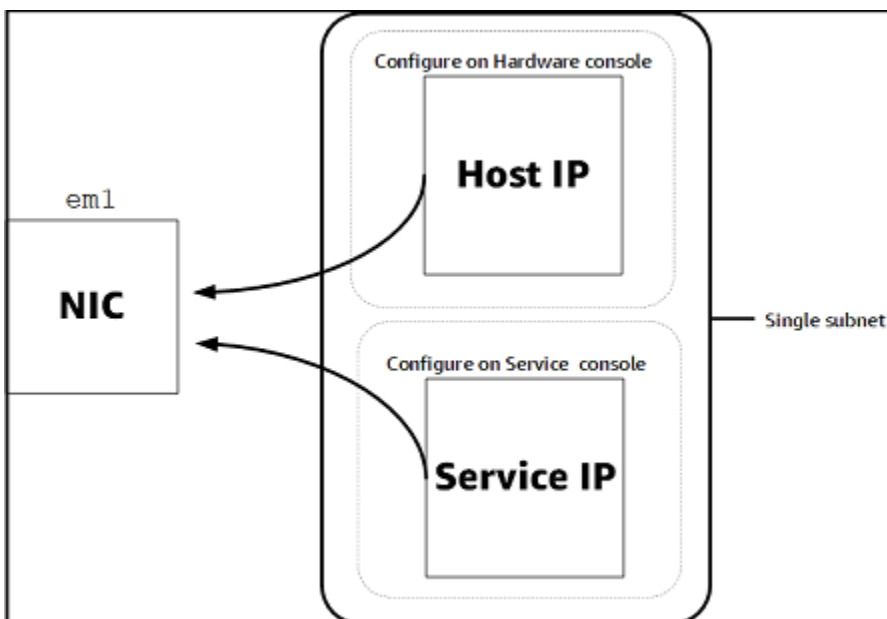
- Configurare tutte le interfacce di rete connesse nella console hardware.

- 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 [Installazione fisica del dispositivo hardware](#)

Tutti gli indirizzi IP sulla stessa interfaccia di rete (NIC), che si tratti di un gateway o di un host, devono trovarsi sulla 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 VPC endpoint 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 *region* nell'endpoint del servizio con la stringa di regione 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
```

Per effettuare API chiamate è necessario il seguente endpoint del servizio gateway.

```
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 FIPS servizio 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 per utilizzare i seguenti NTP server.

```
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 la tua istanza Amazon EC2 Gateway

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

- Il gruppo di sicurezza non deve permettere connessioni in entrata dall'esterno di Internet. Deve consentire solo alle istanze al suo interno di comunicare con il gateway. Se devi consentire alle istanze di connettersi al gateway dall'esterno del relativo gruppo di sicurezza, ti consigliamo di consentire le connessioni solo sulle porte 3260 (per SCSI le connessioni i) e 80 (per l'attivazione).
- Se desideri attivare il gateway da un EC2 host Amazon esterno al gruppo di sicurezza del gateway, consenti le connessioni in entrata sulla porta 80 dall'indirizzo IP di quell'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 AWS Support per la risoluzione dei problemi. Per ulteriori informazioni, consulta [Vuoi aiutarci AWS Support a risolvere i problemi del tuo gateway EC2](#).

In alcuni casi, potresti utilizzare un'EC2 istanza Amazon come iniziatore (ovvero, per connetterti alle SCSI destinazioni i) su un gateway che hai 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 delle porte di rete per Volume Gateway](#).

## Hypervisor supportati e requisiti di hosting

È possibile eseguire Storage Gateway in locale come appliance di macchina virtuale (VM) o appliance hardware fisica o come AWS istanza 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:

- VMwareESXiHypervisor (versione 7.0 o 8.0): per questa configurazione, è inoltre necessario un client per la connessione all'host. VMware vSphere
- 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 Linux (KVM): una tecnologia di virtualizzazione gratuita e open source. KVM è inclusa 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 e Ubuntu LTS 18.04. LTS Qualsiasi altra distribuzione Linux moderna può funzionare, ma la funzione o le prestazioni non sono garantite. Consigliamo questa opzione se disponi già di un KVM ambiente attivo e funzionante e se ne conosce già il funzionamento. KVM
- EC2Istanza Amazon: Storage Gateway fornisce un'Amazon Machine Image (AMI) che contiene l'immagine della macchina virtuale del gateway. Su Amazon possono essere distribuiti solo file, volumi memorizzati nella cache e tipi di gateway a nastro. EC2 Per informazioni su come implementare un gateway su AmazonEC2, consulta [Implementazione di un'EC2istanza Amazon per ospitare Volume Gateway](#).
- 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 ripristino di un gateway da una macchina virtuale creata da uno snapshot o da un clone di un'altra macchina virtuale gateway o dal tuo Amazon. EC2 AMI 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.

## SCSISupportato negli iniziatori

Quando si distribuisce un volume memorizzato nella cache o un Volume Gateway archiviato, è possibile creare volumi di SCSI storage i sul gateway.

Per connettersi a questi SCSI dispositivi i, Storage Gateway supporta i seguenti SCSI iniziatori i:

- 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
- VMwareESXInitiator, che fornisce un'alternativa all'utilizzo degli iniziatori nei sistemi operativi guest del VMs

 Important

Storage Gateway non supporta Microsoft Multipath I/O (MPIO) dai 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 raggruppato) senza utilizzarlo. WSFC

## 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'API endpoint Storage Gateway. Per ulteriori informazioni, consulta [Endpoint e quote di Storage Gateway](#) in Documentazione generale di riferimento di AWS .

Inoltre, è possibile utilizzare il AWS Storage Gateway API per configurare e gestire i gateway in modo programmatico. Per ulteriori informazioni su, vedere. API [API Riferimento per Storage Gateway](#)

È inoltre possibile utilizzarlo AWS SDKs per sviluppare applicazioni che interagiscono con Storage Gateway. Il AWS SDKs per Java, .NET e PHP racchiude lo Storage Gateway sottostante API per semplificare le attività di programmazione. Per informazioni sul download delle SDK librerie, consulta [Sample Code Libraries](#).

# 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 i dispositivi hardware dalla pagina Panoramica del dispositivo 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 del dispositivo 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

- [Regioni supportate AWS](#)
- [Configurazione dell'appliance hardware](#)
- [Installazione fisica del dispositivo hardware](#)
- [Configurazione dei parametri di rete](#)
- [Attivazione dell'appliance hardware](#)
- [Creazione di un gateway](#)
- [Configurazione di un indirizzo IP per il gateway](#)
- [Configurazione del gateway](#)
- [Rimozione di un gateway dall'appliance hardware](#)
- [Eliminazione dell'appliance hardware](#)

## 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

## Installare e configurare l'appliance hardware

1. Montare l'appliance su rack e collegare l'alimentazione e le connessioni di rete. Per ulteriori informazioni, consulta [Installazione fisica del dispositivo hardware](#).
2. Impostare gli indirizzi Internet Protocol versione 4 (IPv4) sia per l'appliance hardware (l'host) che per lo 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 Storage Gateway sulla tua appliance hardware. Per ulteriori informazioni, consulta [Configurazione del gateway](#).

Puoi configurare i gateway sul tuo dispositivo hardware nello stesso modo in cui configuri i gateway su VMware ESXi Microsoft Hyper-V, Linux Kernel-based Virtual Machine () o Amazon. KVM EC2

## Aumento dello storage della cache utilizzabile

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

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

1. Ripristina le impostazioni di fabbrica dell'appliance hardware. Contatta il supporto di Amazon Web Services per le istruzioni su come eseguire questa operazione.
2. Aggiungi cinque 1,92 TB SSDs all'appliance.

### Opzioni della scheda di interfaccia di rete

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

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

## Installazione fisica del dispositivo hardware

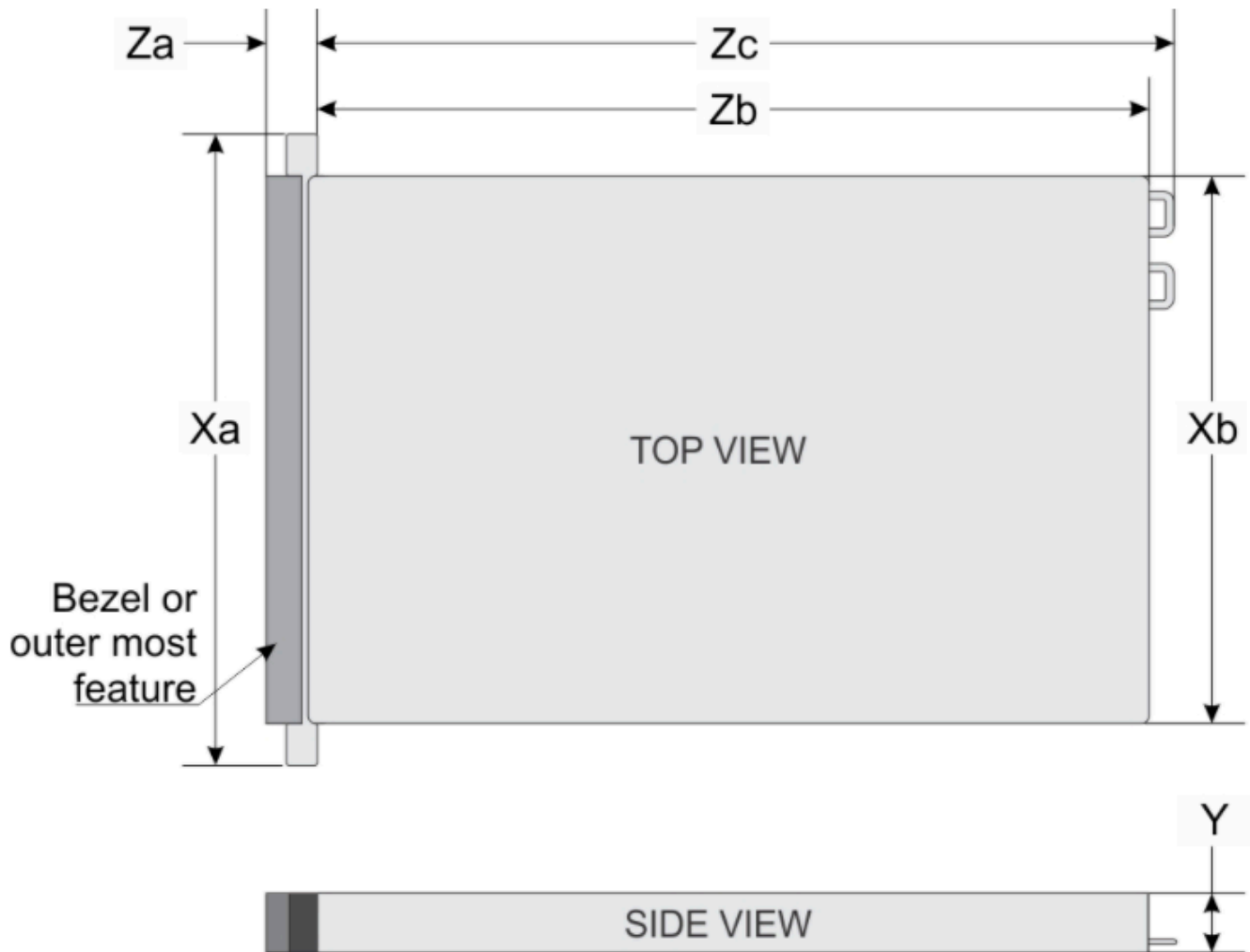
Dopo aver disimballato l'appliance hardware Storage Gateway, seguire le istruzioni contenute nella confezione per montare su rack il server. L'apparecchio ha un fattore di forma 1U e si inserisce in un rack da 19 pollici conforme allo standard della International Electrotechnical Commission (IEC).

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'apparecchiatura hardware). Twinax CopperDAC, SFP + modulo ottico (compatibile con Intel) o SFP ricetrasmittitore in rame Base-T.
- Tastiera e monitor oppure una soluzione di commutazione tra tastiera, video e mouse (). KVM

## Dimensioni dell'appliance hardware

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



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 cornice.



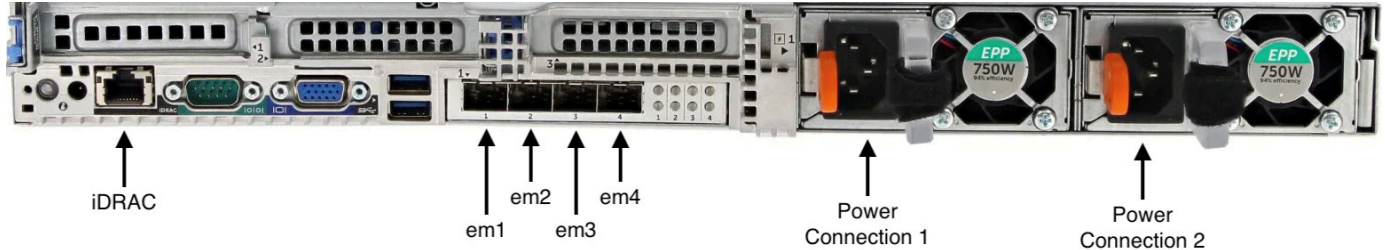
## Collegare il dispositivo hardware all'alimentazione

### 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 VLAN trunking. Configura la porta dello switch a cui stai collegando l'appliance hardware come porta non trunked. 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.

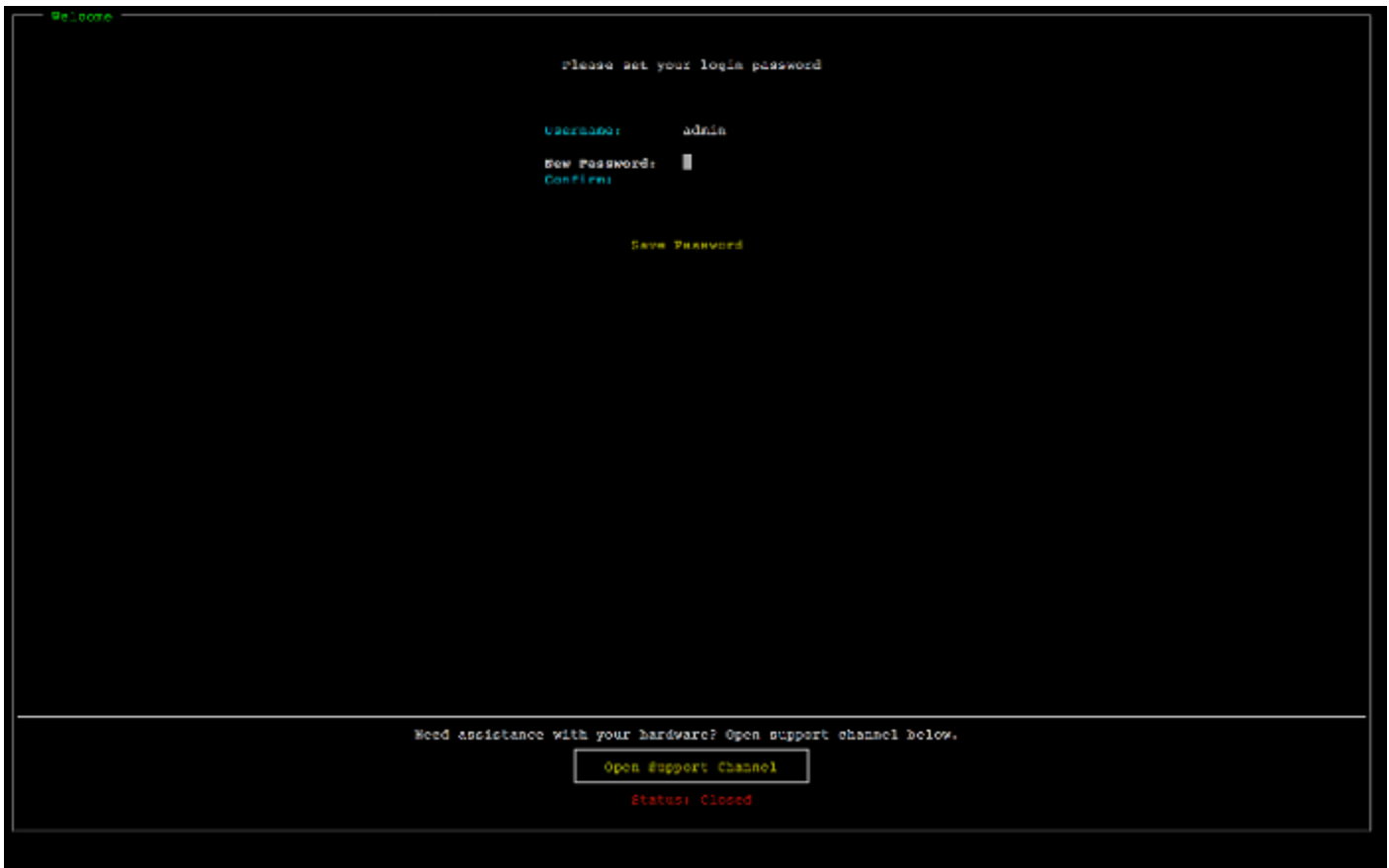
Dopo l'avvio del server, la console hardware viene visualizzata sul monitor. La console hardware presenta un'interfaccia utente specifica AWS che è possibile utilizzare per configurare i parametri di rete iniziali. È possibile configurare questi parametri per collegare l'appliance a AWS e aprire un canale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

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 [Installazione fisica del dispositivo hardware](#).

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.

- Per Indirizzo IP, immettere un IPv4 indirizzo valido proveniente da una delle seguenti fonti:
  - Utilizzate l'IPv4 indirizzo assegnato dal server Dynamic Host Configuration Protocol (DHCP) alla porta di rete fisica.

In tal caso, annota questo IPv4 indirizzo per utilizzarlo in seguito nella fase di attivazione.

- Assegna un IPv4 indirizzo 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 inserito un IPv4 indirizzo valido, premi Down arrow o Tab.

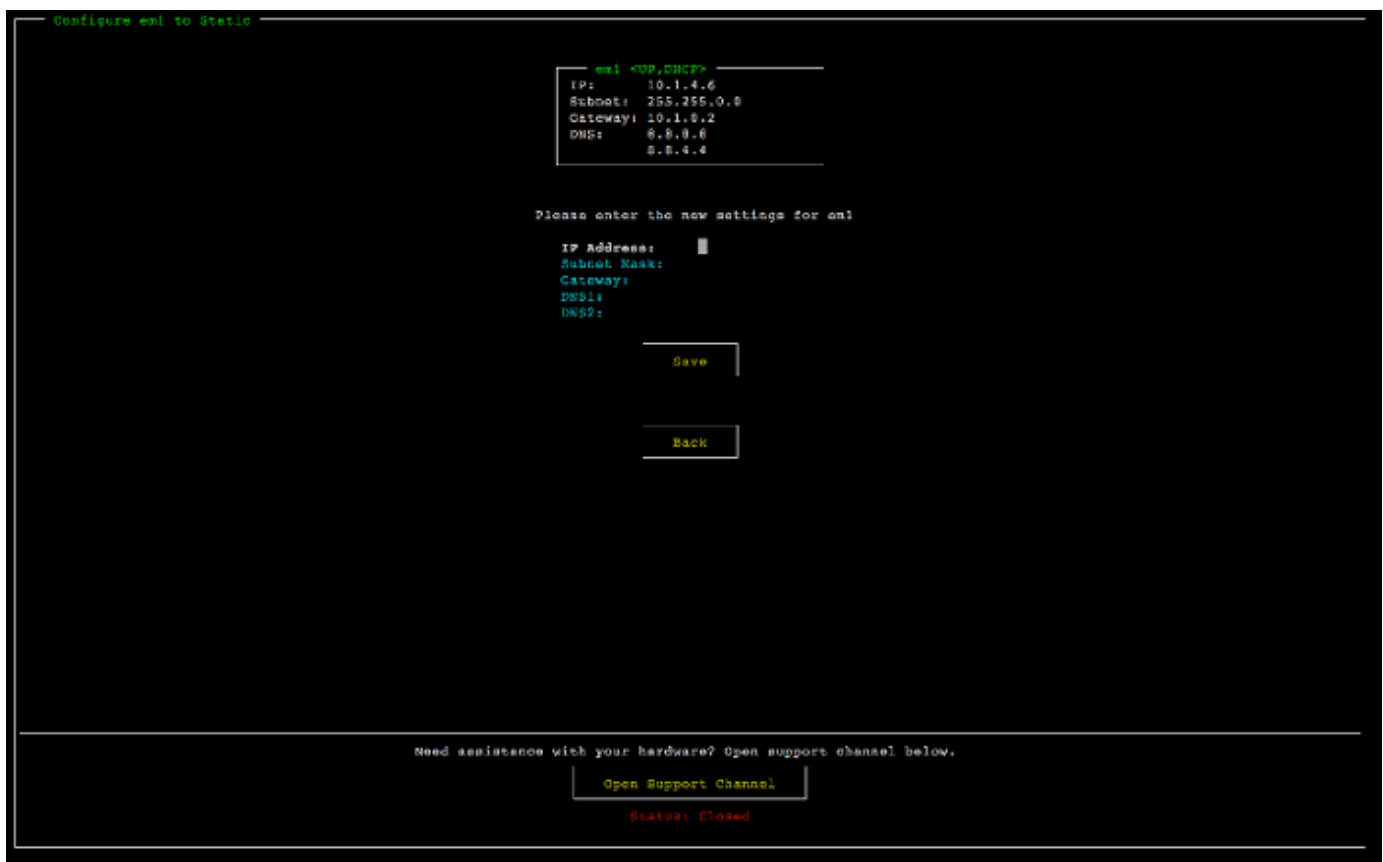
**Note**

È possibile utilizzare questa procedura per configurare altre interfacce di rete oltre a em1 per la ridondanza. Se configuri altre interfacce, queste devono fornire la stessa connessione sempre attiva agli endpoint elencati nei requisiti. AWS

Il Network Bonding e il Link Aggregation Control Protocol (LACP) non sono supportati dall'appliance hardware o da Storage Gateway.

Si sconsiglia di configurare più interfacce di rete sulla sottorete, in quanto ciò a volte può causare problemi di routing.

la console dell'appliance hardware si configura NIC su uno schermo IP statico.



la console dell'appliance hardware è configurata NIC su uno schermo IP statico.

3. Per Subnet (Sottorete), immettere una maschera di sottorete valida, quindi premere Down arrow.
4. Per Gateway, inserisci l'IPv4indirizzo del gateway di rete, quindi premiDown arrow.

5. Per DNS1, inserisci l'IPv4 indirizzo del tuo server Domain Name Service (DNS), quindi premi `Down arrow`.
6. (Facoltativo) Per DNS2, inserisci un secondo IPv4 indirizzo, quindi premi `Down arrow`. Un'assegnazione di un secondo DNS server fornirebbe una ridondanza aggiuntiva nel caso in cui il primo DNS server non fosse più disponibile.
7. Scegliete `Salva`, quindi premete `Enter` per salvare l'impostazione IPv4 dell'indirizzo statico per l'appliance.

Per disconnettersi dalla console hardware

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

Approfondimenti

[Attivazione dell'appliance hardware](#)

## Attivazione dell'appliance hardware

Dopo aver configurato l'indirizzo IP, è necessario immettere tale indirizzo IP 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 qualsiasi 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 HTTP l'accesso alla porta 8080 dell'appliance per il traffico in entrata.

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

Per ulteriori informazioni sulla configurazione dell'indirizzo IP, consulta [Configurazione dei parametri di rete](#).

5. Per Nome, inserisci un nome per il dispositivo. I nomi possono contenere fino a 255 caratteri e non possono includere uno slash.
6. Per Fuso orario del dispositivo hardware inserisci il fuso orario locale da cui verrà generata la maggior parte del carico di lavoro per il gateway, quindi scegli Avanti.

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

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

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

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

## Approfondimenti

[Creazione di un gateway](#)



## Creazione di un gateway

È possibile creare un S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway sull'appliance hardware.

Per creare un gateway sull'appliance hardware

1. Accedi AWS Management Console e apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
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 impostare, 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. Possono volerci 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 tue applicazioni (come il tuo NFS SMB client, il tuo SCSI iniziatore i e così via) 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.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

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.  
gateway, console locale, pagina di configurazione della rete con DHCP opzioni IP statiche.

```
AWS Storage Gateway Network Configuration
1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: _
```

gateway, console locale, pagina di configurazione della rete con DHCP opzioni IP statiche.

7. Configurate un indirizzo DHCP IP o statico per la porta di rete del vostro dispositivo hardware per presentare un file, un volume e un gateway a nastro 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 `Crt1+]` (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 [Configura gateway per il tipo di gateway in uso](#). Per le istruzioni, consulta e [Configurazione del gateway di volumi](#).

## 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 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.

## 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 della panoramica in questa pagina forniscono un riepilogo di alto livello su come funziona il processo di creazione di 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 di volume](#).

## Panoramica: attivazione del gateway

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

## Configurazione di un gateway

Per configurare Storage Gateway, è necessario innanzitutto scegliere il tipo di gateway che si desidera creare e la piattaforma host su cui eseguire l'appliance virtuale gateway. È quindi necessario scaricare il modello di appliance virtuale gateway per la piattaforma prescelta e distribuirlo nell'ambiente on-premise. Puoi anche implementare lo Storage Gateway come appliance hardware fisica che ordini dal tuo rivenditore preferito o come EC2 istanza Amazon nel tuo AWS ambiente cloud. 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 AmazonVPC, dove hai il pieno controllo sulla configurazione di sicurezza della rete. È quindi necessario specificare l'indirizzo IP del gateway o la relativa chiave di attivazione, che è possibile ottenere collegandosi alla console locale sull'appliance gateway.

## Rivedi e attiva

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

## Panoramica: configurazione del gateway

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

## Panoramica: risorse di archiviazione

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

## Creazione di un gateway di volumi

In questa sezione, puoi trovare le istruzioni su come creare e utilizzare un gateway di volumi.

### Argomenti

- [Creazione di un gateway](#)
- [Creazione di un volume](#)
- [Uso del volume](#)
- [Backup dei volumi](#)

## Creazione di un gateway

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

### Argomenti

- [Configura un gateway di volumi](#)
- [Connetti il gateway di volumi a AWS](#)

- [Revisione delle impostazioni e attivazione del gateway di volumi](#)
- [Configurazione del gateway di volumi](#)

## Configura un gateway di volumi

Per configurare un nuovo gateway di volumi

1. Apri AWS Management Console <https://console.aws.amazon.com/storagegateway/home/> e scegli Regione AWS dove vuoi creare il tuo gateway.
2. Scegli Create gateway (Crea gateway) per aprire la pagina Set up gateway (Configura gateway).
3. Nella sezione Impostazioni gateway, procedi nel seguente modo:
  - a. Per Gateway name (Nome gateway), inserire un nome per il gateway. 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 volumi, quindi scegli il tipo di volume che verrà utilizzato dal gateway. Puoi scegliere tra le seguenti opzioni:
  - Volumi memorizzati nella cache: archivia i dati primari in Amazon S3 e conserva i dati a cui si accede di frequente localmente nella cache per un accesso più rapido.
  - Volumi archiviati: archivia tutti i dati localmente eseguendone anche il backup in modo asincrono su Amazon S3. I gateway che utilizzano questo tipo di volume non possono essere distribuiti su Amazon EC2.
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 del gateway utilizzando VMware ESXi.
    - Microsoft Hyper-V: scarica, implementa e configura la macchina virtuale del gateway utilizzando Microsoft Hyper-V.
    - Linux KVM: scarica, implementa e configura la macchina virtuale del 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. In Confirm set up gateway (Conferma configurazione gateway), seleziona la casella di controllo per confermare di aver eseguito i passaggi di implementazione per la piattaforma host scelta. Questo passaggio non è applicabile alla piattaforma host dell'appliance hardware.
6. Scegli Successivo per continuare.

Ora che il gateway è configurato, devi scegliere come connetterlo e comunicare. AWS Per istruzioni, consulta [Connect your Volume Gateway a AWS](#).

## Connetti il gateway di volumi a AWS

Per connettere un nuovo Volume Gateway a AWS

1. Completa la procedura descritta in [Configurare un gateway di volumi](#) se non l'hai già fatto. Al termine, scegliere Avanti per aprire la pagina Connect to (Connessione a) AWS 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 con 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 volumi](#).

## Revisione delle impostazioni e attivazione del gateway di volumi

Per attivare un nuovo gateway di volumi

1. Se non è già stato fatto, completare le procedure descritte negli argomenti seguenti:
  - [Configurare un gateway di volumi](#)
  - [Connect Volume 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 la creazione 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 volumi](#).

## Configurazione del gateway di volumi

Per eseguire la prima configurazione su un nuovo gateway di volumi

1. Se non è già stato fatto, completare le procedure descritte negli argomenti seguenti:
  - [Configurare un gateway di volumi](#)
  - [Connect Volume Gateway a AWS](#)
  - [Revisione delle impostazioni e attivazione del gateway di volumi](#)

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 ARCHIVIAZIONE CACHE e almeno un disco con almeno 150 GiB di capacità per BUFFER DI CARICAMENTO. 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 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.

**Note**

Per ricevere i log di integrità dello Storage Gateway, nella politica delle risorse del gruppo di log devono essere presenti le seguenti autorizzazioni. Sostituisci la *sezione evidenziata* con le informazioni specifiche del gruppo di log ResourceArn per la tua distribuzione.

```
"Sid": "AWSLogDeliveryWrite20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

L'elemento «Resource» è richiesto solo se si desidera che le autorizzazioni si applichino esplicitamente a un singolo gruppo di log.

4. Nella sezione CloudWatch allarmi, scegli come configurare gli CloudWatch allarmi Amazon per avvisarti quando le metriche del 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`: creazione di allarmi
  - `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
  - `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
  - `cloudwatch>DeleteAlarms`: eliminazione di allarmi
- Crea un allarme personalizzato: configura un nuovo CloudWatch allarme per 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 Panoramica del gateway di Storage Gateway.

Dopo aver creato il gateway, è necessario creare un volume da utilizzare. Per istruzioni, consulta [Creazione di un volume](#).

## Creazione di un volume

Hai già allocato i dischi locali aggiunti allo storage della cache e al buffer di caricamento della VM. È giunto il momento di creare un volume di storage su cui le applicazioni possano leggere e scrivere dati. Il gateway conserva i dati del volume a cui è stato effettuato l'accesso di recente in locale nello storage della cache e i dati trasferiti in modo asincrono su Amazon S3. Per i volumi di storage, hai allocato dischi locali associati ai dati dell'applicazione e al buffer di caricamento della VM.

### Note

Puoi usare AWS Key Management Service (AWS KMS) per crittografare i dati scritti su un volume memorizzato nella cache archiviato in Amazon S3. Al momento, questa operazione è possibile utilizzando ilAWS Storage Gateway Riferimento API . [Per ulteriori informazioni, consulta `CreateCachedi ScsiVolume` o `create-cached-iscsi-volume`](#)

## Per creare un volume

1. Apri la console Storage Gateway all'indirizzo <https://console.aws.amazon.com/storagegateway/home>.
2. Nella console Storage Gateway selezionare Create volume (Crea volume).
3. Nella finestra di dialogo Create volume (Crea volume) scegliere un gateway in Gateway.
4. Digitare la capacità per i volumi nella cache in Capacity (Capacità).

Per i volumi archiviati, scegliere un valore Disk ID (ID disco) dall'elenco.

5. Le opzioni disponibili per Volume content (Contenuti del volume) dipendono dal tipo di gateway per cui si crea il volume.

I volumi nella cache presentano le seguenti opzioni:

- Create a new empty volume (Crea un nuovo volume vuoto).
- Create a volume based on an EBS snapshot (Crea un volume basato su uno snapshot EBS). Se si sceglie questa opzione, occorre assegnare un valore a EBS snapshot ID (ID snapshot EBS).

### Note

Storage Gateway non supporta la creazione di volumi memorizzati nella cache da istantanee dei Marketplace AWS volumi.

- Clone from last volume recovery point (Clona dall'ultimo punto di ripristino del volume). La scelta di questa opzione richiede la selezione di un ID volume per Source volume (Volume sorgente). In assenza di volumi nella regione, questa opzione non viene visualizzata.

I volumi archiviati presentano le seguenti opzioni:

- Create a new empty volume (Crea un nuovo volume vuoto).
  - Create a volume based on a snapshot (Crea un volume basato su una snapshot). Se si sceglie questa opzione, occorre assegnare un valore a EBS snapshot ID (ID snapshot EBS).
  - Preserve existing data on the disk (Mantieni i dati esistenti sul disco)
6. Digitare un nome per iSCSI target name (Nome destinazione iSCSI).

Il nome della destinazione può includere lettere minuscole, numeri, punti (.) e trattini (-) e Viene visualizzato come nome di iSCSI target node (Nodo destinazione iSCSI) nella scheda Targets (Destinazioni) dell'interfaccia utente iSCSI Microsoft initiator (Iniziatore Microsoft iSCSI), dopo l'individuazione. Ad esempio, il nome target1 viene visualizzato come iqn.1007-05.com.amazon:target1. Accertarsi che il nome della destinazione sia lo stesso in tutta la rete di storage SAN (Storage Area Network).

7. Assicurarsi che Network interface (Interfaccia di rete) includa un indirizzo IP selezionato o scegliere un indirizzo IP per Network interface (Interfaccia di rete). L'elenco di Network interface (Interfaccia di rete) annovera un indirizzo IP per ogni scheda configurata per la macchina virtuale (VM) del gateway. Se la VM del gateway supporta un'unica scheda di rete e vi è quindi un solo indirizzo IP, non compare alcun elenco per Network interface (Interfaccia di rete).

La destinazione iSCSI sarà disponibile nella scheda di rete selezionata.

Se il gateway è configurato per l'utilizzo di più schede di rete, occorre specificare l'indirizzo IP che le applicazioni di storage dovranno adoperare per accedere al volume. Per informazioni sulla configurazione di più schede di rete, consulta [Configurazione del gateway per più utenti NICs](#).

#### Note

Un volta selezionata una scheda di rete, la configurazione non può essere modificata.

8. (Facoltativo) In Tags (Tag), immettere una chiave e un valore per aggiungere tag al volume. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare i volumi.
9. Selezionare Create volume (Crea volume).

Eventuali volumi precedentemente creati in questa regione sono elencati nella console Storage Gateway.

Viene visualizzata la finestra di dialogo Configure CHAP Authentication (Configura autenticazione CHAP). È possibile configurare il protocollo CHAP (Challenge-Handshake Authentication Protocol) per il volume o farlo successivamente selezionando Cancel (Annulla). Per ulteriori informazioni sulla configurazione CHAP, consulta [Configurazione dell'autenticazione CHAP per i volumi](#).

The screenshot displays the AWS Management Console interface for storage volumes. At the top, there are buttons for 'Create volume' and 'Actions'. Below is a search bar and a table of volumes. The table has columns for Volume ID, Status, Type, Used, Size, and Gateway. The volume 'vol-0e0eb15a2996b3094' is selected, and its details are shown in a 'Details' tab below. The 'Used' field in the details is highlighted with a red box, showing 14.895 GiB.

Volume ID	Status	Type	Used	Size	Gateway
vol-0020a0ecea492c714	Gateway offline	Cached	-	50 GiB	
vol-013c985f1fa00a284	Available	Cached	0%	30 GiB	
vol-0ba4f299e5a12f9b1	Available	Cached	3%	100 GiB	
vol-0e0eb15a2996b3094	Available	Cached	74%	20 GiB	
vol-0518ba25750e1ddb6	Working stor...	Stored	14.895 GiB	150 GiB	

Details	
Volume ID	vol-0e0eb15a2996b3094 (Cached)
Gateway	
CHAP authentication	No
Target name	iqn.1997-05.com.amazon:aws:vol-test-2
Initiator	10.0.0.10:10.10.0.10
Status	Available
Used	14.895 GiB
Size	20 GiB
Monitoring	Cloudwatch
Host IP	
Host port	3260
Snapshot schedule	-
Created	9/26/2017, 8:57:34 PM

Se non si desidera configurare il protocollo CHAP, si può iniziare direttamente a utilizzare il volume. Per ulteriori informazioni, consulta [Uso del volume](#).

## Configurazione dell'autenticazione CHAP per i volumi

Il protocollo CHAP offre protezione dagli attacchi di riproduzione richiedendo l'autenticazione per accedere alle destinazioni del volume di storage. Nella finestra di dialogo Configure CHAP Authentication (Configura autenticazione CHAP), fornisci informazioni per configurare il protocollo CHAP relativo ai volumi.

### Configurazione CHAP

1. Scegliere il volume per il quale configurare il protocollo CHAP.
2. Nel menu Actions (Operazioni), selezionare Configure CHAP authentication (Configura autenticazione CHAP).
3. In Initiator Name (Nome iniziatore), digita il nome dell'iniziatore.
4. In Initiator secret (Segreto dell'iniziatore), digita la frase segreta utilizzata per autenticare l'iniziatore iSCSI.
5. In Target secret (Segreto della destinazione), digitare la frase segreta utilizzata per autenticare la destinazione per il protocollo CHAP reciproco.
6. Seleziona Save (Salva) per salvare le voci.

Per ulteriori informazioni sulla configurazione dell'autenticazione CHAP, consulta [Configurazione dell'CHAP autenticazione per i tuoi obiettivi iSCSI](#).



## Approfondimenti

### [Uso del volume](#)

## Uso del volume

Di seguito sono disponibili istruzioni su come usare il volume. Per utilizzare il volume, è necessario innanzitutto collegarlo al client come SCSI destinazione i, quindi inicializzarlo e formattarlo.

### Argomenti

- [Collegamento dei volumi al tuo client](#)
- [Inizializzazione e formattazione del volume](#)
- [Test del gateway](#)
- [Cosa fare in seguito?](#)

## Collegamento dei volumi al tuo client

Utilizzi l'SCSIiniziatore i del tuo client per connetterti ai tuoi volumi. Al termine della procedura seguente, i volumi diventano disponibili come dispositivi locali sul client.

### Important

Con Storage Gateway, è possibile connettere più host allo stesso volume se gli host coordinano l'accesso utilizzando Windows Server Failover Clustering (WSFC). Non è possibile connettere più host allo stesso volume senza utilizzare WSFC, ad esempio condividendo, un file system /ext4 non raggruppato NTFS.

### Argomenti

- [Connessione a un client Microsoft Windows](#)
- [Connessione a un client Red Hat Enterprise Linux](#)

## Connessione a un client Microsoft Windows

La procedura seguente mostra un riepilogo delle operazioni da eseguire per connettersi a un client Windows. Per ulteriori informazioni, consulta [Connessione degli SCSI iniziatori](#).

## Per connettersi a un client HSM Windows

1. Avviare iscsicpl.exe.
2. Nella finestra di dialogo i SCSI Initiator Properties, scegliete la scheda Discovery, quindi scegliete Discovery Portal.
3. Nella finestra di dialogo Discover Target Portal, digita l'indirizzo IP del tuo i SCSI target come indirizzo IP o DNS nome.
4. Connettere il nuovo portale di destinazione al volume di storage di destinazione nel gateway:
5. Selezionare la destinazione, quindi Connect (Connetti).
6. Nella scheda Targets (Destinazioni), verificare che lo stato di destinazione abbia il valore Connected (Connesso), che indica che la destinazione è collegata, quindi scegliere OK.

## Connessione a un client Red Hat Enterprise Linux

La procedura seguente mostra un riepilogo dei passaggi da seguire per connettersi a un client Red Hat Enterprise Linux (RHEL). Per ulteriori informazioni, consulta [Connessione degli SCSI iniziatori](#).

### Per connettere un client Linux a i SCSI target

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

Puoi utilizzare il seguente comando per installare il pacchetto.

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

2. Assicurati che il SCSI demone i sia in esecuzione.

Per RHEL 5 o 6, usate il seguente comando.

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

Per RHEL 7, usa il seguente comando.

```
sudo service iscsid status
```

3. Scopri i target di volume o VTL dispositivo 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 dovrebbe essere simile all'out 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.

Assicurati di specificare quello corretto `[GATEWAY_IP]` e IQN nel comando connect.

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
```

Si consiglia vivamente di personalizzare le SCSI impostazioni i dopo aver configurato l'iniziatore, come illustrato in [Personalizzazione delle impostazioni di Linux i SCSI](#).

## Inizializzazione e formattazione del volume

Dopo aver utilizzato l'SCSIiniziatore i nel client per connettersi ai volumi, è possibile inizializzare e formattare il volume.

### Argomenti

- [Inizializzazione e formattazione del volume in Microsoft Windows](#)
- [Inizializzazione e formattazione del volume in Red Hat Enterprise Linux](#)

## Inizializzazione e formattazione del volume in Microsoft Windows

Usa la procedura seguente per inizializzare e formattare il volume in Windows.

Per inizializzare e formattare il volume di storage

1. Avviare **diskmgmt.msc** per aprire la console Disk Management (Gestione disco).
2. Nella finestra di dialogo Initialize Disk, inizializzate il volume come partizione MBR(Master Boot Record). Quando si seleziona lo stile della partizione, è necessario tenere conto del tipo di volume cui ci si sta connettendo, presente nella cache o archiviato, come mostrato nella tabella seguente.

Stile di partizione	Uso in base alle condizioni seguenti
MBR(Master Boot Record)	<ul style="list-style-type: none"><li>• Se il gateway è un volume archiviato e le dimensioni del volume di storage sono limitate a un 1 TiB.</li><li>• Se il gateway è un volume nella cache e il volume di storage ha dimensioni inferiori a 2 TiB.</li></ul>
GPT(Tabella GUID delle partizioni)	Se il volume di storage del gateway è di 2 TiB o di dimensioni maggiori.

3. Creare un volume semplice:
  - a. Portate il volume online per iniziarlo. Tutti i volumi disponibili vengono visualizzati nella console di gestione dei dischi.
  - b. Aprire il menu contestuale (clic con il pulsante destro del mouse) per il disco e quindi scegliere New Simple Volume (Nuovo volume semplice).

### Important

Assicurarsi di non formattare il disco errato. Verificare che il disco che si sta formattando corrisponda alla dimensione del disco locale allocato alla macchina virtuale del gateway e che il suo stato sia Unallocated (Non allocato).

- c. Specificare la dimensione massima del disco.
- d. Assegnare una lettera di unità o un percorso al volume e formattare il volume scegliendo Perform a quick format (Esegui formattazione veloce).

**⚠ Important**

Consigliamo assolutamente di utilizzare Perform a quick format (Esegui formattazione veloce) per i volumi nella cache. In questo modo, si ottiene un I/O di inizializzazione inferiore, dimensioni di snapshot iniziali minori e tempi più rapidi per un volume utilizzabile. Si evita inoltre di usare spazio del volume nella cache per il processo di formattazione completo.

**ℹ Note**

Il tempo necessario per formattare il volume dipende dalle dimensioni del volume. Il completamento del processo può richiedere alcuni minuti.

## Inizializzazione e formattazione del volume in Red Hat Enterprise Linux

Utilizzate la seguente procedura per inizializzare e formattare il volume su Red Hat Enterprise Linux (RHEL).

Per inizializzare e formattare il volume di storage

1. Cambiare directory passando alla cartella `/dev`.
2. Esegui il comando `sudo cfdisk`.
3. Identificare il nuovo volume usando il comando seguente. Per trovare nuovi volumi, è possibile visualizzare l'elenco del layout delle partizioni dei volumi.

```
$ lsblk
```

Viene visualizzato un errore che indica la presenza di un'etichetta di volumi non riconosciuti per il nuovo volume non partizionato.

4. Inizializzare il nuovo volume. Quando si seleziona lo stile della partizione, è necessario tenere conto delle dimensioni e del tipo di volume cui ci si sta connettendo, presente nella cache o archiviato, come mostrato nella tabella seguente.

Stile di partizione	Uso in base alle condizioni seguenti
MBR(Master Boot Record)	<ul style="list-style-type: none"> <li>• Se il gateway è un volume archiviato e le dimensioni del volume di storage sono limitate a un 1 TiB.</li> <li>• Se il gateway è un volume nella cache e il volume di storage ha dimensioni inferiori a 2 TiB.</li> </ul>
GPT(Tabella GUID delle partizioni)	Se il volume di storage del gateway è di 2 TiB o di dimensioni maggiori.

Per una MBR partizione, utilizzare il seguente comando: `sudo parted /dev/your volume mklabel msdos`

Per una GPT partizione, utilizzate il seguente comando: `sudo parted /dev/your volume mklabel gpt`

5. Creare una partizione usando il comando seguente.

```
sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
```

6. Assegna una lettera di unità alla partizione e creare un file system usando il comando seguente.

```
sudo mkfs -L datapartition /dev/your volume
```

7. Montare il file system usando il comando seguente.

```
sudo mount -o defaults /dev/your volume /mnt/your directory
```

## Test del gateway

Per eseguire il test della configurazione del gateway di volumi, attieniti alla procedura seguente:

1. Scrivi dati sul volume
2. Acquisisci una snapshot.
3. Ripristina la snapshot per un altro volume.

È possibile verificare la configurazione di un gateway eseguendo un backup istantaneo del volume e archiviando l'istantanea in AWS Ripristina quindi la snapshot per un nuovo volume. Il gateway copia i dati dall'istantanea specificata nel nuovo AWS volume.

#### Note

Il ripristino dei dati da volumi Amazon Elastic Block Store (AmazonEBS) crittografati non è supportato.

Per creare uno EBS snapshot Amazon di un volume di archiviazione su Microsoft Windows

1. Sul computer Windows, copiare alcuni dei dati mappati sul volume di storage.

La quantità di dati copiati non è determinante ai fini di questa dimostrazione. Un file di dimensioni ridotte è sufficiente per dimostrare il processo di ripristino.

2. Nel riquadro di navigazione della console Storage Gateway, scegliere Volumi.
3. Scegliere il volume di storage creato per il gateway.

Questo gateway deve avere solo un volume di storage. La selezione del volume consente di visualizzarne le proprietà.

4. Per Azioni, scegli Crea EBS istantanea per creare un'istantanea del volume.

A seconda della quantità di dati su disco e della larghezza di banda di caricamento, potrebbero essere necessari alcuni secondi per completare la snapshot. Annotare l'ID del volume per il volume da cui si crea una snapshot. Per trovare la snapshot si utilizza l'ID del volume.

5. Nella finestra di dialogo Crea EBS istantanea, fornite una descrizione per l'istantanea.
6. (Facoltativo) In Tags (Tag), immettere una chiave e un valore per aggiungere tag alla snapshot. Un tag è una coppia chiave-valore che fa distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare le snapshot.
7. Selezionare Create Snapshot (Crea snapshot). La tua istantanea viene archiviata come EBS istantanea Amazon. Prendere nota dell'ID snapshot. Il numero di snapshot create per il tuo volume viene visualizzato nella colonna snapshot.
8. Nella colonna EBSistantanee, scegli il link per il volume per cui hai creato lo snapshot per visualizzarlo sulla console EBS Amazon. EC2

Per ripristinare una snapshot in un altro volume

Per informazioni, consulta [Creazione di un volume](#).

## Cosa fare in seguito?

Nelle sezioni precedenti, hai creato ed effettuato il provisioning di un gateway, quindi hai connesso il tuo host al volume di storage del gateway. Hai aggiunto dati al SCSI volume i del gateway, hai scattato un'istantanea del volume e l'hai ripristinata su un nuovo volume, ti sei connesso al nuovo volume e hai verificato che i dati fossero presenti su di esso.

Una volta completato l'esercizio, considera quanto segue:

- Se intendi continuare a utilizzare il gateway, leggi le informazioni sul dimensionamento ideale del buffer di caricamento per carichi di lavoro reali. Per ulteriori informazioni, consulta [Dimensionamento dello storage del gateway del volume per carichi di lavoro reali](#).
- Se non intendi continuare a utilizzare il gateway, considera di eliminare il gateway per evitare di incorrere in costi di utilizzo. Per ulteriori informazioni, consulta [Eliminazione delle risorse non necessarie](#).

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

- Per ulteriori informazioni sui volumi di storage e su come gestirli, consulta [Gestione del gateway](#).
- Per risolvere problemi con il gateway, consulta [Risoluzione dei problemi del gateway](#).
- Per ottimizzare il gateway, consulta [Ottimizzazione delle prestazioni del gateway](#).
- Per ulteriori informazioni sui parametri Storage Gateway e su come monitorare le prestazioni del gateway, consulta [Monitoraggio di Storage Gateway](#).
- Per ulteriori informazioni sulla configurazione SCSI degli obiettivi i del gateway per l'archiviazione dei dati, consulta. [Connessione ai volumi in un client Windows](#)

Per ulteriori informazioni sul dimensionamento dell'archiviazione del gateway di volumi per carichi di lavoro reali e sulla rimozione delle le risorse non necessarie, consulta le seguenti sezioni.

## Dimensionamento dello storage del gateway del volume per carichi di lavoro reali

A questo punto, disponi di un gateway semplice e funzionante. Tuttavia, i presupposti utilizzati per creare questo gateway non sono ideali per carichi di lavoro reali. Per usare questo gateway per carichi di lavoro reali, è necessario eseguire due operazioni:



1. Dimensionare il buffer di caricamento in modo appropriato.
2. Se ancora non è stato fatto, configurare il monitoraggio del buffer di caricamento.

Di seguito è illustrato come eseguire entrambe queste attività. Se hai attivato un gateway per i volumi memorizzati nella cache, è inoltre necessario dimensionare lo storage della cache per carichi di lavoro reali.

Per dimensionare il buffer di caricamento e lo storage della cache per una configurazione nella cache del gateway

- Utilizza la formula illustrata nella [Determinazione delle dimensioni del buffer di caricamento da allocare](#) per dimensionare il buffer di caricamento. È consigliabile allocare almeno 150 GiB per il buffer di caricamento. Se la formula del buffer di caricamento restituisce un valore inferiore a 150 GiB, utilizzare 150 GiB come il buffer di caricamento allocato.

La formula del buffer di caricamento tiene conto della differenza tra la velocità effettiva dall'applicazione al gateway e la velocità effettiva dal gateway a AWS, moltiplicata per il tempo previsto di scrittura dei dati. Ad esempio, supponiamo che le applicazioni scrivano dati di testo 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 2:1 per i dati di testo, la formula specifica che è necessario allocare circa 675 GiB come spazio del buffer di caricamento.

Per dimensionare il buffer di caricamento per una configurazione memorizzata

- Utilizza la formula illustrata in [Determinazione delle dimensioni del buffer di caricamento da allocare](#). È consigliabile allocare almeno 150 GiB per il buffer di caricamento. Se la formula del buffer di caricamento restituisce un valore inferiore a 150 GiB, utilizzare 150 GiB come il buffer di caricamento allocato.

La formula del buffer di caricamento tiene conto della differenza tra la velocità effettiva dall'applicazione al gateway e la velocità effettiva dal gateway verso AWS, moltiplicata per il tempo previsto di scrittura dei dati. Ad esempio, supponiamo che le applicazioni scrivano dati di testo 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 2:1 per i dati di testo, la formula specifica che è necessario allocare circa 675 GiB come spazio del buffer di caricamento.

## Per monitorare il buffer di caricamento

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Scegliere la scheda Gateway, quindi Details (Dettagli), infine individuare il campo Upload Buffer Used (Buffer di caricamento utilizzato) per visualizzare il buffer di caricamento corrente del gateway.
3. Imposta uno o più allarmi per ricevere notifiche sull'uso del buffer di caricamento.

Ti consigliamo vivamente di creare uno o più allarmi del buffer di caricamento nella console Amazon CloudWatch . Ad esempio, è possibile impostare un allarme per il livello di utilizzo per cui si desidera ricevere avvisi e un allarme per un livello di utilizzo che, se superato, è motivo di intervento. L'intervento potrebbe essere aggiungere più spazio per il buffer di caricamento. Per ulteriori informazioni, consulta [Per impostare un allarme soglia superiore allarme per un buffer di caricamento del gateway](#).

## Eliminazione delle risorse non necessarie

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

### Per eliminare risorse non necessarie

1. Eliminare tutti gli snapshot. Per istruzioni, consulta [Eliminazione di uno snapshot](#).
2. Eliminare il gateway, a meno che non si preveda di continuare a utilizzarlo. Per ulteriori informazioni, consulta [Eliminazione del gateway e rimozione delle risorse associate](#).
3. Eliminare la macchina virtuale Storage Gateway dall'host on-premise. Se hai creato il gateway su un'EC2istanza Amazon, interrompi l'istanza.

## Backup dei volumi

Utilizzando Storage Gateway, puoi proteggere le tue applicazioni aziendali on-premise che utilizzano i volumi Storage Gateway per lo storage basato su cloud. Puoi eseguire il backup dei volumi Storage Gateway on-premise utilizzando la pianificazione nativa dello snapshot in Storage Gateway oppure AWS Backup. In entrambi i casi, i backup dei volumi Storage Gateway vengono archiviati come snapshot di Amazon EBS in Amazon Web Services.

## Argomenti

- [Utilizzo di Storage Gateway per il backup dei volumi](#)
- [Utilizzo AWS Backup per il backup dei volumi](#)

## Utilizzo di Storage Gateway per il backup dei volumi

Puoi utilizzare la console di gestione Storage Gateway per eseguire il backup dei volumi, effettuando degli snapshot Amazon EBS e memorizzando tali snapshot in Amazon Web Services. Puoi acquisire snapshot ad hoc una tantum oppure configurare una pianificazione degli snapshot gestita mediante Storage Gateway. Successivamente, puoi ripristinare lo snapshot per un nuovo volume utilizzando la console Storage Gateway. Per informazioni su come eseguire il backup e gestire il backup da Storage Gateway, consulta i seguenti argomenti:

- [Test del gateway](#)
- [Creazione di uno snapshot una tantum](#)
- [Clonazione di un volume](#)

## Utilizzo AWS Backup per il backup dei volumi

AWS Backup è un servizio di backup centralizzato che semplifica ed economico il backup dei dati delle applicazioni tra AWS servizi sia nel cloud di Amazon Web Services che in locale. In questo modo puoi soddisfare i requisiti di conformità in materia di backup aziendali e normativi. AWS Backup semplifica la protezione dei volumi di AWS storage, dei database e dei file system fornendo una posizione centrale in cui è possibile eseguire le seguenti operazioni:

- Configura e controlla le AWS risorse di cui desideri eseguire il backup.
- Automatizzare la pianificazione dei backup.
- Impostare le policy di conservazione.
- Monitorare tutte le attività recenti di backup e ripristino.

Poiché Storage Gateway si integra con AWS Backup, consente ai clienti di eseguire il backup di applicazioni aziendali locali che utilizzano volumi Storage Gateway per lo storage basato sul cloud. AWS Backup supporta il backup e il ripristino di volumi memorizzati e memorizzati nella cache. Per informazioni in merito AWS Backup, consulta la AWS Backup documentazione. Per informazioni su AWS Backup, consulta [What is AWS Backup?](#) nella Guida AWS Backup per l'utente.

È possibile gestire le operazioni di backup e ripristino dei volumi di Storage Gateway evitando la necessità di creare script personalizzati o gestire manualmente i backup. AWS Backup point-in-time Con AWS Backup, puoi anche monitorare i backup dei volumi locali insieme alle risorse nel cloud da un'unica dashboard. AWS Backup Puoi utilizzarlo AWS Backup per creare un backup on-demand o definire un piano di backup da gestire in AWS Backup

I backup dei volumi di Storage Gateway presi da AWS Backup sono archiviati in Amazon S3 come snapshot di Amazon EBS. Puoi visualizzare i backup del volume Storage Gateway dalla AWS Backup console o dalla console Amazon EBS.

È possibile ripristinare facilmente i volumi di Storage Gateway gestiti tramite AWS Backup qualsiasi gateway locale o gateway nel cloud. Puoi inoltre ripristinare tale volume su un volume che puoi utilizzare con istanze Amazon EC2.

### Vantaggi dell'utilizzo AWS Backup per il backup dei volumi dello Storage Gateway

I vantaggi dell'utilizzo AWS Backup per il backup dei volumi di Storage Gateway sono la possibilità di soddisfare i requisiti di conformità, evitare oneri operativi e centralizzare la gestione dei backup. AWS Backup consente di effettuare le seguenti operazioni:

- Impostare policy di backup pianificate personalizzabili che soddisfino i tuoi requisiti di backup.
- Imposta le regole di conservazione e scadenza dei backup in modo da non dover più sviluppare script personalizzati o gestire manualmente i point-in-time backup dei volumi.
- Gestisci e monitora i backup su più gateway e altre AWS risorse da una vista centrale.

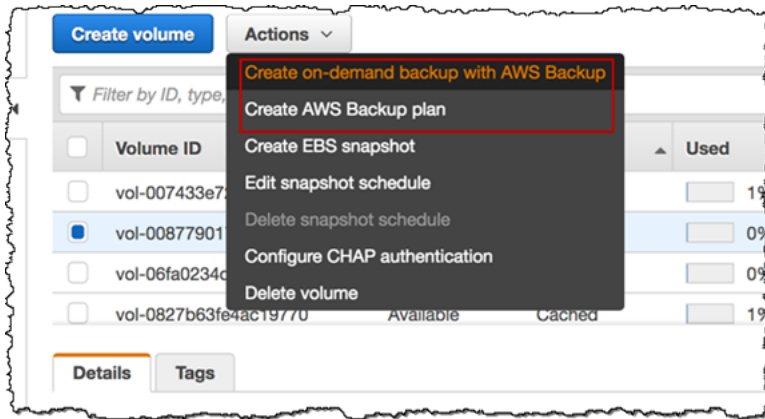
Da utilizzare AWS Backup per creare backup dei volumi

#### Note

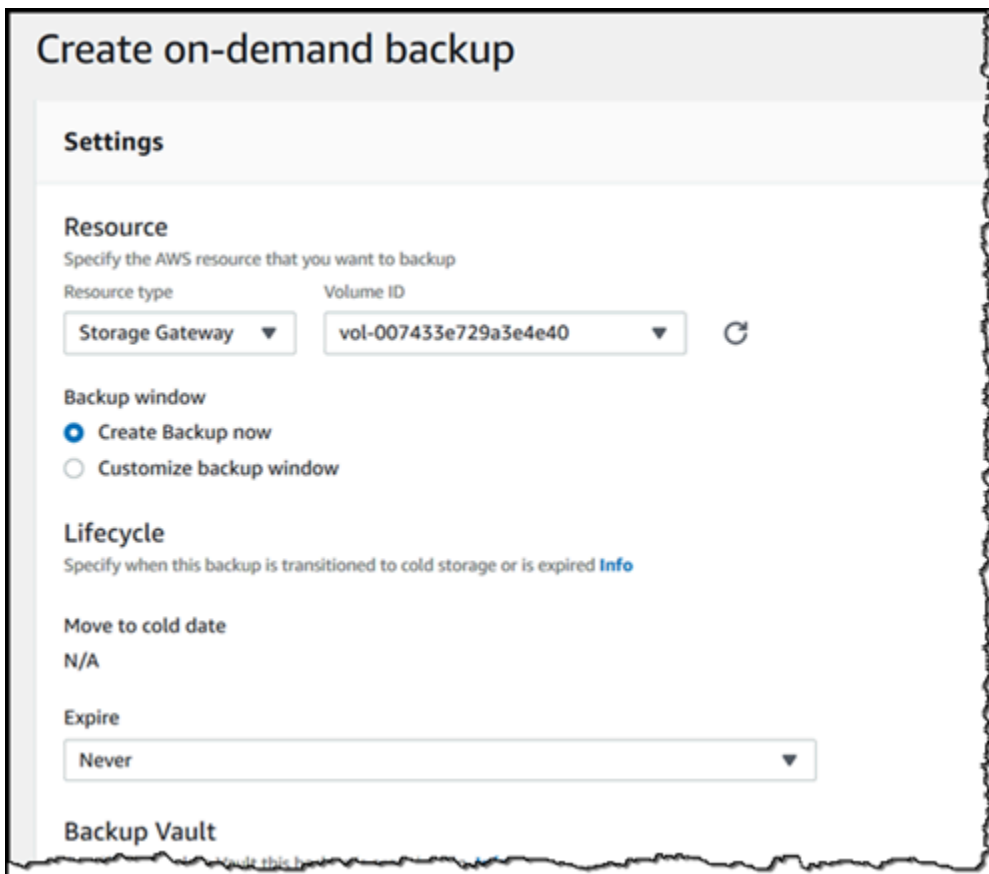
AWS Backup richiede la scelta di un ruolo AWS Identity and Access Management (IAM) che utilizzi AWS Backup . Devi creare questo ruolo perché AWS Backup non lo crea per te. È inoltre necessario creare una relazione di fiducia tra AWS Backup e questo ruolo IAM. Per ulteriori informazioni su come farlo, consulta la AWS Backup Guida per l'utente . Per informazioni su come eseguire questa operazione, consulta [Creazione un piano di backup](#) nella AWS Backup Guida per l'utente .

1. Apri la console Storage Gateway e seleziona Volumes (Volumi) nel riquadro di navigazione di sinistra.

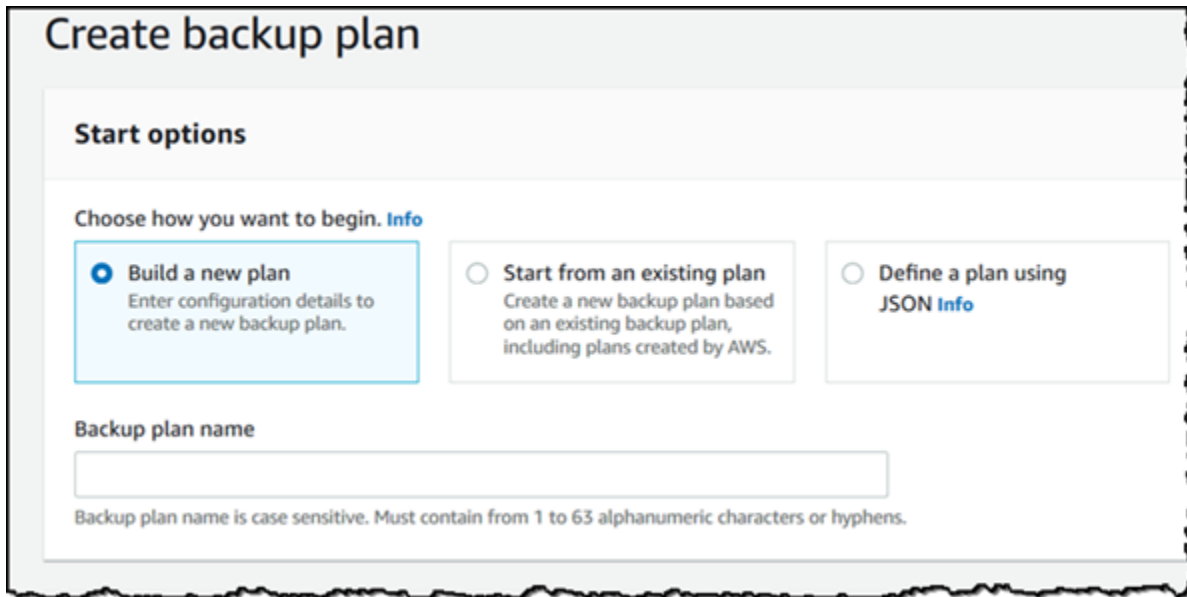
2. Per Azioni, scegli Crea backup su richiesta con AWS Backup o Crea piano AWS di backup.



Se desideri creare un backup su richiesta del volume Storage Gateway, scegli Crea backup su richiesta con. AWS Backup La console è diretta all' AWS Backup utente.



Se desideri creare un nuovo AWS Backup piano, scegli Crea piano di AWS backup. Verrai indirizzato alla AWS Backup console.



**Create backup plan**

**Start options**

Choose how you want to begin. [Info](#)

**Build a new plan**  
Enter configuration details to create a new backup plan.

**Start from an existing plan**  
Create a new backup plan based on an existing backup plan, including plans created by AWS.

**Define a plan using JSON** [Info](#)

**Backup plan name**

Backup plan name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

Sulla AWS Backup console, è possibile creare un piano di backup, assegnare un volume Storage Gateway al piano di backup e creare un backup. Puoi inoltre eseguire attività di gestione del backup in corso.

## Ricerca e ripristino di volumi da AWS Backup

È possibile trovare e ripristinare i volumi dello Storage Gateway di backup dalla AWS Backup console. Per ulteriori informazioni, consulta la AWS Backup Guida per l'utente. Per ulteriori informazioni, consulta [Punti di ripristino](#) nella AWS Backup Guida per l'utente .

Per trovare e ripristinare i volumi

1. Apri la AWS Backup console e trova il backup del volume Storage Gateway che desideri ripristinare. Puoi ripristinare il backup del volume Storage Gateway su un volume Amazon EBS o su un volume Storage Gateway. Seleziona l'opzione appropriata in base alle tue necessità di ripristino.
2. In Restore type (Tipo di ripristino), seleziona un volume memorizzato o un volume Storage Gateway nella cache e inserisci le informazioni richieste:
  - Per un volume memorizzato, fornisci le informazioni relative a Gateway name (Nome gateway), Disk ID (ID disco) e iSCSI target name (Nome destinazione iSCSI).

## Restore backup

### Settings

Snapshot ID  
snap-068e1ef065c6f2704

Resource type  
Specify the type of AWS resource to create when restoring this backup

- EBS volume  
 Storage Gateway volume

Gateway

temp .....

iSCSI target name

1 to 200 characters including a-z, 0-9, and "-;"

- Per un volume nella cache, fornisci le informazioni relative a Gateway name (Nome gateway), Capacity (Capacità) e iSCSI target name (Nome destinazione iSCSI).

## Restore backup

### Settings

Snapshot ID  
snap-068e1ef065c6f2704

Resource type  
Specify the type of AWS resource to create when restoring this backup

- EBS volume  
 Storage Gateway volume

Gateway

v-thinstaller-centos-1

Capacity

TiB

iSCSI target name

1 to 200 characters including a-z, 0-9, and "-;"

### 3. Scegli Restore resource (Ripristina risorsa) per ripristinare il volume.

#### Note

Non puoi utilizzare la console Amazon EBS per eliminare uno snapshot creato da AWS Backup

## 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 i dati ai servizi di AWS archiviazione senza comunicare sulla rete Internet pubblica. Utilizzando il VPC servizio Amazon, puoi avviare AWS risorse, inclusi endpoint di interfaccia di rete privata, in un cloud privato virtuale personalizzato (VPC). A ti VPC consente di controllare le impostazioni di rete come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni su VPCs, consulta [What is AmazonVPC?](#) nella Amazon VPC User Guide.

Per attivare il gateway in aVPC, utilizza la VPC console Amazon per creare un VPC endpoint per Storage Gateway e ottenere l'ID dell'VPC endpoint, quindi specifica questo ID VPC endpoint quando crei e attivi il gateway. Per ulteriori informazioni, consulta [Connect your Volume Gateway a AWS](#).

#### Note

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

### Argomenti

- [Creazione di un VPC endpoint per Storage Gateway](#)

## Creazione di un VPC endpoint per Storage Gateway

Segui queste istruzioni per creare un VPC endpoint. Se disponi già di un VPC endpoint per Storage Gateway, puoi utilizzarlo per attivare il gateway.



## Per creare un VPC endpoint per Storage Gateway

1. Accedi a AWS Management Console e apri la VPC console Amazon 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. Infatti VPC, scegli le tue zone di disponibilità VPC e prendi nota delle relative zone di disponibilità e sottoreti.
6. Verifica che l'opzione Abilita DNS nome privato non sia selezionata.
7. Per Gruppo di sicurezza, scegli il gruppo di sicurezza che desideri utilizzare per il tuo VPC. È possibile accettare il gruppo di sicurezza predefinito. Verifica che tutte le seguenti TCP porte siano consentite nel tuo gruppo di sicurezza:
  - TCP443
  - TCP1026
  - TCP1027
  - TCP1028
  - TCP1031
  - TCP2222
8. Seleziona Crea endpoint. Lo stato iniziale dell'endpoint è pending (in sospeso). Quando viene creato l'endpoint, annota l'ID dell'VPC endpoint che hai appena creato.
9. Quando l'endpoint viene creato, scegli Endpoints, quindi scegli il nuovo endpoint. VPC
10. Nella scheda Dettagli dell'endpoint del gateway di storage selezionato, in DNS Nomi, utilizza il primo DNS nome che non specifica una zona di disponibilità. Il tuo DNS nome è simile al seguente: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ora che hai un VPC endpoint, puoi creare il tuo 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 [Iniziare con AWS Storage Gateway](#).

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 (ad esempio strumenti SSM Hypervisor) diversi dal normale meccanismo di aggiornamento del gateway può compromettere il corretto funzionamento del Gateway.

## Argomenti

- [Gestione del gateway di volumi](#)
- [Spostamento dei dati su un nuovo gateway](#)

# Gestione del gateway di volumi

Di seguito trovi le informazioni su come gestire le risorse del gateway di volumi.

I volumi memorizzati nella cache sono volumi in Amazon Simple Storage Service (Amazon S3) che sono esposti come SCSI destinazioni i su cui è possibile archiviare i dati delle applicazioni. Di seguito trovi le informazioni su come aggiungere ed eliminare volumi per la configurazione nella cache. Puoi anche scoprire come aggiungere e rimuovere volumi Amazon Elastic Block Store (AmazonEBS) nei EC2 gateway Amazon.

## Argomenti

- [Modifica delle informazioni di base sul gateway](#)
- [Aggiunta di un volume](#)
- [Espansione delle dimensioni di un volume](#)

- [Clonazione di un volume](#)
- [Visualizzazione dell'utilizzo del volume](#)
- [Riduzione dell'importo addebitato per lo storage in un volume](#)
- [Eliminazione di un volume](#)
- [Spostamento dei volumi su un gateway differente](#)
- [Creazione di uno snapshot una tantum](#)
- [Modifica di una pianificazione degli snapshot](#)
- [Eliminazione di uno snapshot](#)
- [Informazioni su stati e transizioni dei volumi](#)

#### Important

Se un volume nella cache conserva i dati primari in Amazon S3, devi evitare processi di lettura o scrittura di tutti i dati nell'intero volume. Ad esempio, sconsigliamo di usare un software antivirus che analizza l'intero volume nella cache. Analisi di questo tipo, se eseguite on demand o in base a una pianificazione, comportano il download in locale di tutti i dati archiviati in Amazon S3 per l'analisi, provocando un utilizzo elevato della larghezza di banda. Invece di eseguire un'analisi completa del disco, puoi usare l'analisi antivirus in tempo reale, ovvero l'analisi dei dati man mano che vengono letti o scritti nel volume nella cache.

Il ridimensionamento di un volume non è supportato. Per modificare le dimensioni di un volume, crea uno snapshot del volume e quindi crea un nuovo volume nella cache dallo snapshot. Il nuovo volume può avere dimensioni maggiori del volume da cui è stato creato lo snapshot. Per istruzioni su come rimuovere un volume, consulta [Per eliminare un volume](#). Per istruzioni su come aggiungere un volume e conservare i dati esistenti, consulta [Eliminazione di un volume](#).

Tutti i dati del volume e i dati delle istantanee memorizzati nella cache vengono archiviati in Amazon S3 e crittografati a riposo utilizzando la crittografia lato server (SSE). Tuttavia, non puoi accedere a questi dati utilizzando Amazon S3 API o altri strumenti come la console di gestione Amazon S3.

## 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 a <https://console.aws.amazon.com/storagegateway/casa>.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le informazioni di base.
3. Dal menu a discesa Operazioni, scegli Modifica le informazioni sul gateway.
4. Modificare l'impostazione desiderata, quindi selezionare Salva.

#### Note

La modifica del nome di un gateway disconnetterà tutti gli CloudWatch allarmi impostati per monitorare il gateway. Per ricollegare gli allarmi, aggiorna il file GatewayName per ogni allarme nella console. CloudWatch

## Aggiunta di un volume

Con l'aumentare delle esigenze dell'applicazione, potresti dover aggiungere altri volumi al gateway. Aggiungendo altri volumi, devi tenere conto delle dimensioni dello storage della cache e del buffer di caricamento allocati al gateway. Il gateway deve avere spazio del buffer e della cache sufficiente per i nuovi volumi. Per ulteriori informazioni, consulta [Determinazione delle dimensioni del buffer di caricamento da allocare](#).

È possibile aggiungere volumi utilizzando la console Storage Gateway o l'API Storage Gateway. Per informazioni sull'utilizzo dell'API Storage Gateway per aggiungere volumi, vedere [CreateCachediscsiVolume](#). Per istruzioni su come aggiungere un volume tramite la console Storage Gateway, consulta [Creazione di un volume](#).

## Espansione delle dimensioni di un volume

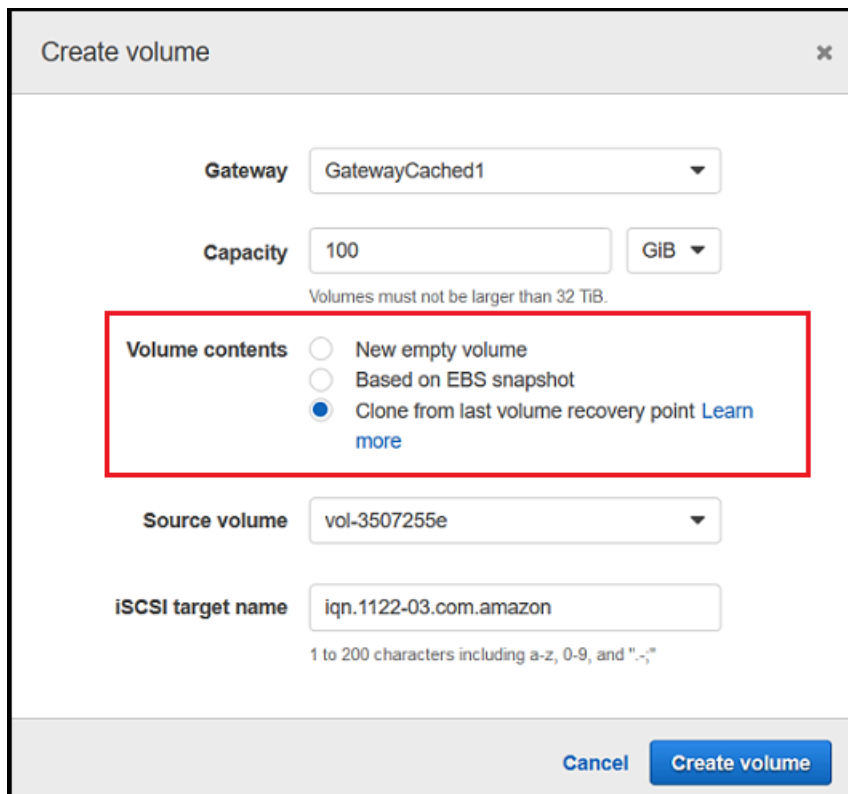
Con l'aumentare delle esigenze dell'applicazione, potresti dover espandere il volume invece di aggiungere altri volumi al gateway. In questo caso, puoi:

- Creare uno snapshot del volume che vuoi espandere e quindi usare questo snapshot per creare un nuovo volume di dimensioni maggiori. Per informazioni su come creare uno snapshot, consulta [Creazione di uno snapshot una tantum](#). Per informazioni su come usare uno snapshot per creare un nuovo volume, consulta [Creazione di un volume](#).

- Usare il volume nella cache che vuoi espandere per clonare un nuovo volume di dimensioni maggiori. Per informazioni su come clonare un volume, consulta [Clonazione di un volume](#). Per informazioni su come creare un volume, consulta [Creazione di un volume](#).

## Clonazione di un volume

È possibile creare un nuovo volume da qualsiasi volume memorizzato nella cache esistente nella stessa AWS regione. Il nuovo volume viene creato dal punto di ripristino più recente del volume selezionato. Un punto di ripristino del volume è un punto temporale in cui tutti i dati del volume sono coerenti. Per clonare un volume, devi scegliere l'opzione Clone from last recovery point (Clona da ultimo punto di ripristino) nella finestra di dialogo Create volume (Crea volume) e quindi selezionare il volume da usare come origine. Lo screenshot seguente mostra la finestra di dialogo Create volume (Crea volume).



The screenshot shows the 'Create volume' dialog box with the following fields and options:

- Gateway:** GatewayCached1
- Capacity:** 100 GIB
- Volume contents:**  New empty volume,  Based on EBS snapshot,  Clone from last volume recovery point [Learn more](#)
- Source volume:** vol-3507255e
- iSCSI target name:** iqn.1122-03.com.amazon

Buttons: Cancel, Create volume

La clonazione da un volume esistente è più rapida ed economica rispetto alla creazione di uno snapshot Amazon EBS. La clonazione esegue una byte-to-byte copia dei dati dal volume di origine al nuovo volume, utilizzando il punto di ripristino più recente dal volume di origine. Storage Gateway crea automaticamente punti di ripristino per i volumi nella cache. Per vedere quando è stato creato l'ultimo punto di ripristino, controlla la `TimeSinceLastRecoveryPoint` metrica in Amazon CloudWatch.

Il volume clonato è indipendente dal volume di origine. Questo significa che le modifiche apportate a uno dei due volumi dopo la clonazione non hanno effetto sull'altro. Ad esempio, se elimini il volume di origine, l'eliminazione non ha effetto sul volume clonato. Puoi clonare un volume di origine mentre sono presenti iniziatori connessi e attivamente in uso. In questo caso, non vi sarà alcun effetto sulle prestazioni del volume di origine. Per informazioni su come clonare un volume, consulta [Creazione di un volume](#).

Puoi usare il processo di clonazione anche in scenari di ripristino. Per ulteriori informazioni, consulta [Il gateway nella cache è irraggiungibile e occorre recuperare i dati](#).

## Clonazione da un punto di ripristino del volume

La procedura seguente mostra come clonare un volume da un punto di ripristino del volume e usare tale volume.

Per clonare e usare un volume da un gateway non raggiungibile

1. Aprire la console Storage Gateway all'[indirizzo https://console.aws.amazon.com/storagegateway/home](https://console.aws.amazon.com/storagegateway/home).
2. Nella console Storage Gateway selezionare Create volume (Crea volume).
3. Nella finestra di dialogo Create volume (Crea volume) scegliere un gateway in Gateway.
4. Per Capacity (Capacità), digitare la capacità per il volume. La capacità deve avere almeno le stesse dimensioni del volume di origine.
5. Scegliere Clone from last recovery point (Clona da ultimo punto di ripristino) e selezionare un ID volume per Source volume (Volume di origine). Il volume di origine può essere qualsiasi volume memorizzato nella cache nella regione selezionata AWS .

The screenshot shows the 'Create volume' dialog box with the following fields and options:

- Gateway:** GatewayCached1
- Capacity:** 100 GIB
- Volume contents:**
  - New empty volume
  - Based on EBS snapshot
  - Clone from last volume recovery point [Learn more](#)
- Source volume:** vol-3507255e
- iSCSI target name:** iqn.1122-03.com.amazon

Buttons at the bottom: Cancel, Create volume

- Digitare un nome per iSCSI target name (Nome destinazione iSCSI).

Il nome della destinazione può includere lettere minuscole, numeri, punti (.) e trattini (-) e Viene visualizzato come nome di iSCSI target node (Nodo destinazione iSCSI) nella scheda Targets (Destinazioni) dell'interfaccia utente iSCSI Microsoft initiator (Iniziatore Microsoft iSCSI), dopo l'individuazione. Ad esempio, il nome target1 viene visualizzato come iqn.1007-05.com.amazon:target1. Assicurarsi che il nome della destinazione sia univoco a livello globale all'interno della rete SAN (Storage Area Network).

- Verificare che l'impostazione Network interface (Interfaccia di rete) corrisponda all'indirizzo IP del gateway oppure scegliere un indirizzo IP per Network interface (Interfaccia di rete).

Se il gateway è stato configurato per l'uso di più schede di rete, scegliere l'indirizzo IP usato dalle applicazioni di storage per accedere al volume. Ogni scheda di rete definita per un gateway rappresenta un indirizzo IP che è possibile scegliere.

Se la macchina virtuale del gateway è configurata per più di una scheda di rete, la finestra di dialogo Create volume (Crea volume) visualizza un elenco per Network interface (Interfaccia di rete). Nell'elenco è incluso un indirizzo IP per ogni scheda di rete configurata per la macchina virtuale del gateway. Se la macchina virtuale del gateway è configurata per una sola scheda di rete, non viene visualizzato alcun elenco, perché è presente un solo indirizzo IP.

8. Selezionare **Create volume (Crea volume)**. Viene visualizzata la finestra di dialogo **Configure CHAP Authentication (Configura autenticazione CHAP)**. È possibile configurare CHAP più avanti. Per informazioni, consulta [Configurazione dell'CHAP autenticazione per i tuoi obiettivi i SCSI](#).

La fase successiva consiste nella connessione del volume al client. Per ulteriori informazioni, consulta [Collegamento dei volumi al tuo client](#).

## Creazione di uno snapshot di ripristino

La procedura seguente mostra come creare uno snapshot da un punto di ripristino del volume e come usare tale snapshot. Puoi acquisire snapshot ad hoc una tantum oppure configurare una pianificazione degli snapshot per il volume.

Per creare e usare uno snapshot di ripristino di un volume da un gateway non raggiungibile

1. Aprire la console Storage Gateway all'[indirizzo https://console.aws.amazon.com/storagegateway/home](https://console.aws.amazon.com/storagegateway/home).
2. Nel riquadro di navigazione, scegliere **Gateways**.
3. Scegliere il gateway non raggiungibile e quindi scegliere la scheda **Details (Dettagli)**.

Nella scheda viene visualizzato un messaggio relativo allo snapshot di ripristino.



4. Scegliere **Create recovery snapshot (Crea snapshot di ripristino)** per aprire la finestra di dialogo **Create recovery snapshot (Crea snapshot di ripristino)**.
5. Nell'elenco dei volumi visualizzati scegliere il volume da ripristinare e quindi scegliere **Create snapshots (Crea snapshot)**.

Storage Gateway avvia il processo di snapshot.

6. Trovare e ripristinare lo snapshot.



## Visualizzazione dell'utilizzo del volume

Se scrivi dati in un volume, puoi visualizzare la quantità di dati archiviati nel volume nella Console di gestione Storage Gateway. La scheda Details (Dettagli) per ogni volume mostra informazioni sull'utilizzo del volume.

Per visualizzare la quantità di dati scritti in un volume

1. Apri la console Storage Gateway all'indirizzo <https://console.aws.amazon.com/storagegateway/home>.
2. Nel riquadro di navigazione scegliere Volumes (Volumi) e quindi il volume desiderato.
3. Seleziona la scheda Details (Dettagli).

I campi seguenti forniscono informazioni sul volume:

- Size (Dimensioni): capacità totale del volume selezionato.
- Used (In uso): dimensioni dei dati archiviati nel volume.

### Note

Questi valori non sono disponibili per i volumi creati prima del 13 maggio 2015, finché i dati non vengono archiviati nel volume.

## Riduzione dell'importo addebitato per lo storage in un volume

L'eliminazione di file dal file system non comporta necessariamente l'eliminazione dei dati dal dispositivo a blocchi sottostante né riduce la quantità di dati archiviati nel volume. Se vuoi ridurre l'importo addebitato per l'archiviazione nel volume, ti consigliamo di sovrascrivere i file con elementi di dimensioni pari a zero per comprimere l'archiviazione a una quantità minima di archiviazione effettiva. Storage Gateway addebita i costi per l'utilizzo del volume in base all'archiviazione compressa.

### Note

Se usi uno strumento di eliminazione che sovrascrive i dati nel volume con dati casuali, l'utilizzo non verrà ridotto. Il motivo è che i dati casuali non sono comprimibili.

## Eliminazione di un volume

Con il mutare delle esigenze dell'applicazione, potresti dover eliminare un volume, ad esempio se esegui la migrazione dell'applicazione per usare un volume di archiviazione di dimensioni maggiori. Prima di eliminare un volume, assicurati che nessuna applicazione stia attualmente scrivendo nel volume. Assicurati inoltre che non vi siano snapshot in corso per il volume. Se per il volume è definita una pianificazione degli snapshot, puoi controllarla nella scheda Pianificazioni snapshot della console Storage Gateway. Per ulteriori informazioni, consulta [Modifica di una pianificazione degli snapshot](#).

È possibile eliminare i volumi utilizzando la console Storage Gateway o lo Storage GatewayAPI. Per informazioni sull'utilizzo dello Storage Gateway API per rimuovere i volumi, vedere [Delete Volume](#). La procedura seguente descrive l'uso della console.

Prima di eliminare un volume, esegui il backup dei dati o acquisisci uno snapshot dei dati critici. Per i volumi archiviati, i dischi locali non vengono cancellati. Dopo aver eliminato un volume, non potrai più recuperarlo.

Per eliminare un volume

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Scegli Volumi, quindi seleziona uno o più volumi da eliminare.
3. In Operazioni, scegliere Elimina volume. Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler eliminare i volumi specificati, quindi digita la parola elimina nella casella di conferma e scegli Elimina.

## Spostamento dei volumi su un gateway differente

Se i tuoi dati e le tue esigenze prestazionali crescono, puoi spostare i volumi su un gateway di volumi differente. Per farlo, puoi scollegare e collegare un volume utilizzando la console Storage Gateway o l'API.

Per scollegare e collegare un volume, puoi effettuare le seguenti operazioni:

- Sposta i volumi su piattaforme di hosting migliori o su nuove istanze Amazon EC2.
- Aggiorna l'hardware utilizzato per il tuo server.
- Sposta i volumi tra vari tipi di hypervisor.

Quando scolleghi un volume, il gateway carica e archivia i dati e i metadati del volume sul servizio Storage Gateway in AWS. Puoi collegare facilmente un volume separato a un gateway su qualsiasi piattaforma host supportata in una fase successiva.

#### Note

Un volume scollegato viene conteggiato in base alla tariffa standard di storage del volume fino a quando non viene eliminato. Per informazioni su come ridurre i costi, consulta [Riduzione dell'importo addebitato per lo storage in un volume](#).

#### Note


Ci sono alcune limitazioni di collegamento e scollegamento dei volumi:

- Lo scollegamento di un volume può richiedere molto tempo. Quando si scollega un volume, il gateway carica tutti i dati sul volume AWS prima che il volume venga scollegato. Il tempo necessario per completare il caricamento dipende dalla quantità di dati che devono essere caricati e dalla tua connessione di rete in AWS.
- Se scolleghi un volume nella cache, non potrai ricollegarlo come volume memorizzato.
- Se scolleghi un volume memorizzato, non potrai ricollegarlo come volume nella cache.
- Un volume scollegato non può essere utilizzato finché non è associato a un gateway.
- Quando colleghi un volume memorizzato, devi ripristinarlo completamente prima di collegarlo a un gateway.
- Quando colleghi o scolleghi un volume, devi attendere che l'operazione sia completata prima di utilizzare il volume.
- Attualmente, l'eliminazione forzata di un volume è supportata solo mediante API.
- Se cancelli un gateway mentre il volume viene scollegato da tale gateway, si verificherà una perdita di dati. Attendi il completamento dell'operazione di scollegamento del volume prima di eliminare il gateway.
- Se un gateway memorizzato è in stato di ripristino, non potrai scollegare un volume da esso.

La procedura seguente mostra come scollegare e collegare un volume utilizzando la console Storage Gateway. Per ulteriori informazioni su come eseguire questa operazione utilizzando l'API, consulta [DetachVolume](#) o [AttachVolume](#) nell'API Reference.AWS Storage Gateway

Scollegare un volume da un gateway

1. Aprire la console Storage Gateway all'[indirizzo https://console.aws.amazon.com/storagegateway/home](https://console.aws.amazon.com/storagegateway/home).
2. Scegli Volumes, quindi seleziona uno o più volumi da scollegare.
3. In Actions (Operazioni), seleziona Detach Volume (Scollega volume). Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler scollegare i volumi specificati, quindi digita la parola distacca nella casella di conferma e scegli Scollega.

 Note

Se un volume che viene scollegato dispone di una notevole quantità di dati, esso passa dallo stato Attached (Collegato) a Detaching (Scollegamento in corso) fino a quando non viene completato il caricamento di tutti i dati. Successivamente lo stato passerà a Detached (Scollegato). Per piccole quantità di dati, potresti non visualizzare affatto lo stato Detaching (Scollegamento in corso). Se il volume non dispone di dati, lo stato passa da Attached (Collegato) a Detached (Scollegato).

Ora puoi collegare il volume a un altro gateway.

Per collegare un volume a un gateway

1. Aprire la console Storage Gateway all'[indirizzo https://console.aws.amazon.com/storagegateway/home](https://console.aws.amazon.com/storagegateway/home).
2. Nel riquadro di navigazione, seleziona Volumes (Volumi). Lo stato di ogni volume scollegato sarà Detached (Scollegato).
3. Dall'elenco dei volumi scollegati, seleziona il volume che desideri collegare. Puoi collegare soltanto un volume per volta.
4. In Actions (Operazioni), seleziona Attach Volume (Collega volume).
5. Nella finestra di dialogo Attach Volume (Collega volume), seleziona il gateway al quale desideri collegare il volume e quindi immetti la destinazione iSCSI alla quale collegare il volume.

Se colleghi un volume memorizzato, immetti l'identificatore del disco per Disk ID (ID disco).

6. Scegli Attach volume (Collega volume). Se un volume collegato dispone di una notevole quantità di dati, il suo stato passerà da Detached (Scollegato) a Attached (Collegato) se l'operazione AttachVolume va a buon fine.
7. Nella procedura guidata di autenticazione Configure CHAP (Configura CHAP), inserisci Initiator name (Nome iniziatore), Initiator secret (Segreto iniziatore) e Target secret (Segreto destinazione), quindi seleziona Save (Salva). Per ulteriori informazioni sull'utilizzo dell'autenticazione "Challenge-Handshake Authentication Protocol (CHAP)", consulta [Configurazione dell'CHAP autenticazione per i tuoi obiettivi i SCSI](#).

## Creazione di uno snapshot una tantum

Oltre agli snapshot pianificati, per i gateway di volumi puoi acquisire snapshot ad hoc una tantum. In questo modo, puoi eseguire il backup del volume di storage immediatamente, senza attendere il successivo snapshot pianificato.

Per acquisire uno snapshot una tantum del volume di storage

1. Aprire la console Storage Gateway all'[indirizzo https://console.aws.amazon.com/storagegateway/home](https://console.aws.amazon.com/storagegateway/home).
2. Nel riquadro di navigazione scegliere Volumes (Volumi) e quindi selezionare il volume da cui si vuole creare la snapshot.
3. In Actions (Operazioni), scegli Create snapshot (Crea snapshot).
4. Nella finestra di dialogo Create Snapshot (Crea snapshot) digitare una descrizione della snapshot e quindi scegliere Create Snapshot (Crea snapshot).

Per verificare che lo snapshot sia stato creato, è possibile usare la console.

La snapshot è elencata in Snapshots (Snapshot), nella stessa riga del volume.

## Modifica di una pianificazione degli snapshot

Per i volumi archiviati, AWS Storage Gateway crea una pianificazione istantanea predefinita di una volta al giorno.

### Note

Non puoi rimuovere la pianificazione predefinita degli snapshot. I volumi archiviati richiedono almeno una pianificazione degli snapshot. Tuttavia, puoi modificare una pianificazione degli snapshot specificando le ore in cui acquisire lo snapshot ogni giorno o la frequenza (ogni 1, 3, 4, 8, 12 o 24 ore) oppure entrambe.

Per i volumi memorizzati nella cache, AWS Storage Gateway non crea una pianificazione di snapshot predefinita. Non viene creata alcuna pianificazione predefinita perché i dati sono archiviati in Amazon S3 e di conseguenza non sono necessari snapshot o una pianificazione degli snapshot per scopi di ripristino di emergenza. Se necessario, tuttavia, puoi configurare una pianificazione degli snapshot in qualsiasi momento. La creazione di snapshot per il volume nella cache offre un ulteriore metodo per ripristinare i dati, se necessario.

Tramite la procedura seguente, puoi modificare la pianificazione degli snapshot per un volume.

Per modificare la pianificazione degli snapshot per un volume

1. Apri la console Storage Gateway all'indirizzo <https://console.aws.amazon.com/storagegateway/home>.
2. Nel riquadro di navigazione scegliere Volumes (Volumi) e quindi selezionare il volume da cui è stata creata la snapshot.
3. In Actions (Operazioni) scegliere Edit snapshot schedule (Modifica pianificazione snapshot).
4. Nella finestra di dialogo Edit snapshot schedule (Modifica pianificazione snapshot) modificare la pianificazione e quindi scegliere Save (Salva).

## Eliminazione di uno snapshot

Puoi eliminare uno snapshot del volume di storage. Ad esempio, potresti doverlo fare se hai acquisito molti snapshot di un volume di storage nel tempo e quelli meno recenti non ti servono più. Poiché gli snapshot sono backup incrementali, se ne elimini uno, verranno eliminati solo i dati che non sono necessari negli altri snapshot.

### Argomenti

- [Eliminazione di snapshot tramite l'SDK AWS per Java](#)
- [Eliminazione di snapshot tramite l'SDK AWS per .NET](#)

- [Eliminazione di snapshot tramite AWS Tools for Windows PowerShell](#)

Nella console Amazon EBS puoi eliminare uno snapshot per volta. Per informazioni su come eliminare snapshot tramite la console Amazon EBS, consulta [Eliminazione di uno snapshot Amazon EBS](#) nella Guida per l'utente di Amazon EC2.

Per eliminare più istantanee alla volta, puoi utilizzare uno degli AWS SDK che supportano le operazioni di Storage Gateway. Per alcuni esempi, consulta [Eliminazione di snapshot tramite l'SDK AWS per Java](#), [Eliminazione di snapshot tramite l'SDK AWS per .NET](#) e [Eliminazione di snapshot tramite AWS Tools for Windows PowerShell](#).

## Eliminazione di snapshot tramite l'SDK AWS per Java

Per eliminare molti snapshot associati a un volume, puoi usare un approccio programmatico. L'esempio seguente descrive come eliminare snapshot tramite l'SDK AWS per 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 dell'SDK AWS per Java. Se devi eliminare solo pochi snapshot, usa la console, come descritto in [Eliminazione di uno snapshot](#).

Example : eliminazione di istantanee utilizzando l' AWS SDK for Java

L'esempio di codice Java seguente elenca gli snapshot per ogni volume di un gateway e indica se la data di inizio dello snapshot è precedente o successiva a una data specificata. Utilizza l'API AWS SDK for Java per Storage Gateway e Amazon EC2. L'API di Amazon EC2 include operazioni per l'uso di snapshot.

Aggiorna il codice per fornire l'endpoint del servizio, il nome della risorsa Amazon (ARN) del gateway e il numero di giorni precedenti per cui vuoi salvare gli snapshot. Verranno eliminati gli snapshot acquisiti prima di questo limite. Potresti anche dover specificare il valore booleano `viewOnly`, che indica se vuoi visualizzare gli snapshot da eliminare o eseguire effettivamente le eliminazioni degli snapshot. Prima di tutto, esegui il codice solo con l'opzione di visualizzazione, ovvero con `viewOnly` impostato su `true`, per visualizzare gli snapshot eliminati dal codice. 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 java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
```

```
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
the daysBack criteria
    public static boolean viewOnly = true;

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

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);
```



```
    ec2Client = new AmazonEC2Client(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
    ec2Client.setEndpoint(serviceURLEC2);

    List<VolumeInfo> volumes = ListVolumesForGateway();
    DeleteSnapshotsForVolumes(volumes, daysBack);

}
public static List<VolumeInfo> ListVolumesForGateway()
{
    List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

    String marker = null;
    do {
        ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
        ListVolumesResult result = sgClient.listVolumes(request);
        marker = result.getMarker();

        for (VolumeInfo vi : result.getVolumeInfos())
        {
            volumes.add(vi);
            System.out.println(OutputVolumeInfo(vi));
        }
    } while (marker != null);

    return volumes;
}
private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
    int daysBack2) {

    // Find snapshots and delete for each volume
    for (VolumeInfo vi : volumes) {

        String volumeARN = vi.getVolumeARN();
        String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
        Collection<Filter> filters = new ArrayList<Filter>();
        Filter filter = new Filter().withName("volume-id").withValues(volumeId);
        filters.add(filter);

        DescribeSnapshotsRequest describeSnapshotsRequest =
            new DescribeSnapshotsRequest().withFilters(filters);
```

```

DescribeSnapshotsResult describeSnapshotsResult =
    ec2Client.describeSnapshots(describeSnapshotsRequest);

List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
System.out.println("volume-id = " + volumeId);
for (Snapshot s : snapshots){
    StringBuilder sb = new StringBuilder();
    boolean meetsCriteria = !CompareDates(daysBack, s.getStartTimestamp());
    sb.append(s.getId() + ", " + s.getStartTimestamp().toString());

    sb.append(", meets criteria for delete? " + meetsCriteria);
    sb.append(", deleted? ");
    if (!viewOnly & meetsCriteria) {
        sb.append("yes");
        DeleteSnapshotRequest deleteSnapshotRequest =
            new DeleteSnapshotRequest().withSnapshotId(s.getId());
        ec2Client.deleteSnapshot(deleteSnapshotRequest);
    }
    else {
        sb.append("no");
    }
    System.out.println(sb.toString());
}
}

private static String OutputVolumeInfo(VolumeInfo vi) {

    String volumeInfo = String.format(
        "Volume Info:\n" +
        "  ARN: %s\n" +
        "  Type: %s\n",
        vi.getVolumeARN(),
        vi.getVolumeType());
    return volumeInfo;
}

// Returns the date in two formats as a list
public static boolean CompareDates(int daysBack, Date snapshotDate) {
    Date today = new Date();
    Calendar cal = new GregorianCalendar();
    cal.setTime(today);
    cal.add(Calendar.DAY_OF_MONTH, -daysBack);
    Date cutoffDate = cal.getTime();

```

```
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }
}
```

## Eliminazione di snapshot tramite l'SDK AWS per .NET

Per eliminare molti snapshot associati a un volume, puoi usare un approccio programmatico. L'esempio seguente descrive come eliminare snapshot tramite l'SDK AWS per .NET versioni 2 e 3. 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 dell'SDK AWS per .NET. Se devi eliminare solo pochi snapshot, usa la console, come descritto in [Eliminazione di uno snapshot](#).

Example : eliminazione di istantanee utilizzando l' AWS SDK for .NET

Nel seguente esempio di codice C#, un AWS Identity and Access Management utente può elencare le istantanee per ogni volume di un gateway. L'utente può quindi determinare se la data di inizio dello snapshot è precedente o successiva a una data specificata (periodo di conservazione) ed eliminare gli snapshot che hanno superato questo periodo di conservazione. L'esempio utilizza l'API SDK AWS per .NET per Storage Gateway e Amazon EC2. L'API di Amazon EC2 include operazioni per l'uso di snapshot.

L'esempio di codice seguente utilizza l' AWS SDK for .NET versione 2 e 3. Puoi eseguire la migrazione delle versioni precedenti di .NET alla versione più recente. Per ulteriori informazioni, consulta [Migrazione del codice all'ultima versione dell' AWS SDK for .NET](#).

Aggiorna il codice per fornire l'endpoint del servizio, il nome della risorsa Amazon (ARN) del gateway e il numero di giorni precedenti per cui vuoi salvare gli snapshot. Verranno eliminati gli snapshot acquisiti prima di questo limite. Potresti anche dover specificare il valore booleano `viewOnly`, che indica se vuoi visualizzare gli snapshot da eliminare o eseguire effettivamente le eliminazioni degli snapshot. Prima di tutto, esegui il codice solo con l'opzione di visualizzazione, ovvero con `viewOnly` impostato su `true`, per visualizzare gli snapshot eliminati dal codice. 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

Prima di tutto, devi creare un utente e collegare la policy IAM minima all'utente. Puoi quindi pianificare gli snapshot automatici per il gateway.

Il codice seguente crea la policy minima che permette a un utente di eliminare snapshot. In questo esempio, la policy è denominata **sgw-delete-snapshot**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StmtEC2Snapshots",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "StmtSgwListVolumes",
      "Effect": "Allow",
      "Action": [
        "storagegateway:ListVolumes"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Il codice C# seguente trova nel gateway specificato tutti gli snapshot che corrispondono ai volumi e al periodo limite e quindi li elimina.

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
```

```
class Program
{
    /*
     * Replace the variables below to match your environment.
     */

    /* IAM AccessKey */
    static String AwsAccessKey = "AKIA.....";

    /* IAM SecretKey */
    static String AwsSecretKey = "*****";

    /* Account number, 12 digits, no hyphen */
    static String OwnerID = "123456789012";

    /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXX* */
    static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXX";

    /* Snapshot status: "completed", "pending", "error" */

    static String SnapshotStatus = "completed";

    /* Region where your gateway is activated */
    static String AwsRegion = "ap-southeast-2";

    /* Minimum age of snapshots before they are deleted (retention policy) */
    static int daysBack = 30;

    /*
     * Do not modify the four lines below.
     */
    static AmazonEC2Config ec2Config;
    static AmazonEC2Client ec2Client;
    static AmazonStorageGatewayClient sgClient;
    static AmazonStorageGatewayConfig sgConfig;

    static void Main(string[] args)
    {
        // Create an EC2 client.
        ec2Config = new AmazonEC2Config();
        ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
        ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);
    }
}
```

```
// Create a Storage Gateway client.
sgConfig = new AmazonStorageGatewayConfig();
sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                        daysBack);
DeleteSnapshots(StorageGatewaySnapshots);
}

/*
 * List all volumes for your gateway
 * returns: A list of VolumeInfos, or null.
 */
private static List<VolumeInfo> ListVolumesForGateway()
{
    ListVolumesResponse response = new ListVolumesResponse();
    try
    {
        ListVolumesRequest request = new ListVolumesRequest();
        request.GatewayARN = GatewayARN;
        response = sgClient.ListVolumes(request);

        foreach (VolumeInfo vi in response.VolumeInfos)
        {
            Console.WriteLine(OutputVolumeInfo(vi));
        }
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine(ex.Message);
    }
    return response.VolumeInfos;
}

/*
 * Gets the list of snapshots that match the requested volumes
 * and cutoff period.
 */
```

```
private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
{
    List<Snapshot> SelectedSnapshots = new List<Snapshot>();
    try
    {
        foreach (VolumeInfo vi in volumes)
        {
            String volumeARN = vi.VolumeARN;
            String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

            DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

            Filter ownerFilter = new Filter();
            List<String> ownerValues = new List<String>();
            ownerValues.Add(OwnerID);
            ownerFilter.Name = "owner-id";
            ownerFilter.Values = ownerValues;
            describeSnapshotsRequest.Filters.Add(ownerFilter);

            Filter statusFilter = new Filter();
            List<String> statusValues = new List<String>();
            statusValues.Add(SnapshotStatus);
            statusFilter.Name = "status";
            statusFilter.Values = statusValues;
            describeSnapshotsRequest.Filters.Add(statusFilter);

            Filter volumeFilter = new Filter();
            List<String> volumeValues = new List<String>();
            volumeValues.Add(volumeID);
            volumeFilter.Name = "volume-id";
            volumeFilter.Values = volumeValues;
            describeSnapshotsRequest.Filters.Add(volumeFilter);

            DescribeSnapshotsResponse describeSnapshotsResponse =
                ec2Client.DescribeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
            Console.WriteLine("volume-id = " + volumeID);
            foreach (Snapshot s in snapshots)
            {
                if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
```

```
        {
            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                " + s.StartTime + ", " + s.Description);
            SelectedSnapshots.Add(s);
        }
    }
}
}
}
}
catch (AmazonEC2Exception ex)
{
    Console.WriteLine(ex.Message);
}
return SelectedSnapshots;
}

/*
 * Deletes a list of snapshots.
 */
private static void DeleteSnapshots(List<Snapshot> snapshots)
{
    try
    {
        foreach (Snapshot s in snapshots)
        {
            DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
            DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
            Console.WriteLine("Volume: " +
                s.VolumeId +
                " => Snapshot: " +
                s.SnapshotId +
                " Response: "
                + response.HttpStatusCode.ToString());
        }
    }
    catch (AmazonEC2Exception ex)
    {
        Console.WriteLine(ex.Message);
    }
}

/*
```



```
    * Checks if the snapshot creation date is past the retention period.
    */
    private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
snapshotDate)
    {
        DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
        return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
    }

    /*
    * Displays information related to a volume.
    */
    private static String OutputVolumeInfo(VolumeInfo vi)
    {
        String volumeInfo = String.Format(
            "Volume Info:\n" +
            "  ARN: {0}\n" +
            "  Type: {1}\n",
            vi.VolumeARN,
            vi.VolumeType);
        return volumeInfo;
    }
}
}
```

## Eliminazione di snapshot tramite AWS Tools for Windows PowerShell

Per eliminare molti snapshot associati a un volume, puoi usare un approccio programmatico. L'esempio seguente descrive come eliminare snapshot tramite AWS Tools for Windows PowerShell. Per utilizzare lo script di esempio, è necessario avere dimestichezza con l'esecuzione di uno PowerShell script. Per ulteriori informazioni, consulta l'argomento relativo alle [nozioni di base](#) nella AWS Tools for Windows PowerShell. Se devi eliminare solo pochi snapshot, usa la console, come descritto in [Eliminazione di uno snapshot](#).

Example : Eliminazione di istantanee utilizzando AWS Tools for Windows PowerShell

Il seguente esempio di PowerShell script elenca le istantanee per ogni volume di un gateway e indica se l'ora di inizio dell'istantanea è precedente o successiva a una data specificata. Utilizza i AWS Tools for Windows PowerShell cmdlet per Storage Gateway e Amazon EC2. L'API di Amazon EC2 include operazioni per l'uso di snapshot.

Devi aggiornare lo script e specificare l'ARN (Amazon Resource Name) del gateway e il numero di giorni precedenti per cui vuoi salvare gli snapshot. Verranno eliminati gli snapshot acquisiti prima di questo limite. Potresti anche dover specificare il valore booleano `viewOnly`, che indica se vuoi visualizzare gli snapshot da eliminare o eseguire effettivamente le eliminazioni degli snapshot. Prima di tutto, esegui il codice solo con l'opzione di visualizzazione, ovvero con `viewOnly` impostato su `true`, per visualizzare gli snapshot eliminati dal codice.

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS 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_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "**** provide gateway ARN ****"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
{ Write-Output("`nVolume Info:")
  Write-Output("ARN: " + $volumes.VolumeARN)
  write-Output("Type: " + $volumes.VolumeType)
}

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
{
  $volumeARN = $volume.VolumeARN

  $volumeId = ($volumeARN-split"/")[3].ToLower()
```

```
$filter = New-Object Amazon.EC2.Model.Filter
$filter.Name = "volume-id"
$filter.Value.Add($volumeId)

$snapshots = get-EC2Snapshot -Filter $filter
Write-Output("`nFor volume-id = " + $volumeId)
foreach ($s in $snapshots)
{
    $d = ([DateTime]::Now).AddDays(-$daysBack)
    $meetsCriteria = $false
    if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
    {
        $meetsCriteria = $true
    }

    $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
    $meetsCriteria
    if (!$viewOnly -AND $meetsCriteria)
    {
        $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
        #Can get RequestId from response for troubleshooting.
        $sb = $sb + ", deleted? yes"
    }
    else {
        $sb = $sb + ", deleted? no"
    }
    Write-Output($sb)
}
}
```

## Informazioni su stati e transizioni dei volumi

Ogni volume ha uno stato associato che indica chiaramente l'integrità del volume. Nella maggior parte dei casi, lo stato indica che il volume funziona correttamente e che non è richiesta alcuna operazione da parte tua. In alcuni casi, lo stato indica un problema nel volume che potrebbe richiedere il tuo intervento. Puoi trovare le informazioni seguenti per aiutarti a decidere quando è necessario agire. È possibile visualizzare lo stato del volume sulla console Storage Gateway o utilizzando una delle API operazioni di Storage Gateway, ad esempio [DescribeCachediSCSIVolumes](#) o [DescribeStorediSCSIVolumes](#).

### Argomenti

- [Informazioni sullo stato del volume](#)
- [Informazioni sullo stato di collegamento](#)
- [Informazioni sulle transizioni tra stati dei volumi nella cache](#)
- [Informazioni sulle transizioni tra stati dei volumi archiviati](#)

## Informazioni sullo stato del volume

La seguente tabella mostra lo stato del volume nella console Storage Gateway. Lo stato del volume viene visualizzato nella colonna Status (Stato) per ogni volume di storage nel gateway. Lo stato di un volume che funziona normalmente è Available (Disponibile).

La tabella seguente contiene le descrizioni per ogni stato del volume di storage, con l'indicazione se per lo stato specifico è necessario un intervento. Lo stato Available (Disponibile) è lo stato normale di un volume. Un volume deve avere questo stato per tutto o quasi il tempo in cui viene usato.

Stato	Significato
Disponibilità	<p>Il volume è disponibile per l'uso. Questo stato è lo stato di esecuzione normale per un volume.</p> <p>Quando viene completata una fase con stato Bootstrapping (Processo di bootstrap), il volume torna allo stato Available (Disponibile). Questo significa che il gateway ha sincronizzato tutte le modifiche apportate al volume dalla prima volta in cui è passato allo stato Pass Through (Transito).</p>
Bootstrapping (Processo di bootstrap)	<p>Il gateway sincronizza i dati localmente con una copia dei dati archiviati in AWS. In genere non devi intervenire in alcun modo per questo stato, perché il volume di storage vede automaticamente lo stato Available (Disponibile) nella maggior parte dei casi.</p> <p>Di seguito vengono presentati alcuni scenari in cui lo stato del volume è Bootstrapping (Processo di bootstrap):</p> <ul style="list-style-type: none"> <li>• Un gateway si è arrestato in modo imprevisto.</li> <li>•</li> </ul>

Stato	Significato
	<p>È stata superata la capacità del buffer di caricamento di un gateway. In questo scenario il bootstrap avviene quando il volume è in stato Pass Through (Transito) e la quantità di spazio del buffer di caricamento gratuita aumenta in misura sufficiente. Puoi fornire altro spazio per il buffer di caricamento come metodo per aumentare la percentuale di spazio del buffer di caricamento gratuita. In questo scenario specifico il volume di storage passa dallo stato Pass Through (Transito) a Bootstrapping (Processo di bootstrap) fino ad Available (Disponibile). Puoi continuare a usare questo volume durante il periodo di bootstrap. Tuttavia, non puoi acquisire snapshot del volume in questa fase.</p> <ul style="list-style-type: none"> <li>• Stai creando un gateway di volumi archiviati, preservando i dati del disco locale esistenti. In questo scenario, il gateway inizia a caricare tutti i dati su. AWS Il volume ha lo stato Bootstrap fino a quando non vengono copiati tutti i dati dal disco locale. AWS Puoi usare il volume durante il periodo di bootstrap. Tuttavia, non puoi acquisire snapshot del volume in questa fase.</li> </ul>
Creating (Creazione in corso)	Il volume è attualmente in fase di creazione e non è pronto per l'uso. Lo stato Creating (Creazione in corso) è transitorio. Nessuna operazione richiesta.
Deleting (Eliminazione in corso)	Il volume è attualmente in fase di eliminazione. Lo stato Deleting (Eliminazione in corso) è transitorio. Nessuna operazione richiesta.
Irrecoverable (Irrecuperabile)	Si è verificato un errore per cui il volume non può essere ripristinato. Per informazioni su cosa fare in questa situazione, consulta <a href="#">Come risolvere i problemi dei volumi</a> .

Stato	Significato
Pass Through (Transito)	<p>I dati mantenuti localmente non sono sincronizzati con i dati archiviati in AWS. I dati scritti su un volume mentre il volume è in stato Pass Through (Transito) rimangono nella cache fino a quando il volume è nello stato Bootstrapping (Processo di bootstrap). Questi dati iniziano a essere caricati AWS quando inizia lo stato di Bootstrap.</p> <p>Lo stato Pass Through (Transito) può verificarsi per diversi motivi, indicati di seguito:</p> <ul style="list-style-type: none"><li>• Lo stato Pass Through (Transito) si verifica se il gateway ha esaurito lo spazio del buffer di caricamento. Le applicazioni possono continuare a leggere e scrivere dati dai e nei volumi di storage mentre i volumi sono in stato Pass Through (Transito). Tuttavia, il gateway non scrive alcun dato del volume nel buffer di caricamento né carica questi dati in AWS.</li></ul> <p>Il gateway continua a caricare tutti i dati scritti nel volume prima del passaggio del volume allo stato Pass Through (Transito). Tutti gli snapshot di un volume di storage in attesa o pianificati non riescono mentre il volume è in stato Pass Through (Transito). Per informazioni su cosa fare quando il volume di storage è in stato Pass Through (Transito) a causa del superamento dello spazio del buffer di caricamento, consulta <a href="#">Come risolvere i problemi dei volumi</a>.</p> <p>Per tornare allo ACTIVE stato, un volume in Pass Through deve completare la fase di Bootstrap. Durante il Bootstrap, il volume ristabilisce la sincronizzazione interna AWS, in modo da poter riprendere la registrazione (registro) delle modifiche al volume e attivare la funzionalità. <code>CreateSnapshot</code> Durante la fase con stato Bootstrapping (Processo di bootstrap), le scritture nel volume vengono registrate nel buffer di caricamento.</p> <ul style="list-style-type: none"><li>• Lo stato Pass Through (Transito) si verifica quando avviene più di un processo di bootstrap dei volumi di storage per volta. Il bootstrap può essere eseguito da un solo volume di storage del gateway per volta. Ad esempio, supponiamo di creare due volumi di storage e di</li></ul>

Stato	Significato
	<p>scegliere di conservare i dati esistenti in entrambi. In questo caso, il secondo volume di storage è in stato Pass Through (Transito) finché il primo non completa il bootstrap. Questo scenario non richiede alcun intervento. Una volta creato, ogni volume di storage passa automaticamente allo stato Available (Disponibile). Puoi leggere e scrivere nel volume di storage mentre è in stato Pass Through (Transito) o Bootstrapping (Processo di bootstrap).</p> <ul style="list-style-type: none"> <li>• Più raramente lo stato Pass Through (Transito) può indicare che un disco allocato per l'uso del buffer di caricamento è danneggiato. Per informazioni su come intervenire in questo scenario, consulta <a href="#">Come risolvere i problemi dei volumi</a>.</li> <li>• Lo stato Pass Through (Transito) può verificarsi quando un volume è in stato Active (Attivo) o Bootstrapping (Processo di bootstrap). In questo caso, il volume riceve una scrittura, ma il buffer di caricamento non ha capacità sufficiente per registrare la scrittura.</li> <li>• Lo stato Pass Through (Transito) si verifica quando un volume è in qualsiasi stato e il gateway non viene arrestato in modo corretto. Questo tipo di arresto può verificarsi a causa di un arresto anomalo del software o dello spegnimento della macchina virtuale. In questo caso, un volume in qualsiasi stato passa allo stato Pass Through (Transito).</li> </ul>
Restoring (Ripristino)	<p>Il volume è in fase di ripristino da uno snapshot esistente. Questo stato interessa solo i volumi archiviati. Per ulteriori informazioni, consulta <a href="#">Come funziona il gateway di volumi (architettura)</a>.</p> <p>Se ripristini due volumi di storage contemporaneamente, entrambi indicano Restoring (Ripristino in corso) come stato. Una volta creato, ogni volume di storage passa automaticamente allo stato Available (Disponibile). Puoi leggere e scrivere in un volume di storage e acquisire uno snapshot del volume mentre è in stato Restoring (Ripristino in corso).</p>

Stato	Significato
Restoring Pass Through (Transito ripristino)	<p>Il volume è in fase di ripristino da uno snapshot esistente e ha riscontrato un problema relativo al buffer di caricamento. Questo stato interessa solo i volumi archiviati. Per ulteriori informazioni, consulta <a href="#">Come funziona il gateway di volumi (architettura)</a>.</p> <p>Una possibile causa dello stato Restoring Pass Through (Transito ripristino) è l'esaurimento dello spazio del buffer di caricamento da parte del gateway. Le applicazioni possono continuare a leggere e scrivere dati dai e nei volumi di storage mentre i volumi sono in stato Restoring Pass Through (Transito ripristino). Tuttavia, non puoi acquisire snapshot di un volume di storage durante lo stato Restoring Pass Through (Transito ripristino). Per informazioni su come intervenire quando il volume di storage è in stato Restoring Pass Through (Transito ripristino) a causa del superamento della capacità del buffer di caricamento, consulta <a href="#">Come risolvere i problemi dei volumi</a>.</p> <p>Più raramente lo stato Restoring Pass Through (Transito ripristino) può indicare che un disco allocato per un buffer di caricamento è danneggiato. Per informazioni su come intervenire in questo scenario, consulta <a href="#">Come risolvere i problemi dei volumi</a>.</p>
Upload Buffer Not Configured (Buffer di caricamento non configurato)	<p>Non puoi creare o usare il volume perché non è stato configurato alcun buffer di caricamento per il gateway. Per informazioni su come aggiungere e capacità del buffer di caricamento per i volumi in una configurazione di volumi nella cache, consulta <a href="#">Determinazione delle dimensioni del buffer di caricamento da allocare</a>. Per informazioni su come aggiungere capacità del buffer di caricamento per i volumi in una configurazione di volumi archiviati, consulta <a href="#">Determinazione delle dimensioni del buffer di caricamento da allocare</a>.</p>

## Informazioni sullo stato di collegamento

È possibile scollegare un volume da un gateway o collegarlo a un gateway utilizzando la console Storage Gateway oAPI. La seguente tabella mostra lo stato di collegamento del volume nella console Storage Gateway. Lo stato di collegamento del volume viene visualizzato nella colonna



Attachment status (Stato di collegamento) per ogni volume di storage nel gateway. Ad esempio, un volume scollegato da un gateway presenta lo stato Detached (Scollegato). Per informazioni su come scollegare e collegare un volume, consulta [Spostamento dei volumi su un gateway differente](#).

Stato	Significato
Collegato	Il volume è collegato a un gateway.
Distaccato	Il volume è scollegato a un gateway.
Scollegamento in corso	Il volume viene scollegato da un gateway. Quando scolleghi un volume e il volume non dispone di dati, potresti non visualizzare questo stato.

## Informazioni sulle transizioni tra stati dei volumi nella cache

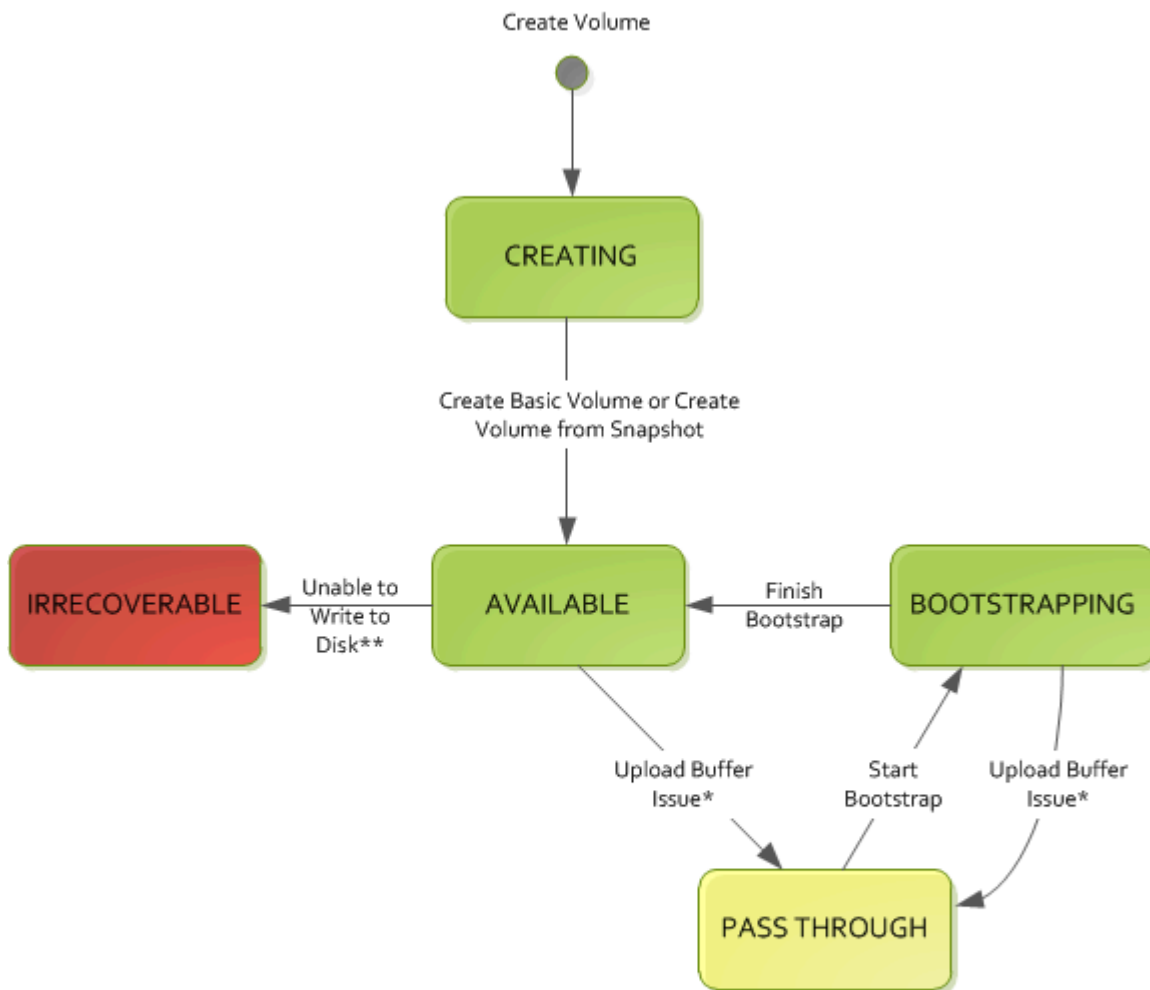
Usa il diagramma degli stati seguente per identificare le transizioni più comuni tra stati per volumi in gateway nella cache. Non devi comprendere tutti i dettagli del diagramma per poter usare il gateway in modo efficace. Il diagramma fornisce informazioni dettagliate se vuoi saperne di più sul funzionamento dei gateway di volumi.

Il diagramma non mostra gli stati Upload Buffer Not Configured (Buffer di caricamento non configurato) e Deleting (Eliminazione in corso). Gli stati del volume nel diagramma sono visualizzati in caselle verdi, gialle e rosse. Puoi interpretare i colori come descritto nella tabella.

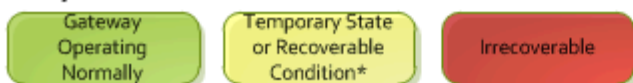
Colore	Stato del volume
Verde	Il gateway funziona normalmente. Lo stato del volume è Available (Disponibile) o può diventare Available (Disponibile).
Giallo	Il volume è in stato Pass Through (Transito), che indica la presenza di un possibile problema relativo al volume di storage. Se questo stato viene visualizzato perché lo spazio del buffer di caricamento è completo, in alcuni casi lo spazio del buffer torna di nuovo disponibile. A questo punto, il volume di storage si corregge automaticamente.

Colore	Stato del volume
	<p>amente passando allo stato Available (Disponibile). In altri casi, potresti dover aggiungere altro spazio del buffer di caricamento al gateway per permettere al volume di storage di passare allo stato Available (Disponibile). Per informazioni su come risolvere un problema di superamento della capacità del buffer di caricamento, consulta <a href="#">Come risolvere i problemi dei volumi</a>. Per informazioni su come aggiungere capacità del buffer, consulta <a href="#">Determinazione delle dimensioni del buffer di caricamento da allocare</a>.</p>
Rosso	<p>Il volume di storage è in stato Irrecoverable (Irrecuperabile). In questo caso, devi eliminare il volume. Per informazioni su come fare, consulta <a href="#">Per eliminare un volume</a>.</p>

Nel diagramma una transizione tra due stati è rappresentata da una linea con etichetta. Ad esempio, la transizione dallo stato Creating (Creazione in corso) allo stato Available (Disponibile) è indicata come creazione del volume di base o creazione del volume da snapshot. Questa transizione rappresenta la creazione di un volume nella cache. Per ulteriori informazioni sulla creazione di volumi di storage, consulta [Aggiunta di un volume](#).



### Key



\* e.g. run out of upload buffer

\*\* e.g. lost connectivity

### Note

Lo stato Pass Through (Transito) del volume è visualizzato in giallo nel diagramma. Tuttavia, questo non corrisponde al colore dell'icona di stato nella casella Stato della console Storage Gateway.

## Informazioni sulle transizioni tra stati dei volumi archiviati

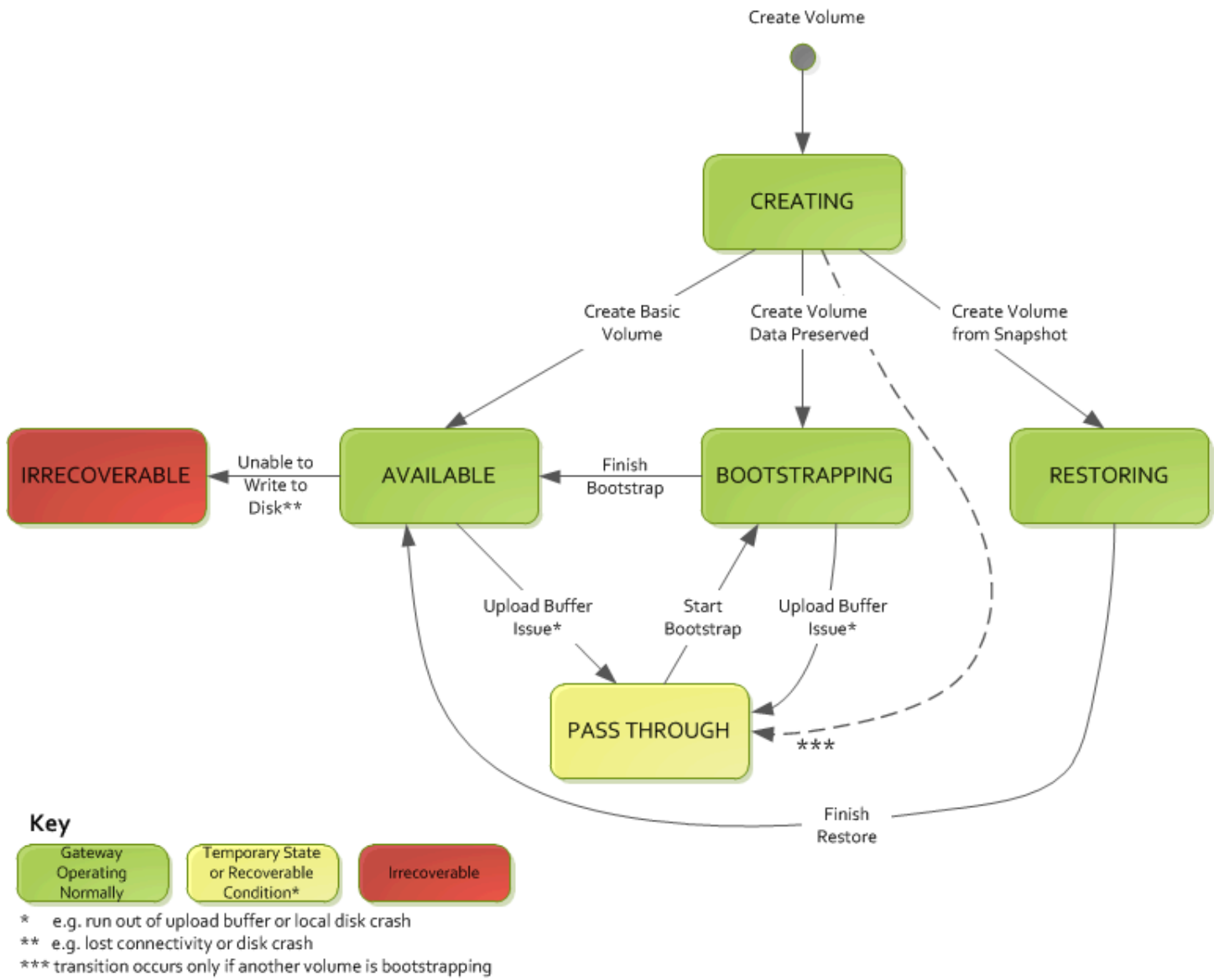
Usa il diagramma degli stati seguente per identificare le transizioni più comuni tra stati per volumi in gateway archiviati. Non devi comprendere tutti i dettagli del diagramma per poter usare il gateway in modo efficace. Il diagramma fornisce informazioni dettagliate se vuoi saperne di più sul funzionamento dei gateway di volumi.

Il diagramma non mostra gli stati Upload Buffer Not Configured (Buffer di caricamento non configurato) e Deleting (Eliminazione in corso). Gli stati del volume nel diagramma sono visualizzati in caselle verdi, gialle e rosse. Puoi interpretare i colori come descritto nella tabella.

Colore	Stato del volume
Verde	Il gateway funziona normalmente. Lo stato del volume è Available (Disponibile) o può diventare Available (Disponibile).
Giallo	Quando crei un volume di storage e conservi i dati, il passaggio dallo stato Creating (Creazione e in corso) allo stato Pass Through (Transito) avviene se è in corso il bootstrap di un altro volume. In questo caso, il volume con stato Pass Through (Transito) passa allo stato Bootstrapping (Processo di bootstrap) e quindi allo stato Available (Disponibile) al termine del bootstrap del primo volume. In scenari diversi da quello specifico descritto, il giallo, corrispondente allo stato Pass Through (Transito), indica un possibile problema nel volume di storage, il più comune dei quali riguarda il buffer di caricamento. Se la capacità del buffer di caricamento è stata superata, in alcuni casi lo spazio del buffer torna disponibile. A questo punto, il volume di storage si corregge automaticamente passando allo stato Available (Disponibile). In altri casi, potresti dover aggiungere altra capacità del buffer di caricamento al gateway per riportare il volume di storage allo stato Available (Disponibile). Per

Colore	Stato del volume
	informazioni su come risolvere un problema di superamento della capacità del buffer di caricamento, consulta <a href="#">Come risolvere i problemi dei volumi</a> . Per informazioni su come aggiungere e capacità del buffer, consulta <a href="#">Determinazione delle dimensioni del buffer di caricamento da allocare</a> .
Rosso	Il volume di storage è in stato Irrecuperabile (Irrecuperabile). In questo caso, devi eliminare il volume. Per informazioni su come fare, consulta <a href="#">Eliminazione di un volume</a> .

Nel diagramma seguente una transizione tra due stati è rappresentata da una linea con etichetta. Ad esempio, la transizione dallo stato Creating (Creazione in corso) allo stato Available (Disponibile) è indicata come creazione del volume di base. Questa transizione rappresenta la creazione di un volume di storage senza la necessità di conservare i dati o creare il volume da uno snapshot.



**Note**

Lo stato Pass Through (Transito) del volume è visualizzato in giallo nel diagramma. Tuttavia, questo non corrisponde al colore dell'icona di stato nella casella Stato della console Storage Gateway.

## 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 di migrazione del gateway. Di seguito sono riportati alcuni motivi per eseguire questa operazione:

- Sposta i tuoi dati su piattaforme di hosting migliori o su EC2 istanze Amazon più recenti.
- 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 dei volumi archiviati su un nuovo gateway di volumi archiviato

Per spostare il volume archiviato su un nuovo gateway di volumi archiviato

1. Interrompi tutte le applicazioni che stanno scrivendo sul vecchio gateway di volumi archiviato.
2. Utilizza la procedura seguente per creare uno snapshot per il volume, quindi attendi che lo snapshot sia completato.
  - a. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
  - b. Nel riquadro di navigazione scegliere Volumi e quindi selezionare il volume da cui si vuole creare lo snapshot.
  - c. In Actions (Operazioni), scegli Create snapshot (Crea snapshot).
  - d. Nella finestra di dialogo Crea snapshot immettere una descrizione dello snapshot e quindi scegliere Crea snapshot.

Per verificare che lo snapshot sia stato creato, è possibile usare la console. Se il caricamento dei dati sul volume è ancora in corso, attendi il completamento del caricamento prima di continuare con il passaggio successivo. Per visualizzare lo stato degli snapshot e verificare che nessuno sia in sospeso, seleziona i collegamenti agli snapshot sui volumi.

3. Utilizza i seguenti passaggi per arrestare il vecchio gateway di volumi archiviato:

- a. Nel riquadro di navigazione scegliere Gateway e quindi scegliere il vecchio gateway di volumi archiviato 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 gateway, 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. Quando il gateway si arresta, lo stato del gateway è Arresto.

- c. Spegni la macchina virtuale utilizzando i controlli dell'hypervisor.

Per informazioni su come arrestare un gateway, consulta [Avvio e arresto di un gateway di volumi](#).

4. Scollega i dischi di archiviazione associati ai volumi archiviati dalla macchina virtuale del gateway. Ciò esclude il disco root della macchina virtuale.
5. [Attiva un nuovo Volume Gateway archiviato con una nuova immagine di macchina virtuale hypervisor disponibile dalla console Storage Gateway a casa. https://console.aws.amazon.com/storagegateway/](https://console.aws.amazon.com/storagegateway/)
6. Collega i dischi di archiviazione fisici che hai scollegato dalla macchina virtuale del vecchio gateway di volumi archiviato nel passaggio 5.
7. Per conservare i dati esistenti sul disco, utilizza i seguenti passaggi per creare volumi archiviati.
  - a. Nella console Storage Gateway seleziona Crea volume.
  - b. Nella finestra di dialogo Crea volume, seleziona il gateway di volumi archiviato creato nel passaggio 5.
  - c. Scegli un valore di ID disco dall'elenco.
  - d. Per Contenuto del volume, seleziona l'opzione Mantieni i dati esistenti sul disco.

Per ulteriori informazioni sulla creazione di volumi, consulta [Creazione di un volume](#).

8. (Facoltativo) Nella procedura guidata di configurazione dell'CHAPautenticazione che appare, inserisci il nome dell'iniziatore, il segreto dell'iniziatore e il segreto di destinazione, quindi scegli Salva.



Per ulteriori informazioni sull'utilizzo dell'autenticazione Challenge-Handshake Authentication Protocol (), consulta. CHAP [Configurazione dell'CHAPautenticazione per i tuoi obiettivi i SCSI](#)

9. Avvia l'applicazione che scrive sul volume archiviato.
10. Dopo aver verificato che il nuovo gateway di volumi archiviato funziona correttamente, è possibile eliminare il vecchio gateway di volumi archiviato.

**⚠ 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.

Utilizza i seguenti passaggi per eliminare il vecchio gateway di volumi archiviato:

**⚠ Warning**

Un gateway eliminato non può più essere recuperato.

- a. Nel riquadro di navigazione scegliere Gateway e quindi scegliere il vecchio gateway di volumi archiviato da eliminare.
- b. Per Actions (Operazioni), scegli Delete stack (Elimina stack).
- c. Nella finestra di dialogo visualizzata, selezionare la casella di controllo appropriata per confermare l'eliminazione. Verificare che l'ID gateway riportato indichi il vecchio gateway di volumi archiviato da eliminare, quindi selezionare Elimina.



11. Elimina la macchina virtuale del vecchio gateway. Per ulteriori informazioni su come eliminare una macchina virtuale, consultare la documentazione del proprio hypervisor.

## Spostamento dei volumi memorizzati nella cache su una nuova macchina virtuale del gateway di volumi memorizzata nella cache

Per spostare i volumi memorizzati nella cache su una nuova macchina virtuale (VM) del gateway di volumi memorizzata nella cache

1. Interrompi tutte le applicazioni che stanno scrivendo sul vecchio gateway di volumi memorizzato nella cache.
2. Smonta o disconnetti i SCSI volumi da tutti i client che li utilizzano. Questo aiuta a mantenere coerenti i dati su tali volumi impedendo ai client di modificare o aggiungere dati a tali volumi.
3. Utilizza la procedura seguente per creare uno snapshot per il volume, quindi attendi che lo snapshot sia completato.
  - a. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
  - b. Nel riquadro di navigazione scegliere Volumi e quindi selezionare il volume da cui si vuole creare lo snapshot.
  - c. In Actions (Operazioni), scegli Create snapshot (Crea snapshot).
  - d. Nella finestra di dialogo Crea snapshot immettere una descrizione dello snapshot e quindi scegliere Crea snapshot.

Per verificare che lo snapshot sia stato creato, è possibile usare la console. Se il caricamento dei dati sul volume è ancora in corso, attendi il completamento del caricamento prima di continuare con il passaggio successivo. Per visualizzare lo stato degli snapshot e verificare che nessuno sia in sospeso, seleziona i collegamenti agli snapshot sui volumi.

Per ulteriori informazioni sulla verifica dello stato del volume nella console, consulta [Informazioni su stati e transizioni dei volumi](#). Per informazioni sullo stato di un volume, consulta [Informazioni sulle transizioni tra stati dei volumi nella cache](#).

4. Utilizza i seguenti passaggi per arrestare il vecchio gateway di volumi memorizzato nella cache:
  - a. Nel riquadro di navigazione scegliere Gateway e quindi scegliere il vecchio gateway di volumi memorizzato nella cache 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. Prendere nota dell'ID del gateway, in quanto sarà necessario in una fase successiva.

Durante l'arresto del vecchio gateway, è possibile che venga visualizzato un messaggio che indica lo stato del gateway. Quando il vecchio gateway viene arrestato, sulla scheda Dettagli vengono visualizzati un messaggio e un pulsante Avvia gateway. Quando il gateway si arresta, lo stato del gateway è Arresto.

- c. Spegni la vecchia macchina virtuale utilizzando i controlli dell'hypervisor. Per ulteriori informazioni sulla chiusura di un'EC2istanza Amazon, consulta la sezione [Arresto e avvio delle istanze](#) nella Amazon EC2 User Guide. Per ulteriori informazioni sullo spegnimento di una macchina virtuale o Hyper-V KVMVMware, consulta la documentazione dell'hypervisor.

Per informazioni su come arrestare un gateway, consulta [Avvio e arresto di un gateway di volumi](#).

5. Scollega tutti i dischi, inclusi il disco root, i dischi di cache e i dischi di buffer di caricamento, dalla vecchia macchina virtuale del gateway.

#### Note

Prendi nota dell'ID del volume del disco root e dell'ID del gateway associato a quel disco root. Questo disco viene scollegato dal nuovo hypervisor Storage Gateway in una fase successiva. (Consulta la fase 11).

Se utilizzi un'EC2istanza Amazon come macchina virtuale per il tuo Volume Gateway in cache, consulta Scollegare [un EBS volume Amazon da un'istanza Linux](#) nella Amazon EC2 User Guide. Per informazioni su come scollegare i dischi da una macchina virtuale o Hyper-V KVMVMware, consulta la documentazione del tuo hypervisor.

6. Crea una nuova istanza della macchina virtuale dell'hypervisor Storage Gateway, ma non attivarla come gateway. Per ulteriori informazioni sulla creazione di una nuova macchina virtuale dell'hypervisor Storage Gateway, consulta [Configura un gateway di volumi](#). Questo nuovo gateway assumerà l'identità del vecchio gateway.

**Note**

Non aggiungere dischi per la cache o il buffer di caricamento alla nuova macchina virtuale. La nuova macchina virtuale utilizzerà gli stessi dischi di cache e gli stessi dischi di buffer di caricamento utilizzati dalla vecchia macchina virtuale.

7. La nuova istanza della macchina virtuale dell'hypervisor Storage Gateway deve utilizzare la stessa configurazione di rete della vecchia macchina virtuale. La configurazione di rete predefinita per il gateway è Dynamic Host Configuration Protocol (). DHCP ConDHCP, al gateway viene assegnato automaticamente un indirizzo IP.

Se è necessario configurare manualmente un indirizzo IP statico per la nuova macchina virtuale, consulta [Configurazione di rete del gateway](#) per ulteriori dettagli. Se il gateway deve utilizzare un proxy Socket Secure versione 5 (SOCKS5) per connettersi a Internet, consulta [Instradamento del gateway in locale tramite un proxy](#) per ulteriori dettagli.

8. Avvia la nuova macchina virtuale.
9. Collega i dischi scollegati dalla vecchia macchina virtuale del gateway di volumi memorizzato nella cache nel passaggio 5 al nuovo gateway di volumi memorizzato nella cache. Collegali alla nuova macchina virtuale del gateway nello stesso ordine in cui si trovano sulla vecchia macchina virtuale del gateway.

Tutti i dischi devono mantenere invariata la transizione. Non modificate le dimensioni dei volumi, poiché ciò causerebbe una incoerenza dei metadati.

10. Avvia il processo di migrazione del gateway connettendoti alla nuova macchina virtuale con un file URL che utilizza il seguente formato.

```
http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
```

È possibile riutilizzare lo stesso indirizzo IP per la nuova macchina virtuale del gateway utilizzato per la vecchia macchina virtuale del gateway. Il tuo aspetto URL dovrebbe essere simile all'esempio seguente.

```
http://198.51.100.123/migrate?gatewayId=sgw-12345678
```

Usalo URL da un browser o dalla riga di comando utilizzando `curl`, per avviare il processo di migrazione.

Quando il processo di migrazione del gateway viene avviato, viene visualizzato il seguente messaggio:

```
Successfully imported Storage Gateway information. Please refer to
Storage Gateway documentation to perform the next steps to complete the
migration.
```

11. Scollega il disco root del vecchio gateway, il cui ID di volume è stato annotato nel passaggio 5.
12. Avvia il gateway.

Utilizza i seguenti passaggi per avviare il nuovo gateway di volumi memorizzato nella cache:

- a. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
- b. Nel riquadro di navigazione scegliere Gateway, quindi selezionare il nuovo gateway da avviare. Lo stato del gateway è Shutdown (Arrestato).
- c. Scegliere Dettagli quindi scegliere Avvia gateway.

Per ulteriori informazioni sull'avvio di un gateway, consulta [Avvio e arresto di un gateway di volumi](#).

13. I volumi dovrebbero ora essere disponibili per le applicazioni all'indirizzo IP della nuova macchina virtuale del gateway.
14. Conferma che i volumi siano disponibili ed elimina la vecchia macchina virtuale del gateway. 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](#)
- [Dimensioni per i parametri di Storage Gateway](#)
- [Monitoraggio del buffer di caricamento](#)
- [Monitoraggio dello storage della cache](#)
- [Comprensione degli allarmi CloudWatch](#)
- [Creazione di CloudWatch allarmi consigliati per il tuo gateway](#)
- [Creazione di un CloudWatch allarme personalizzato per il gateway](#)
- [Monitoraggio del gateway di volumi](#)

## 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
<code>AvailabilityNotifications</code>	<p>Numero di notifiche di stato relative alla disponibilità generate dal gateway.</p> <p>Utilizza questo parametro con la statistica <code>Sum</code> per verificare se il gateway sta riscontrando eventi correlati alla disponibilità. Per dettagli sugli eventi, controlla il gruppo di <code>CloudWatch log</code> configurato.</p> <p>Unità: numero</p>
<code>CacheHitPercent</code>	<p>Percentuale di letture delle applicazioni servite dalla cache. Il campione si riferisce al termine del periodo di reporting.</p>

Parametro	Descrizione	
	Unità: percentuale	
CacheUsed	Numero totale di byte utilizzati i 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 dati RAM forniti alla macchina virtuale del gateway, in byte.  Unità: byte	
MemUsedBytes	Quantità di dati RAM attualmente in uso dalla macchina virtuale del gateway, in byte.  Unità: byte	



Parametro	Descrizione	
QueuedWrites	<p>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.</p> <p>Unità: byte</p>	
ReadBytes	<p>Numero totale di byte letti dalle applicazioni in locale durante il periodo di reporting per tutti i volumi nel gateway.</p> <p>Utilizzate questa metrica con la Sum statistica per misurare il throughput e con la statistica Samples IOPS per misurare. Samples IOPS</p> <p>Unità: byte</p>	
ReadTime	<p>Numero totale di millisecondi dedicati allo svolgimento delle operazioni di lettura dalle applicazioni in locale durante il periodo di reporting per tutti i volumi nel gateway.</p> <p>Usa questo parametro con la statistica Average per misurare la latenza.</p> <p>Unità: millisecondi</p>	

Parametro	Descrizione	
TimeSinceLastRecoveryPoint	<p>Tempo trascorso dall'ultimo punto di ripristino disponibile. Per ulteriori informazioni, consulta <a href="#">Il gateway nella cache è irraggiungibile e occorre recuperare i dati.</a></p> <p>Unità: secondi</p>	
TotalCacheSize	<p>Dimensione totale della cache in byte. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: byte</p>	
UploadBufferPercentageUsed	<p>Percentuale di utilizzo del buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: percentuale</p>	
UploadBufferUsed	<p>Numero totale di byte utilizzati nel buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: byte</p>	
UserCpuPercent	<p>Percentuale di CPU tempo dedicato all'elaborazione del gateway, media su tutti i core.</p> <p>Unità: percentuale</p>	

Parametro	Descrizione	
WorkingStorageFree	<p>Quantità totale di spazio inutilizzato nello storage di lavoro del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: byte</p>	
WorkingStoragePercentUsed	<p>Percentuale di utilizzo del buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: percentuale</p>	
WorkingStorageUsed	<p>Numero totale di byte utilizzati nel buffer di caricamento del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Unità: byte</p>	
WriteBytes	<p>Numero totale di byte scritti nelle applicazioni in locale durante il periodo di reporting per tutti i volumi nel gateway.</p> <p>Utilizza questa metrica con la Sum statistica per misurare il throughput e con la statistica per misurare. Samples IOPS</p> <p>Unità: byte</p>	

Parametro	Descrizione
<code>WriteTime</code>	<p>Numero totale di millisecondi dedicati allo svolgimento delle operazioni di scrittura dalle applicazioni in locale durante il periodo di reporting per tutti i volumi nel gateway.</p> <p>Usa questo parametro con la statistica <code>Average</code> per misurare la latenza.</p> <p>Unità: millisecondi</p>

## 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
<code>GatewayId</code> , <code>GatewayName</code>	<p>Queste dimensioni filtrano i dati richiesti sui parametri specifici per il gateway. Puoi identificare un gateway mediante il valore <code>GatewayId</code> o <code>GatewayName</code> . Se il nome del gateway è cambiato per l'intervallo di tempo per cui vuoi visualizzare i parametri, utilizza <code>GatewayId</code> .</p> <p>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 <a href="#">Measuring Performance Between Your Gateway and AWS</a></p>
<code>VolumeId</code>	<p>Questa dimensione filtra i dati richiesti sui parametri specifici per il volume. Identifica un volume di storage con il quale lavorare in base al relativo valore <code>VolumeId</code>. Per informazioni su come</p>

Dimensione	Descrizione
	utilizzare i parametri del volume, consulta <a href="#">Measuring Performance Between Your Application and Gateway</a> .

## 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 volumi \(architettura\)](#).

### 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 <code>UploadBufferPercentUsed</code> , <code>UploadBufferUsed</code> e <code>UploadBufferFree</code> con la statistica <code>Average</code> . Ad esempio, utilizzare <code>UploadBufferUsed</code> con la statistica <code>Average</code> 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. CloudWatch <https://console.aws.amazon.com/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, e 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 SNS argomento Amazon. Per ulteriori informazioni su AmazonSNS, consulta [Configurare Amazon SNS](#) nella Amazon CloudWatch User Guide.

- 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. Apri l'SNS e-mail di Amazon che è stata inviata all'indirizzo e-mail che hai 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 volumi \(architettura\)](#).

Articolo di interesse	Come misurare
Utilizzo totale della cache	Utilizzare i parametri <code>CachePercentUsed</code> e <code>TotalCacheSize</code> con la statistica <code>Average</code> . Ad esempio, utilizzare <code>CachePercentUsed</code> con la statistica <code>Average</code> per analizzare l'impiego della cache per un dato periodo di tempo.  Il parametro <code>TotalCacheSize</code> cambia solo quando aggiungi cache al gateway.
La percentuale di richieste di lettura gestite dalla cache.	Utilizzare il parametro <code>CacheHitPercent</code> con la statistica <code>Average</code> .



Articolo di interesse	Come misurare
	Generalmente, desideri che il valore <code>CacheHitPercent</code> rimanga elevato.
Percentuale di cache sporca, ovvero che contiene contenuti che non sono stati caricati su AWS	Utilizzare i parametri <code>CachePercentDirty</code> con la statistica <code>Average</code> . Generalmente, desideri che il valore <code>CachePercentDirty</code> rimanga basso.

Per misurare la percentuale di una cache sporca per un gateway e tutti i suoi volumi

1. Apri la console all' CloudWatch 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 volumi, consulta [Comprensione dei parametri del gateway](#) e [Comprensione dei parametri dei volumi](#). Per ogni allarme, si specificano le condizioni che ne avvieranno lo stato. ALARM Gli indicatori di stato degli allarmi nella console Storage Gateway diventano rossi quando si ALARM trovano nello stato, 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, ti consigliamo di creare i seguenti CloudWatch allarmi:

- 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 Missing data treatment su. `notBreaching`

### Note

È possibile impostare un allarme di notifica sanitaria solo se il gateway aveva precedentemente ricevuto una notifica sanitaria. CloudWatch

Per i gateway su piattaforme VMware host con la modalità HA attivata, consigliamo anche questo CloudWatch allarme aggiuntivo:

- Notifiche di disponibilità: `AvailabilityNotifications >= 1` per 1 datapoint entro 5 minuti.  
Quando configuri questo allarme, imposta `Missing data treatment` 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 <a href="#">Creazione di un CloudWatch allarme personalizzato per il gateway</a> .
Non disponibile	Lo stato dell'allarme è sconosciuto. Scegliere <code>Unavailable</code> (Non disponibile) per visualizzare le informazioni sugli errori nella scheda <code>Monitoring</code> (Monitoraggio) .

## Creazione di CloudWatch allarmi consigliati per il tuo 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 volumi](#). 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`: creazione di allarmi
- `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
- `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
- `cloudwatch>DeleteAlarms`: eliminazione di allarmi

1. Aprire la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa/>.
2. Nel pannello 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 (AmazonSNS) 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'azione è una notifica inviata a un SNS argomento di Amazon. Puoi creare un SNS argomento Amazon quando crei un CloudWatch allarme. Per ulteriori informazioni su AmazonSNS, consulta [What is AmazonSNS?](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

## Per creare un CloudWatch allarme nella console Storage Gateway

1. Aprire la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa/>.
2. Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera creare un allarme.
3. Nella pagina dei dettagli del gateway, scegliere la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarme per aprire la CloudWatch console.
5. Usa la CloudWatch console per creare il tipo di allarme che desideri. Puoi creare i seguenti tipi di allarmi:
  - Allarme di soglia statica: un allarme basato su una soglia impostata per un parametro scelto. L'allarme entra ALARM nello stato quando la metrica supera la soglia per un determinato numero di periodi di valutazione.

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

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

Per creare un allarme di rilevamento delle anomalie, consulta [Creazione di un CloudWatch allarme basato sul rilevamento delle anomalie](#) nella Amazon CloudWatch User Guide.

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

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

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

Per creare un allarme composito, consulta [Creazione di un allarme composito](#) nella Amazon CloudWatch User Guide.

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

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

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

- Nel pannello di navigazione scegliere Gateway, quindi scegliere lo stato di allarme del gateway per cui si desidera visualizzare gli allarmi.

Per informazioni su come modificare o eliminare un avviso, consulta [Modificare o eliminare](#) un avviso. CloudWatch

#### Note

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

## Monitoraggio del gateway di volumi

Questa sezione illustra su come monitorare un gateway in una configurazione di volumi nella cache o di volumi archiviati, incluso il monitoraggio dei volumi associati al gateway e del buffer di caricamento. Lo usi AWS Management Console per visualizzare le metriche per il tuo 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. Per informazioni dettagliate in merito CloudWatch, consulta la [Amazon CloudWatch User Guide](#).

## Argomenti

- [Ottenere i log di Volume Gateway Health con Amazon CloudWatch Logs](#)
- [Utilizzo di Amazon CloudWatch Metrics](#)
- [Misurazione delle prestazioni tra l'applicazione il gateway](#)
- [Misurazione delle prestazioni tra il gateway e AWS](#)
- [Informazioni sui parametri dei volumi](#)

## Ottenere i log di Volume Gateway Health con Amazon CloudWatch Logs

Puoi utilizzare Amazon CloudWatch Logs per ottenere informazioni sullo stato di salute del tuo Volume Gateway e delle risorse correlate. Puoi utilizzare questi 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 High Availability (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 [Configurazione del gateway di volumi](#). 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 volumi](#).

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 gateway

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

2. Nel riquadro di navigazione a sinistra, scegli Gateway, quindi scegli il gateway per cui desideri configurare il gruppo di CloudWatch log.
3. Per Azioni, scegli Modifica informazioni sul gateway oppure nella scheda Dettagli, in Health logs e Not Enabled, scegli Configura gruppo di log per aprire la finestra di *CustomerGatewayName* dialogo 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 a sinistra, 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 Amazon.

## Utilizzo di Amazon CloudWatch Metrics

Puoi ottenere i dati di monitoraggio per il tuo gateway utilizzando l'API AWS Management Console o l' CloudWatchAPI. La console mostra una serie di grafici basati sui dati grezzi dell' CloudWatch API. Puoi anche utilizzare l' CloudWatch API tramite uno dei [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, GatewayName e VolumeId. Nella CloudWatch console, puoi utilizzare le Volume Metrics viste Gateway Metrics e per selezionare facilmente dimensioni specifiche del gateway e del volume. 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 che puoi usare.

CloudWatch Namespace	Dimensione	Descrizione
AWS/StorageGateway	GatewayId , GatewayName	<p>Queste dimensioni filtrano in base ai dati dei parametri che descrivono gli aspetti del gateway. Puoi identificare un gateway da usare specificando le dimensioni GatewayId e GatewayName .</p> <p>I dati di velocità di trasmissione effettiva e latenza di un gateway si basano su tutti i volumi nel gateway.</p> <p>I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.</p>
	VolumeId	<p>Questa dimensione filtra in base ai dati dei parametri specifici per un volume. Identifica un volume da usare tramite la relativa dimensione VolumeId.</p> <p>I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.</p>

L'utilizzo di parametri di gateway e volume è simile all'utilizzo di altri parametri di 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](#)

## Misurazione delle prestazioni tra l'applicazione il gateway

Il throughput 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. Se usi la statistica di aggregazione corretta, puoi usare parametri Storage Gateway per misurare questi valori.

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), utilizzate la statistica per la velocità effettiva dei dati (byte al secondo) e utilizzate la `Sum` statistica per le operazioni di input/output al secondo (IOPS). `Samples` Per ulteriori informazioni, consulta [Statistics](#) nella Amazon CloudWatch User Guide.

La tabella seguente contiene un riepilogo dei parametri e della statistica corrispondente che puoi usare per misurare throughput, latenza e operazioni di input/output al secondo tra le applicazioni e il gateway.

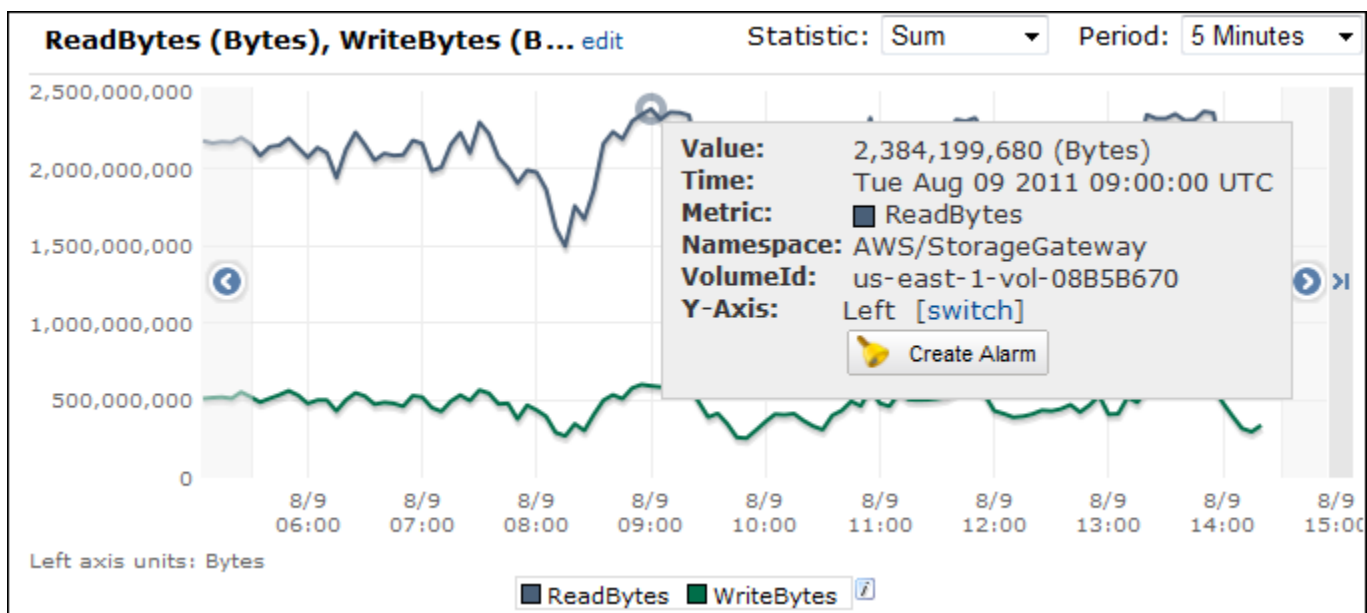
Articolo di interesse	Come misurare
Prestazioni	Utilizzare i parametri <code>ReadBytes</code> e <code>WriteBytes</code> con la statistica <code>Sum</code> CloudWatch . Ad esempio, il valore <code>Sum</code> del parametro <code>ReadBytes</code> in un periodo campione di 5 minuti diviso per 300 secondi restituisce il throughput come velocità in byte al secondo.
Latenza	Utilizzare i parametri <code>ReadTime</code> e <code>WriteTime</code> con la statistica <code>Average</code> CloudWatch . Ad esempio, il valore <code>Average</code> del parametro <code>ReadTime</code> restituisce la latenza per ogni operazione in un periodo di tempo campione.
IOPS	Utilizzare i parametri <code>ReadBytes</code> e <code>WriteBytes</code> con la statistica <code>Samples</code> CloudWatch . Ad esempio, il valore <code>Samples</code> del parametro <code>ReadBytes</code> in un periodo campione di 5 minuti diviso per 300 secondi restituisce le operazioni di input/output al secondo.

Per i grafici di latenza media e i grafici di dimensione media, la media viene calcolata sul numero totale di operazioni (lettura o scrittura, qualunque sia applicabile al grafico) completate durante il periodo.

Per misurare il throughput dei dati da un'applicazione a un volume

1. Apri la CloudWatch console all'[indirizzo https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Scegliere Metrics (Parametri), scegliere la scheda All metrics (Tutti i parametri) e quindi Storage Gateway.
3. Scegliere la dimensione Volume metrics (Parametri volume) e individuare il volume che si vuole usare.
4. Scegliere i parametri ReadBytes e WriteBytes.
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. Nei set di punti dati in ordine cronologico risultanti, uno per ReadBytes e uno per WriteBytes, dividere ogni punto dati per il periodo (in secondi) per ottenere il throughput in corrispondenza del punto campione. Il throughput totale è la somma dei throughput.

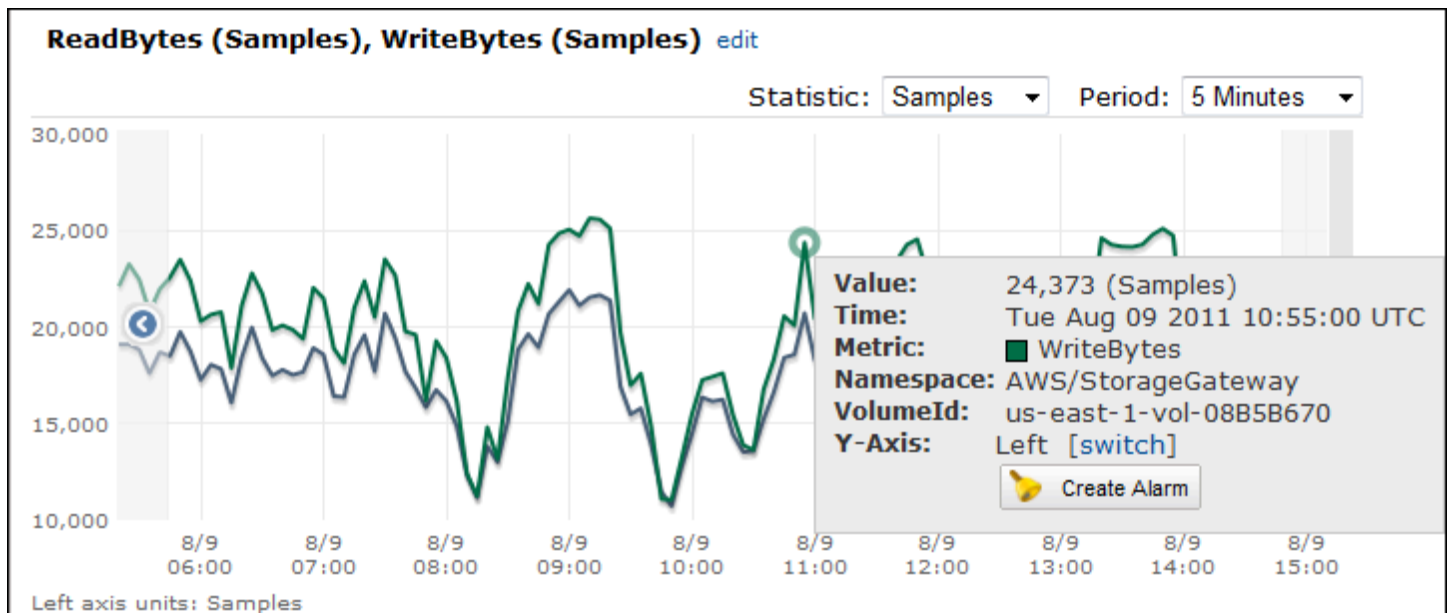
L'immagine seguente mostra i parametri ReadBytes e WriteBytes per un volume con la statistica Sum. Nell'immagine il cursore su un punto dati visualizza le informazioni sul punto dati, tra cui il valore e il numero di byte. Dividere il valore dei byte per il valore di Period (Periodo) (5 minuti) per ottenere il throughput dei dati in corrispondenza del punto campione. Per il punto evidenziato, il throughput di lettura è 2.384.199.680 byte diviso per 300 secondi, ovvero 7,6 megabyte al secondo.



Per misurare le operazioni di input/output dei dati al secondo da un'applicazione a un volume

1. Apri la CloudWatch console all'[indirizzo https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Scegliere Metrics (Parametri), scegliere la scheda All metrics (Tutti i parametri) e quindi Storage Gateway.
3. Scegliere la dimensione Volume metrics (Parametri volume) e individuare il volume che si vuole usare.
4. Scegliere i parametri ReadBytes e WriteBytes.
5. Scegliere un valore per Time Range (Intervallo di tempo).
6. Scegliere la statistica Samples.
7. Per Period (Periodo), scegliere un valore maggiore o uguale a 5 minuti.
8. Nei set di punti dati in ordine cronologico risultanti, uno per ReadBytes e uno per WriteBytes, dividere ogni punto dati per il periodo (in secondi) per ottenere le operazioni di input/output al secondo.

L'immagine seguente mostra i parametri ReadBytes e WriteBytes per un volume di storage con la statistica Samples. Nell'immagine il cursore su un punto dati visualizza le informazioni sul punto dati, tra cui il valore e il numero di campioni. Dividere il valore dei campioni per il valore di Period (Periodo) (5 minuti) per ottenere le operazioni al secondo in corrispondenza del punto campione. Per il punto evidenziato, il numero di operazioni di scrittura è 24.373 byte diviso per 300 secondi, ovvero 81 operazioni di scrittura al secondo.



## Misurazione delle prestazioni tra il 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 Storage Gateway. Questi tre valori possono essere misurati tramite i parametri Storage Gateway forniti quando usi la statistica di aggregazione corretta. La tabella seguente contiene un riepilogo dei parametri e della statistica corrispondente da usare per misurare velocità di trasmissione effettiva, latenza e operazioni di input/output al secondo (IOPS) tra il gateway e AWS.

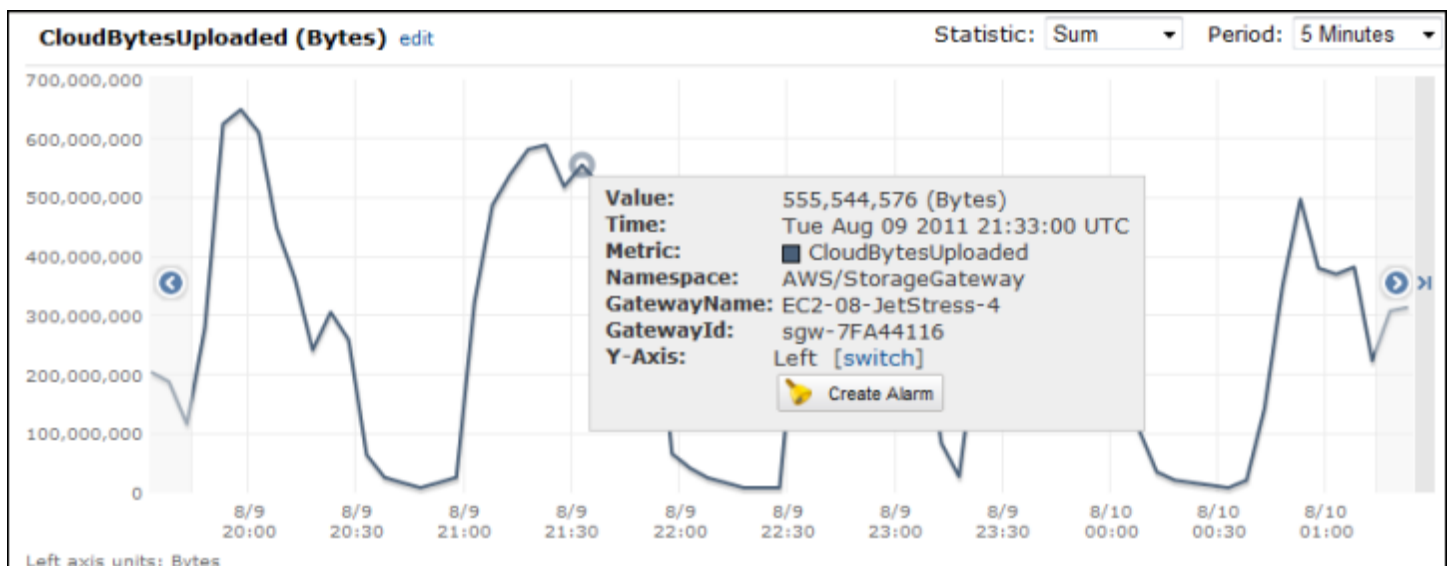
Articolo di interesse	Come misurare
Prestazioni	Utilizzare i parametri <code>ReadBytes</code> e <code>WriteBytes</code> con la statistica <code>Sum</code> <code>CloudWatch</code> . Ad esempio, il valore <code>Sum</code> del parametro <code>ReadBytes</code> in un periodo campione di 5 minuti diviso per 300 secondi restituisce il throughput come velocità in byte al secondo.
Latenza	Utilizzare i parametri <code>ReadTime</code> e <code>WriteTime</code> con la statistica <code>Average</code> <code>CloudWatch</code> . Ad esempio, il valore <code>Average</code> del parametro <code>ReadTime</code> restituisce la latenza per ogni operazione in un periodo di tempo campione.
IOPS	Utilizzare i parametri <code>ReadBytes</code> e <code>WriteBytes</code> con la statistica <code>Samples</code> <code>CloudWatch</code> . Ad esempio, il valore <code>Samples</code> del parametro <code>ReadBytes</code> in un periodo campione di 5 minuti diviso per 300 secondi restituisce le operazioni di input/output al secondo.
Throughput a AWS	Usa le <code>CloudBytesUploaded</code> metriche <code>CloudBytesDownload</code> ed <code>and</code> con la <code>Sum</code> <code>CloudWatch</code> statistica. Ad esempio, il <code>Sum</code> valore della <code>CloudBytesDownloaded</code> metrica su un periodo di campionamento di 5 minuti diviso per 300 secondi fornisce la velocità effettiva dal gateway in byte AWS al secondo.
Latenza dei dati verso AWS	Utilizzare il parametro <code>CloudDownloadLatency</code> con la statistica <code>Average</code> . Ad esempio, la statistica <code>Average</code> del parametro <code>CloudDownloadLatency</code> restituisce la latenza per ogni operazione.

Per misurare la velocità di caricamento dei dati da un gateway a AWS

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.

2. Scegliere Metrics (Parametri), scegliere la scheda All metrics (Tutti i parametri) e quindi Storage Gateway.
3. Scegliere la dimensione Gateway metrics (Parametri gateway) e individuare il volume che si vuole usare.
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 volume del gateway con la statistica Sum. Nell'immagine il cursore su un punto dati visualizza le informazioni sul punto dati, tra cui il valore e i 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, la velocità effettiva dal gateway a AWS è di 555.544.576 byte divisi per 300 secondi, ovvero 1,7 megabyte al secondo.



Per misurare la latenza per ogni operazione di un gateway

1. [Apri](https://console.aws.amazon.com/cloudwatch/) la console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>. CloudWatch

2. Scegliere Metrics (Parametri), scegliere la scheda All metrics (Tutti i parametri) e quindi Storage Gateway.
3. Scegliere la dimensione Gateway metrics (Parametri gateway) e individuare il volume che si vuole usare.
4. Scegliere i parametri ReadTime e WriteTime.
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.
8. Nei set di punti dati in ordine cronologico risultanti, uno per ReadTime e uno per WriteTime, aggiungere i punti dati nello stesso campione di tempo per ottenere la latenza totale in millisecondi.

Per misurare la latenza dei dati da un gateway a AWS

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Scegliere Metrics (Parametri), scegliere la scheda All metrics (Tutti i parametri) e quindi Storage Gateway.
3. Scegliere la dimensione Gateway metrics (Parametri gateway) e individuare il volume che si vuole usare.
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 il throughput di un gateway su AWS

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Scegliere Alarms (Allarmi).
3. Scegliere Create Alarm (Crea allarme) per avviare la procedura guidata di creazione allarme.
4. Scegliere la dimensione Storage Gateway e cercare il gateway da utilizzare.

5. Scegliere il parametro `CloudBytesUploaded`.
6. Per definire l'allarme, definire 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 MB per 60 minuti.
7. Configurare le operazioni da eseguire per lo stato di allarme. Ad esempio, è possibile scegliere di ricevere una notifica tramite e-mail.
8. 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/](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 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.

## Informazioni sui parametri dei volumi

Di seguito vengono fornite informazioni sui parametri Storage Gateway relativi a un volume di un gateway. Ogni volume di un gateway è associato a un set di parametri.

Alcuni parametri specifici dei volumi hanno lo stesso nome di certi parametri specifici dei gateway. Questi parametri rappresentano lo stesso tipo di misure, ma vengono definiti per il volume invece che per il gateway. Prima di iniziare, specifica se vuoi utilizzare un parametro di gateway o di volumi. In particolare, quando si utilizzano i parametri di volume, specifica l'ID per il volume di storage 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 usare per ottenere informazioni sui volumi di archiviazione.

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
AvailabilityNotification	Numero di notifiche di disponibilità inviate dal volume.  Unità: conteggio	Sì	Sì
CacheHitPercent	Percentuale delle operazioni di lettura dell'applicazione dal volume, fornite dalla cache. Il campione si riferisce al termine del periodo di reporting.  In assenza di operazioni di lettura dell'applicazione dal volume, questo parametro segnala il 100%.  Unità: percentuale	Sì	No
CachePercentDirty	Contributo del volume alla percentuale totale della cache del gateway non	Sì	Sì

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
	<p>conservata in AWS. Il campione si riferisce al termine del periodo di reporting.</p> <p>Usa il parametro <code>CachePercEntDirty</code> del gateway per visualizzare la percentuale totale della cache del gateway non conservata in AWS. Per ulteriori informazioni, consulta <a href="#">Comprendere i parametri del gateway</a>.</p> <p>Unità: percentuale</p>		

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
CachePercentUsed	<p>Contributo del volume all'utilizzo della percentuale totale dello storage della cache del gateway. Il campione si riferisce al termine del periodo di reporting.</p> <p>Usa il parametro CachePercentUsed del gateway per visualizzare la percentuale totale di utilizzo dello storage della cache del gateway. Per ulteriori informazioni, consulta <a href="#">Comprendere i parametri del gateway</a>.</p> <p>Unità: percentuale</p>	Sì	No
CloudBytesDownloaded	<p>Il numero di byte scaricati dal cloud sul volume.</p> <p>Unità: byte</p>	Sì	Sì
CloudBytesUploaded	<p>Il numero di byte caricati dal cloud sul volume.</p> <p>Unità: byte</p>	Sì	Sì

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
HealthNotification	Numero di notifiche di stato inviate dal volume.  Unità: conteggio	Sì	Sì
IoWaitPercent	La percentuale di IoWaitPercent unità attualmente utilizzate dal volume.  Unità: percentuale	Sì	Sì
MemTotalBytes	Percentuale di memoria totale attualmente utilizzata dal volume.  Unità: percentuale	Sì	No
MemoryUsage	Percentuale di memoria attualmente utilizzata dal volume.  Unità: percentuale	Sì	No

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
ReadBytes	<p>Numero totale di byte letti dalle applicazioni in locale durante il periodo di reporting.</p> <p>Usa questo parametro con la statistica Sum per misurare il throughput e con la statistica Samples per misurare le operazioni IOPS.</p> <p>Unità: byte</p>	Sì	Sì
ReadTime	<p>Numero totale di millisecondi dedicati allo svolgimento delle operazioni di lettura dalle applicazioni in locale durante il periodo di reporting.</p> <p>Usa questo parametro con la statistica Average per misurare la latenza.</p> <p>Unità: millisecondi</p>	Sì	Sì

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
UserCpuPercent	<p>Percentuale di unità di elaborazione della CPU allocate attualmente utilizzate dal volume.</p> <p>Unità: percentuale</p>	Sì	Sì
WriteBytes	<p>Numero totale di byte scritti nelle applicazioni in locale durante il periodo di reporting.</p> <p>Usa questo parametro con la statistica Sum per misurare il throughput e con la statistica Samples per misurare le operazioni IOPS.</p> <p>Unità: byte</p>	Sì	Sì

Parametro	Descrizione	Volumi nella cache	Volumi archiviati
<code>WriteTime</code>	<p>Numero totale di millisecondi dedicati allo svolgimento delle operazioni di scrittura dalle applicazioni in locale durante il periodo di reporting.</p> <p>Usa questo parametro con la statistic a Average per misurare la latenza.</p> <p>Unità: millisecondi</p>	Sì	Sì
<code>QueuedWrites</code>	<p>Il numero di byte in attesa di scrittura AWS, campionati alla fine del periodo di riferimento.</p> <p>Unità: byte</p>	Sì	Sì

# 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](#)
- [Gestione dei dischi locali per Storage Gateway](#)
- [Gestione della larghezza di banda per il gateway di volumi](#)
- [Gestione degli aggiornamenti del gateway](#)
- [Esecuzione di attività di manutenzione utilizzando la console locale](#)
- [Eliminazione del gateway e rimozione delle risorse associate](#)

## 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 si concentri sull'avvio e l'arresto del gateway utilizzando la Storage Gateway Management Console, è possibile interrompere il gateway anche utilizzando la console locale della macchina virtuale o lo Storage Gateway API. Quando accendi la macchina virtuale, ricorda di riavviare il gateway.

### Important

Se interrompi e avvii un EC2 gateway Amazon che utilizza lo storage temporaneo, il gateway sarà permanentemente 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](#).
- Storage Gateway API —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 di volumi

Per arrestare un gateway di volumi

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

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

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 su EC2 istanze Amazon utilizzano i EBS volumi Amazon come dischi locali.

### Argomenti

- [Determinazione della quantità di archiviazione su disco locale](#)
- [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:

- Gateway di volumi:
  - I gateway archiviati richiedono almeno un disco da usare come buffer di caricamento.
  - I gateway nella cache 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.

Storage locale	Descrizione	
Buffer di caricamento	Il buffer di caricamento fornisce un'area di gestione temporanea per i dati prima che il gateway	

Storage locale	Descrizione	
	carichi i dati in Amazon S3. Il gateway carica questi dati del buffer tramite una connessione Secure Sockets Layer () crittografata a. SSL AWS	
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'applicazione 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'applicazione 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 archiviazione fisica sottostanti sono rappresentate come un archivio dati in VMware. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando 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. Questo vale anche se il backup è una RAID configurazione meno performante 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.

## 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 Volume Gateways, quando il buffer di caricamento raggiunge la sua capacità, il volume passa allo stato impostato. **PASS THROUGH** In questo stato, i nuovi dati scritti dall'applicazione vengono conservati localmente ma non vengono caricati immediatamente. **AWS** Non è quindi possibile acquisire nuovi snapshot. Quando la capacità del buffer di caricamento si esaurisce, il volume passa allo stato successivo. **BOOTSTRAPPING** In questo stato, tutti i nuovi dati che sono stati resi persistenti localmente vengono caricati su. **AWS** Infine, il volume torna allo **ACTIVE** stato. Storage Gateway riprende quindi la normale sincronizzazione dei dati archiviati localmente con la copia archiviata in AWS ed è possibile iniziare a scattare nuove istantanee. Per ulteriori informazioni sullo stato dei volumi, consulta [Informazioni su stati e transizioni dei volumi](#).

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 riferimento si 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 ove 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

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

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 cache o buffer di caricamento a un gateway esistente, devi creare nuovi dischi sull'hypervisor host del gateway o sull'istanza Amazon. EC2 Non rimuovere o modificare le dimensioni dei dischi esistenti che sono già stati allocati come cache 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'host del gateway, sull'hypervisor 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 di EBS volumi Amazon per un'istanza Amazon, consulta [EBSi volumi Amazon](#) nella Amazon Elastic Compute Cloud User Guide for Linux Instances. Nei passaggi seguenti, configurerai questo disco come buffer di caricamento o archiviazione cache.

2. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
3. Nel riquadro di navigazione, scegliere Gateways.
4. Nell'elenco, cerca e seleziona il tuo gateway.
5. Dal menu Operazioni scegli Configura evento test.
6. Nella sezione Configura lo storage, 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 uno dei due UPLOADBUFFERo CACHESTORAGEdal menu a discesa Allocated a.

#### Note

UPLOADBUFFERè l'unica opzione disponibile per l'allocazione dei dischi sugli Stored Volume Gateway.

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

## Gestione della larghezza di banda per il gateway di volumi

È possibile limitare (o limitare) la velocità effettiva di caricamento dal gateway verso AWS o la velocità effettiva di download dal gateway. AWS 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 programmazione utilizzando lo Storage Gateway API (vedere [UpdateBandwidthRateLimit](#)) o un AWS Software Development Kit (SDK). AWS Management Console 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 banda non sono attualmente supportati per Amazon FSx File Gateway.

## 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 a <https://console.aws.amazon.com/storagegateway/casa>.
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 a <https://console.aws.amazon.com/storagegateway/casa>.
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, inserisci **59** il minuto finale del primo intervallo. Inserisci **00** per 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

bandwidth-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 utilizzando il 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, devi fornire l'endpoint del servizio, il gateway Amazon Resource Name (ARN) e i limiti di upload e download. 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 bandwidth.\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 utilizzare il codice di esempio, è necessario avere familiarità con l'esecuzione di un .NET applicazione console. 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 il 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, devi fornire l'endpoint del servizio, il gateway Amazon Resource Name (ARN) e i limiti di upload e download. 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 bandwidth.\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, devi fornire il gateway Amazon Resource Name (ARN) e i limiti di upload e download.

```
<#
.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

Storage Gateway è costituito da un componente di servizi cloud gestiti e da un componente di appliance gateway che puoi distribuire in locale o su un'EC2istanza Amazon nel cloud. AWS Entrambi i componenti ricevono aggiornamenti regolari. Gli argomenti di questa sezione descrivono la frequenza di questi aggiornamenti, come vengono applicati e come configurare le impostazioni relative agli aggiornamenti sui gateway della distribuzione.

### Important

È necessario trattare l'appliance Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare in alcun modo la sua installazione. Il tentativo di installare o aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del AWS gateway (ad esempio, SSM o strumenti dell'hypervisor) può causare il malfunzionamento del gateway.

## Frequenza di aggiornamento e comportamento previsto

AWS aggiorna il componente dei servizi cloud in base alle esigenze senza causare interruzioni ai gateway implementati. I dispositivi gateway distribuiti ricevono aggiornamenti di manutenzione mensili. Gli aggiornamenti di manutenzione mensili possono includere aggiornamenti del sistema operativo e del software, correzioni per migliorare la stabilità, le prestazioni e la sicurezza e l'accesso a nuove funzionalità. Tutti gli aggiornamenti sono cumulativi e, se applicati, aggiornano i gateway alla versione corrente. Per informazioni sulle modifiche specifiche incluse in ogni aggiornamento, vedere le [Volume Gateway Appliance](#).



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

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

#### Note

A volte gli aggiornamenti urgenti vengono applicati in base alla pianificazione della finestra di manutenzione, anche se gli aggiornamenti di manutenzione regolari sono disattivati.

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

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

## Attiva o disattiva gli aggiornamenti di manutenzione

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

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

#### Note

La procedura seguente descrive come attivare o disattivare gli aggiornamenti del gateway utilizzando la console Storage Gateway. Per modificare questa impostazione a livello

di codice utilizzando ilAPI, vedere [UpdateMaintenanceStartTime](#)Storage Gateway API Reference.

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

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

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

## Modifica la pianificazione della finestra di manutenzione del gateway

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

### Note

La procedura seguente descrive come modificare la pianificazione della finestra di manutenzione utilizzando la console Storage Gateway. Per modificare questa impostazione a livello di codice utilizzando ilAPI, vedere [UpdateMaintenanceStartTime](#)Storage Gateway API Reference.

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

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri configurare gli aggiornamenti di manutenzione.

3. Scegli Azioni, quindi scegli Modifica impostazioni di manutenzione.
4. In Ora di inizio della finestra di manutenzione, procedi come segue:
  - a. Per Pianificazione, scegli Settimanale o Mensile per impostare la cadenza della finestra di manutenzione.
  - b. Se scegli Settimanale, modifica i valori di Giorno della settimana e Ora per impostare il momento specifico durante ogni settimana in cui inizierà la finestra di manutenzione.

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

#### Note

Il valore massimo che può essere impostato per il giorno del mese è 28. Non è possibile impostare il programma di manutenzione in modo che inizi nei giorni dal 29 al 31.

Se ricevi un errore durante la configurazione di questa impostazione, è possibile che il software del gateway non sia aggiornato. Valuta la possibilità di aggiornare prima il gateway manualmente e poi di riprovare a configurare la pianificazione della finestra di manutenzione.

5. Al termine, scegli Salva le modifiche.

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

## Esecuzione di attività di manutenzione utilizzando la console locale

Con la console locale dell'host è possibile svolgere le seguenti operazioni di manutenzione. Le attività della console locale possono essere eseguite sull'host VM o sull'EC2istanza Amazon. 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 Linux Kernel-based Virtual Machine (). KVM

## 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 Storage Gateway AWS , dal quale è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configura un SOCKS proxy per il tuo gateway	<a href="#">Instradamento del gateway in locale tramite un proxy.</a>
Configurare la rete	<a href="#">Configurazione di rete del gateway.</a>
Verificare la connettività di rete	<a href="#">Verifica della connessione del gateway a Internet.</a>
Gestione dell'ora della VM	<a href="#">Sincronizzazione dell'ora della VM associata al gateway.</a>
Esecuzione dei comandi della console Storage Gateway	<a href="#">Esecuzione di comandi Storage Gateway sulla console locale.</a>
Visualizzare lo stato delle risorse di sistema	<a href="#">Visualizzazione dello stato relativo alle risorse di sistema del gateway.</a>

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 a <https://console.aws.amazon.com/storagegateway/casa>.
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

Volume Gateway e Tape Gateways supportano la configurazione di un proxy Socket Secure versione 5 (SOCKS5) tra il gateway locale e AWS.

### Note

L'unica configurazione proxy supportata è SOCKS5.

Se il gateway deve utilizzare un server proxy per comunicare con Internet, è necessario configurare le impostazioni SOCKS proxy 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 mostra come configurare il SOCKS proxy per Volume Gateway e Tape Gateway.

Per configurare un SOCKS5 proxy per Volume e Tape Gateway

1. Accedere alla console locale del gateway.
  - VMwareESXi— per ulteriori informazioni, vedere [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, vedere [Accesso alla console locale del gateway con Linux KVM](#).
2. Dal menu principale AWS Storage Gateway - Configuration, immettere il numero corrispondente per selezionare SOCKSProxy Configuration.
3. Dal menu AWS Storage Gateway SOCKS Proxy Configuration, immettere il numero corrispondente per eseguire una delle seguenti attività:

Per eseguire questa operazione	e eseguire questa operazione
Configurare un proxy SOCKS	<p>Inserisci il numero corrispondente per selezionare Configure SOCKS Proxy.</p> <p>Specificare un nome host e una porta per completare la configurazione.</p>
Visualizza la configurazione attuale del SOCKS proxy	<p>Immettere il numero corrispondente per selezionare Visualizza la configurazione attuale SOCKS del proxy.</p> <p>Se un SOCKS proxy non è configurato, SOCKS Proxy not configured viene visualizzato il messaggio. Se è configurato un SOCKS</p>

Per eseguire questa operazione	eseguire questa operazione
	proxy, vengono visualizzati il nome host e la porta del proxy.
Rimuovere una configurazione SOCKS proxy	<p>Immettere il numero corrispondente per selezionare Rimuovi configurazione SOCKS proxy.</p> <p>Viene visualizzato il messaggio SOCKS Proxy Configuration Removed</p>

4. Riavvia la macchina virtuale per applicare la configurazione HTTP.

## Configurazione di rete del gateway

La configurazione di rete predefinita per il gateway è Dynamic Host Configuration Protocol (DHCP). 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, vedere [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, vedere [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 operazione	eseguire questa operazione
Descrivere la scheda di rete	



Per eseguire questa operazione	eseguire questa operazione
	<p>Immettere il numero corrispondente per selezionare Descrivi adattatore.</p> <p>Viene visualizzato un elenco di nomi di schede e viene richiesto di digitare un nome per la scheda, ad esempio <b>eth0</b>. Se la scheda specificata è in uso, vengono mostrate le seguenti informazioni:</p> <ul style="list-style-type: none"><li>• Indirizzo di controllo dell'accesso ai media (MAC)</li><li>• Indirizzo IP</li><li>• Netmask</li><li>• Indirizzo IP del gateway</li><li>• DHCPstato attivato</li></ul> <p>I nomi degli adattatori elencati qui vengono utilizzati quando si configura un indirizzo IP statico o si imposta l'adattatore predefinito del gateway.</p>
Configurare DHCP	<p>Inserisci il numero corrispondente per selezionare Configura DHCP.</p> <p>Ti viene richiesto di configurare l'interfaccia di rete da utilizzare. DHCP</p>

## Per eseguire questa operazione


Configurare un indirizzo IP statico per il gateway

## eseguire questa operazione

Inserisci 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 primario del Domain Name Service (DNS)
- DNSIndirizzo 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](#).

Se il gateway utilizza più di un'interfaccia di rete, è necessario impostare tutte le interfacce

Per eseguire questa operazione	eseguire questa operazione
	<p>attivate in modo che DHCP utilizzino indirizzi IP statici.</p> <p>Ad esempio, supponiamo che la macchina virtuale 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.</p> <p>Se entrambe le interfacce sono inizialmente impostate per utilizzare indirizzi IP statici e successivamente si imposta il gateway da utilizzare DHCP, verranno utilizzate entrambe le interfacce. DHCP</p>

Per eseguire questa operazione	eseguire questa operazione
Configura un nome host per il gateway	<p>Immettere il numero corrispondente per selezionare Configura nome host.</p> <p>Ti viene richiesto di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o ne acquisirà uno automaticamente tramite o r. DHCP DNS</p> <p>Se si seleziona Statico, viene richiesto di fornire un nome host statico, ad esempio. <code>testgateway.example.com</code> Entra y per applicare la configurazione.</p> <div data-bbox="829 800 1507 1255"><p> <b>Note</b></p><p>Se configuri un nome host statico per il gateway, assicurati che il nome host fornito si trovi nel dominio a cui è unito il gateway. È inoltre necessario creare un record A nel DNS sistema che punti l'indirizzo IP del gateway al relativo nome host statico.</p></div>

Per eseguire questa operazione	eseguire questa operazione
<p>Reimposta tutta la configurazione di rete del gateway su DHCP</p>	<p>Inserisci il numero corrispondente per selezionare Reimposta tutto su DHCP.</p> <p>Tutte le interfacce di rete sono impostate per l'uso. DHCP</p> <div data-bbox="829 541 1507 999" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> <b>Important</b></p><p>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 <a href="#">Spegnimento della macchina virtuale gateway</a>.</p></div>
<p>Impostare l'adattatore di routing predefinito del gateway</p>	<p>Immettere il numero corrispondente per selezionare Imposta scheda predefinita.</p> <p>Compaiono le schede disponibili per il gateway e viene richiesto di selezionarne una, ad esempio <b>eth0</b>.</p>
<p>Visualizza la configurazione del DNS tuo gateway</p>	<p>Inserisci il numero corrispondente per selezionare Visualizza DNS configurazione.</p> <p>Vengono visualizzati gli indirizzi IP dei DNS name server primari e secondari.</p>

Per eseguire questa operazione	eseguire questa operazione
Visualizzare le tabelle di routing	<p>Immettere il numero corrispondente per selezionare Visualizza instradamenti.</p> <p>Viene visualizzato l'instradamento predefinito del gateway.</p>

## 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.
  - VMwareESXi— per ulteriori informazioni, vedere [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, vedere [Accesso alla console locale del gateway con Linux KVM](#).
2. Dal menu principale AWS Storage Gateway: configurazione, immettere il numero corrispondente per selezionare Verifica connettività di rete.

Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e procedere Regione AWS come descritto nei passaggi seguenti.

3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere [AWS Storage Gateway endpoint e quote nel](#). Riferimenti generali di AWS

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

Messaggio	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.

Per un gateway distribuito su VMwareESXi, è sufficiente impostare l'ora dell'host dell'hypervisor e sincronizzare l'ora della macchina virtuale con l'host per evitare variazioni di tempo. 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 VMware ESXi locale, vedere. [Accesso alla console locale del Gateway con VMware ESXi](#)
  - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare [Accesso alla console locale del gateway con Microsoft Hyper-V](#).
  - Per ulteriori informazioni sull'accesso alla console KVM locale, vedere. [Accesso alla console locale del gateway con Linux KVM](#)
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Console del Gateway.
  3. Dal prompt dei comandi della console del gateway, immettere **h**.

La console visualizza il AVAILABLECOMMANDSmenu, che elenca i comandi disponibili:

Comando	Funzione
dig	Raccogli l'output da dig per la DNS risoluzione dei problemi.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete. <div data-bbox="836 1228 1510 1648" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>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 <a href="#">Configurazione della rete del gateway</a>.</p> </div>
ip	Mostra/manipola routing, dispositivi e tunnel.



Comando	Funzione
	<p> <b>Note</b></p> <p>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 <a href="#">Configurazione della rete del gateway</a>.</p>
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e. NAT
ncport	Verifica la connettività a una TCP porta 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.

Comando	Funzione
sslcheck	Restituisce l'output con l'emittente del certificato
	<div data-bbox="834 352 1510 953" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> <b>Note</b></p> <p>Storage Gateway utilizza la verifica dell'emittente del certificato e non supporta l'ispezione SSL. Se questo comando restituisce un emittente diverso da <code>aws-appliance@amazon.com</code>, è probabile che sia un'applicazione che esegue un'ispezione ssl. In tal caso, si consiglia di ignorare l'ispezione SSL per l'appliance Storage Gateway.</p> </div>
tcptraceroute	Raccogli l'output del traceroute sul TCP traffico 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 ulteriori informazioni su un comando, digitate + **man** *command name* al prompt dei comandi.

## Visualizzazione dello stato relativo alle risorse di sistema del gateway

All'avvio del gateway, ne controlla i CPU core virtuali, la dimensione del volume root e. RAM Quindi stabilisce se tali risorse di sistema sono sufficienti per il corretto funzionamento del gateway. I risultati di questi controlli sono riportati nella console locale del gateway.

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedere alla console locale del gateway:
  - Per ulteriori informazioni sull'accesso alla VMware ESXi console, vedere. [Accesso alla console locale del Gateway con VMware ESXi](#)

- Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare [Accesso alla console locale del gateway con Microsoft Hyper-V](#).
  - Per ulteriori informazioni sull'accesso alla console KVM locale, vedere. [Accesso alla console locale del gateway con Linux KVM](#)
2. Nel menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero seriale corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

Ogni risorsa visualizza [OK], [WARNING] o [FAIL], che indica 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

Per impostazione predefinita, Storage Gateway è configurato per utilizzare il tipo di adattatore di rete E1000, ma è possibile riconfigurare il gateway per utilizzare l'adattatore 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'utilizzo dell'adattatore di rete VMXNET3](#)
- [Configurazione del gateway per più utenti NICs](#)

### Configurazione del gateway per l'utilizzo dell'adattatore di rete VMXNET3

Storage Gateway supporta il tipo di scheda di rete E1000 sia VMware ESXi negli host hypervisor Microsoft Hyper-V che negli host hypervisor Microsoft. Tuttavia, il tipo di scheda di rete VMXNET3 (10 GbE) è supportato solo nell'VMwareESXi hypervisor. Se il gateway è ospitato su un VMware ESXi hypervisor, è possibile riconfigurarli per utilizzare il tipo di adattatore (VMXNET3 10 GbE). Per ulteriori informazioni su questi adattatori, vedere [Scelta di un adattatore di rete per la macchina virtuale](#) sul sito Web Broadcom (). VMware

#### Important

Per effettuare la selezione VMXNET3, il tipo di sistema operativo guest deve essere Altro Linux64.

Di seguito sono riportati i passaggi da seguire per configurare il gateway per l'utilizzo dell'adattatore: VMXNET3

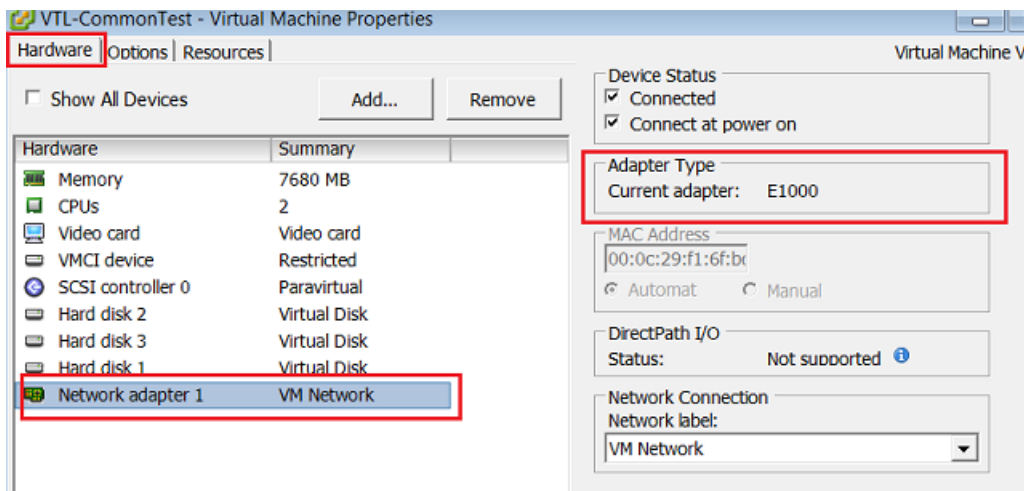
1. Rimuovere la scheda E1000 predefinita.
2. Aggiungere l'VMXNET3 adattatore.
3. Riavviare il gateway.
4. Configurare la scheda per la rete.

Seguono informazioni dettagliate su ogni passaggio.

Per rimuovere l'adattatore E1000 predefinito e configurare il gateway per l'utilizzo dell'VMXNET3 adattatore

1. In VMware, aprire il menu contestuale (fai clic con il pulsante destro del mouse) del gateway e scegli Modifica impostazioni.
2. Nella finestra Virtual Machine Properties (Proprietà macchina virtuale), selezionare la scheda Hardware (Hardware).

- Per Hardware, scegliere Network adapter (Scheda di rete). Nella sezione Adapter Type (Tipo di scheda) è riportata l'attuale scheda E1000, Sostituirai questo adattatore con l'VMXNET3adattatore.



- 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 eseguire contemporaneamente l'E1000 e gli adattatori di VMXNET3 rete nel gateway, non è consigliabile farlo perché può causare problemi di rete.

- Scegliere Add (Aggiungi) per avviare la procedura guidata di aggiunta dell'hardware.
- Selezionare prima Ethernet Adapter (Scheda Ethernet) e poi Next (Avanti).
- Nel corso della procedura guidata, scegliere **VMXNET3** come Adapter Type (Tipo di scheda), quindi selezionare Next (Avanti).
- Nella procedura guidata delle proprietà della macchina virtuale, verifica nella sezione Tipo di adattatore che Current Adapter sia impostato su VMXNET3, quindi scegli OK.
- Nel VMware VSphere client, spegni il gateway.
- Nel VMware VSphere client, riavvia 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 VSphere client, scegli 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. Alla richiesta, inserisci il numero corrispondente per selezionare Reimposta tutto suDHCP, quindi inserisci **y** (se sì) alla richiesta per impostare tutti gli adattatori per utilizzare Dynamic Host Configuration Protocol (). DHCP Tutti gli adattatori disponibili sono impostati per l'uso. 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 [connessione gateway a Internet](#).

## Configurazione del gateway per più utenti NICs

Se configuri il gateway per utilizzare più adattatori di rete (NICs), è possibile 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 di mantenere i SCSI target i e gli iniziatori che si connettono ad essi in una rete isolata diversa dalla rete con cui comunica il gateway. AWS

In un tipico caso di utilizzo con più adattatori, un adattatore è configurato come route con cui il gateway comunica AWS (ovvero come gateway predefinito). Ad eccezione di questo adattatore, gli iniziatori devono trovarsi nella stessa sottorete dell'adattatore che contiene le destinazioni i a cui si connettono. SCSI 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 e SCSI AWS il traffico per quella destinazione 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 utenti NICs in un host VMware ESXi](#)
- [Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host](#)

## Esecuzione di attività sulla console EC2 locale di Amazon

Alcune attività di manutenzione richiedono l'accesso alla console locale quando si esegue un gateway distribuito su un'EC2istanza Amazon. Questa sezione descrive come accedere alla console locale ed eseguire attività di manutenzione.

### Argomenti

- [Accesso alla console locale di Amazon EC2 Gateway](#)
- [Instradamento del gateway distribuito EC2 tramite un proxy HTTP](#)
- [Verifica 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 di Amazon EC2 Gateway

Puoi connetterti alla tua EC2 istanza Amazon utilizzando un client Secure Shell (SSH). Per informazioni dettagliate, consulta [Connect to Your Instance](#) nella Amazon EC2 User Guide. Per connetterti in questo modo, avrai bisogno della SSH key pair specificata al momento del lancio dell'istanza. Per informazioni sulle coppie di EC2 chiavi Amazon, consulta [Amazon EC2 Key Pairs](#) nella Amazon EC2 User Guide.

### Accedere alla console locale del gateway

1. Accedere alla tua console locale. Se ti connetti alla tua EC2 istanza da un computer Windows, accedi come amministratore.
2. Dopo aver effettuato l'accesso, viene visualizzato il menu principale Configurazione di Storage Gateway AWS , dal quale è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configura un SOCKS proxy per il tuo gateway	<a href="#">Instradamento del gateway distribuito EC2 tramite un proxy HTTP</a>
Verificare la connettività di rete	<a href="#">Verifica della connettività di rete del gateway</a>
Esecuzione dei comandi della console Storage Gateway	<a href="#">Esecuzione di comandi Storage Gateway sulla console locale</a>
Visualizzare un controllo delle risorse di sistema	<a href="#">Visualizzazione dello stato relativo alle risorse di sistema del gateway.</a>

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

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

## Instradamento del gateway distribuito EC2 tramite un proxy HTTP

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

Se il gateway deve utilizzare un server proxy per comunicare con Internet, è necessario configurare le impostazioni HTTP proxy 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 HTTP proxy.

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 di Amazon EC2 Gateway](#).
2. Dal menu principale AWS Appliance Activation - Configuration, immettere il numero corrispondente per selezionare Configure Proxy. HTTP
3. Dal menu di configurazione del HTTP proxy di attivazione dell'AWS appliance, immettete il numero corrispondente all'operazione che desiderate eseguire:



- Configura HTTP proxy: sarà necessario fornire un nome host e una porta per completare la configurazione.
- Visualizza la configurazione attuale del HTTP proxy: se un HTTP proxy non è configurato, HTTP Proxy not configured viene visualizzato il messaggio. Se è configurato un HTTP proxy, vengono visualizzati il nome host e la porta del proxy.
- Rimuovere una configurazione HTTP proxy: HTTP Proxy Configuration Removed viene visualizzato il messaggio.

## Verifica della connettività di rete del gateway

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

Per testare la connettività del gateway

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

Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e procedere Regione AWS come descritto nei passaggi seguenti.

3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere [AWS Storage Gateway endpoint e quote nel](#). Riferimenti generali di AWS

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

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

All'avvio del gateway, verifica i CPU core virtuali, la dimensione del volume root e. 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 di Amazon EC2 Gateway](#).
2. Nel menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero seriale corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

Ogni risorsa visualizza [OK], [WARNING] o [FAIL], indicando 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

Messaggio	Descrizione
	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 di Amazon EC2 Gateway](#).
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Console del Gateway.
3. Dal prompt dei comandi della console del gateway, immettere h.

La console visualizza il AVAILABLECOMMANDSmenu, che elenca i comandi disponibili:

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

Comando	Funzione
	<p> <b>Note</b></p> <p>Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata.</p>
ip	<p>Mostra/manipola routing, dispositivi e tunnel.</p> <p> <b>Note</b></p> <p>Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata.</p>
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e. NAT
ncport	Verifica la connettività a una TCP porta 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.
sslcheck	Verifica la SSL validità per la risoluzione dei problemi di rete.

Comando	Funzione
tcptraceroute	Raccogli l'output del traceroute sul TCP traffico 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, puoi trovare informazioni su come accedere alla console locale della macchina virtuale utilizzando Linux Kernel-based Virtual Machine (KVM) VMware ESXi e Microsoft Hyper-V Manager.

### Argomenti

- [Accesso alla console locale del gateway con Linux KVM](#)
- [Accesso alla console locale del Gateway con VMware ESXi](#)
- [Accesso alla console locale del gateway con Microsoft Hyper-V](#)

## Accesso alla console locale del gateway con Linux KVM

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

Per accedere alla console locale del gateway con KVM

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

```
# virsh list
```

Puoi scegliere disponibile VMs per Id.

```
[[root@localhost vms]# virsh list
 Id   Name           State
-----
 7    SGW_KVM        running

[[root@localhost vms]# virsh console 7
```

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

```
# virsh console VM_Id
```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

3. Per ottenere le credenziali predefinite per accedere alla console locale, consulta [Accedere alla console locale utilizzando credenziali predefinite](#).
4. Dopo aver effettuato l'accesso, è possibile attivare e configurare il gateway.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.3.32
#####

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

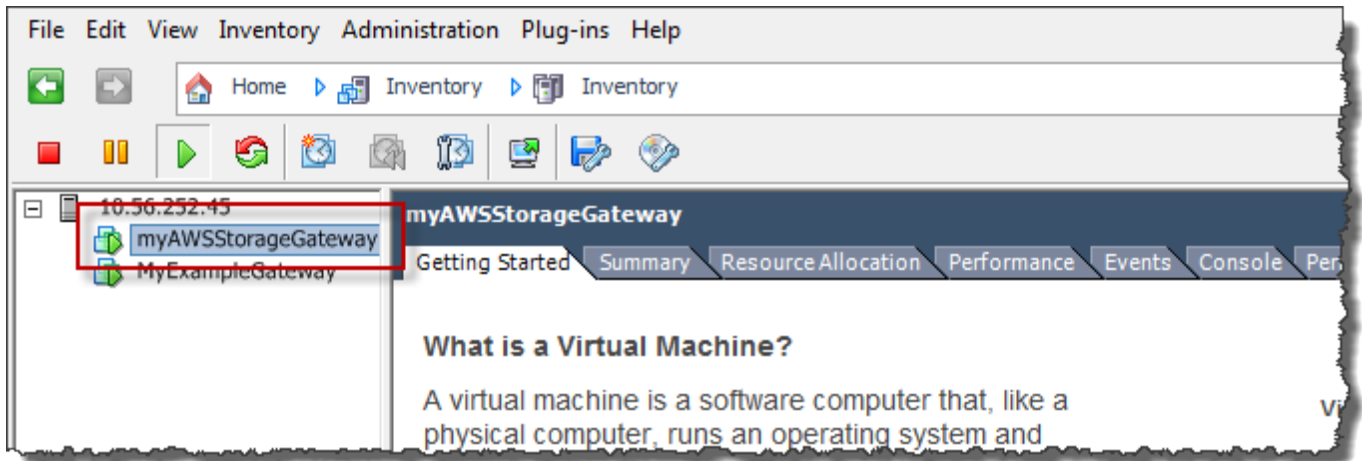
## Accesso alla console locale del Gateway con VMware ESXi

Per accedere alla console locale del gateway con VMware ESXi

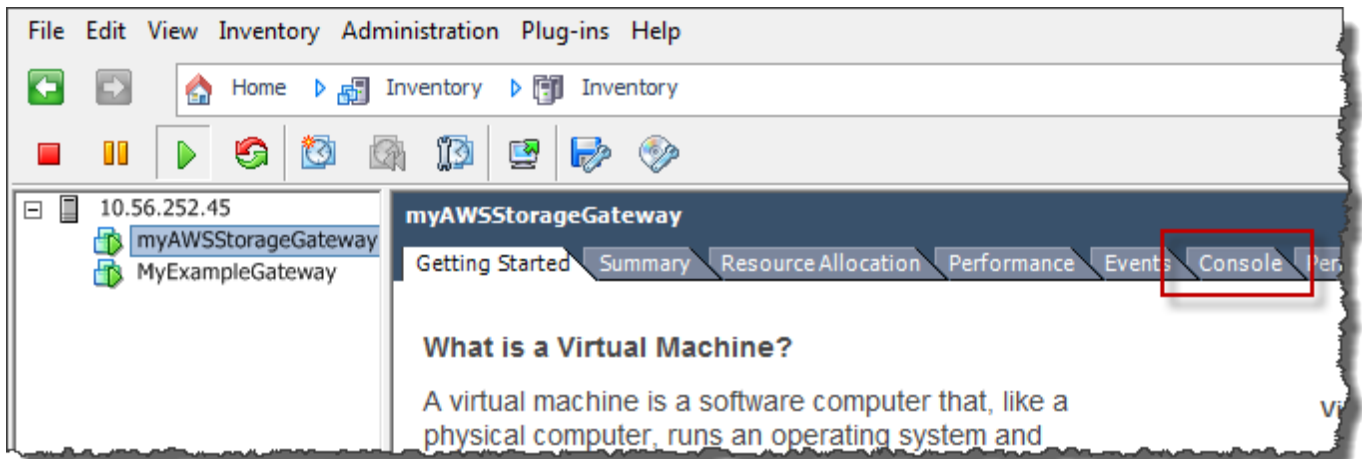
1. Nel VMware vSphere client, seleziona la tua macchina virtuale gateway.
2. Verifica che il gateway sia attivo.

### 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.



```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Per accedere tramite le credenziali predefinite, continua con la procedura [Accedere alla console locale utilizzando credenziali predefinite](#).

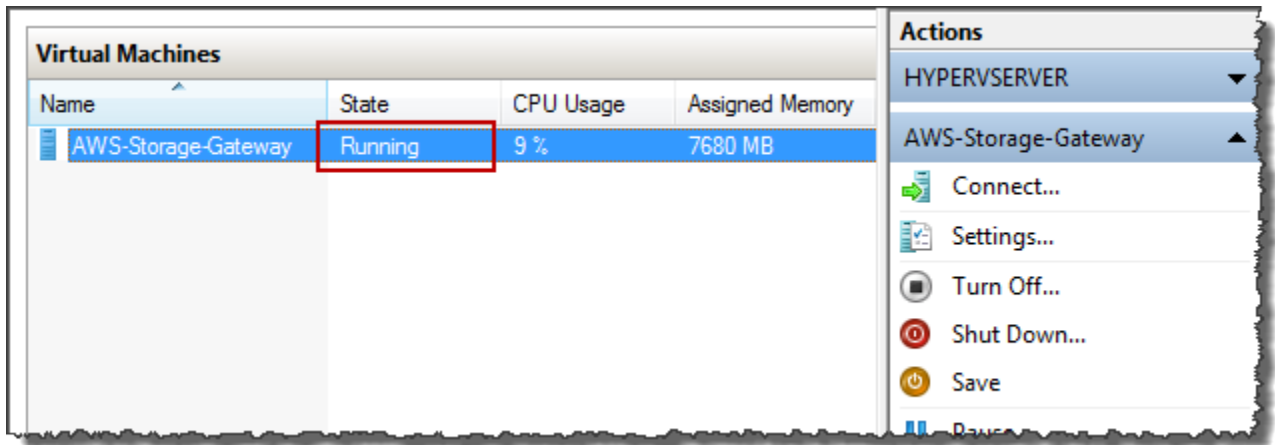
## Accesso alla console locale del gateway con Microsoft Hyper-V

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.

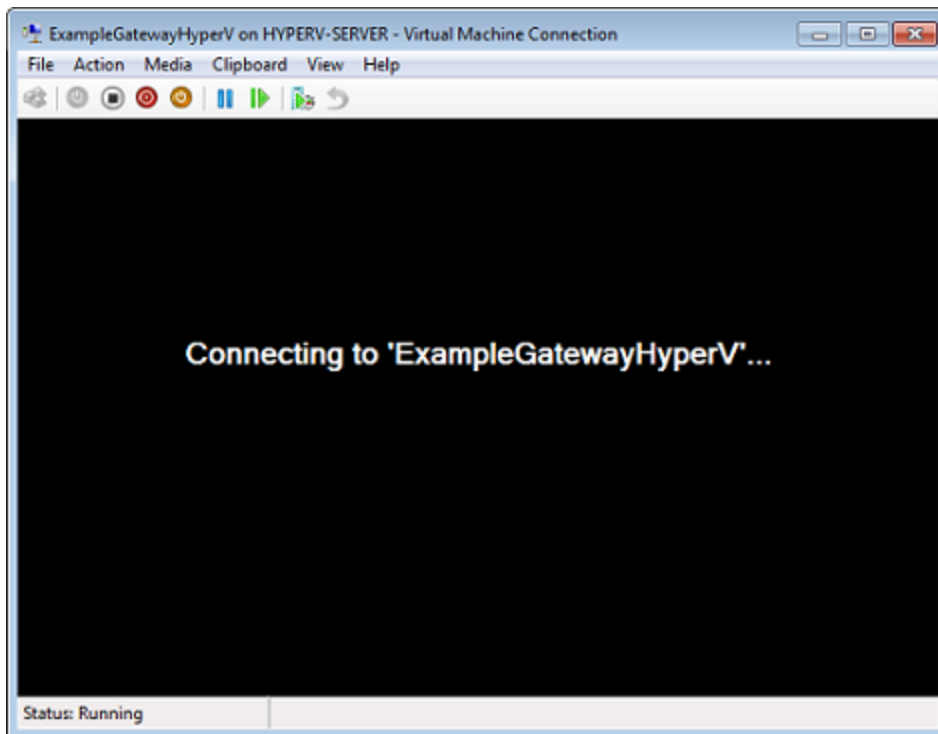
### Note

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.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

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 utenti NICs in un host VMware ESXi](#)
- [Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host](#)

## Configurazione del gateway per più utenti NICs in un host VMware ESXi

La procedura seguente presuppone che la macchina virtuale gateway abbia già definito un adattatore di rete e descrive come aggiungere un adattatore. VMware ESXi

Per configurare il gateway per l'utilizzo di un adattatore di rete aggiuntivo nell'host VMware ESXi

1. Arresta il gateway.
2. Nel VMware vSphere client, seleziona la tua VM gateway.

Per questa procedura, la macchina virtuale può rimanere attiva.

3. Nel client, apri il menu contestuale (clic con il pulsante destro del mouse) per la VM del gateway e scegli Edit Settings (Modifica impostazioni).
4. Nella scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), scegli Add (Aggiungi) per aggiungere un dispositivo.
5. Segui la procedura guidata Add Hardware (Aggiungi hardware) per aggiungere una scheda di rete.

- a. Nel riquadro Device Type (Tipo di dispositivo), scegli Ethernet Adapter (Scheda Ethernet) per aggiungere una scheda, quindi scegli Next (Avanti).
- b. Nel riquadro Network Type (Tipo di rete), assicurati che Connect at power on (Connetti all'accensione) sia selezionato per Type (Tipo), quindi scegli Next (Avanti).

Si consiglia di utilizzare l'adattatore di VMXNET3 rete con Storage Gateway. Per ulteriori informazioni sui tipi di adattatore che potrebbero apparire nell'elenco degli adattatori, vedere Tipi di adattatori di rete nella [documentazione di ESXi and vCenter Server](#).

- c. Nel riquadro Ready to Complete (Pronto al completamento), rivedi le informazioni, quindi scegli Finish (Fine).
6. Scegli la scheda Riepilogo della VM, quindi scegli Visualizza tutto accanto alla casella Indirizzo IP. Nella finestra Indirizzi IP macchina virtuale vengono visualizzati tutti gli indirizzi IP da poter utilizzare per accedere al gateway. Verifica che un secondo indirizzo IP sia elencato per il gateway.

#### Note

Potrebbero volerci alcuni istanti prima che le modifiche della scheda diventino effettive e che le informazioni di riepilogo della VM si aggiornino.

7. Nella console Storage Gateway, accendere il gateway.
8. Nel riquadro Navigazione della console Storage Gateway, scegliere Gateway, quindi scegliere il gateway a cui aggiungere la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

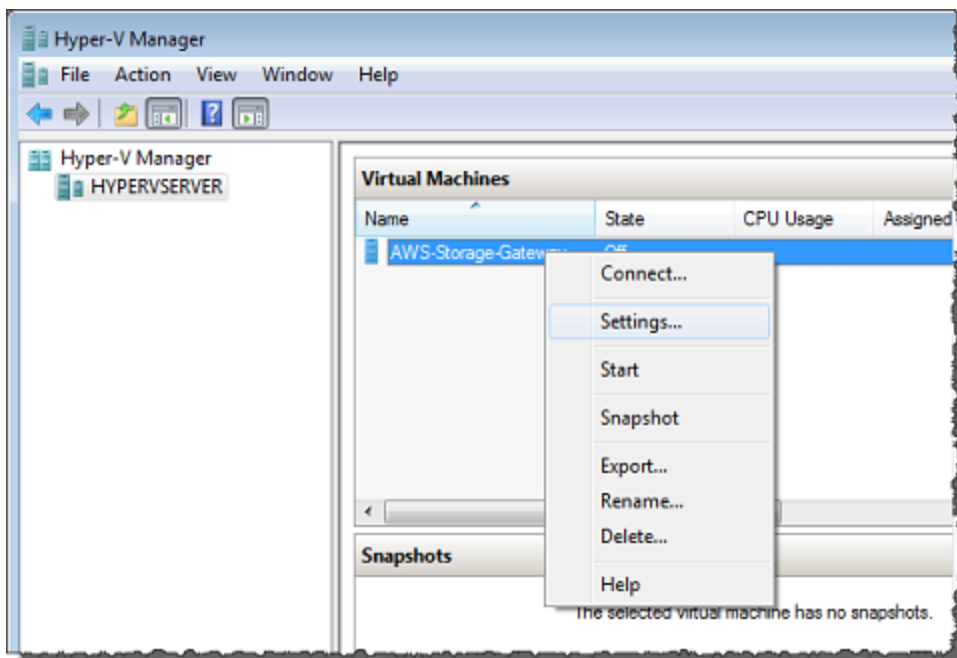
Per informazioni sulle attività della console locale comuni a VMware Hyper-V e agli KVM host, vedere [Esecuzione delle operazioni sulla console locale della VM di](#)

## Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host

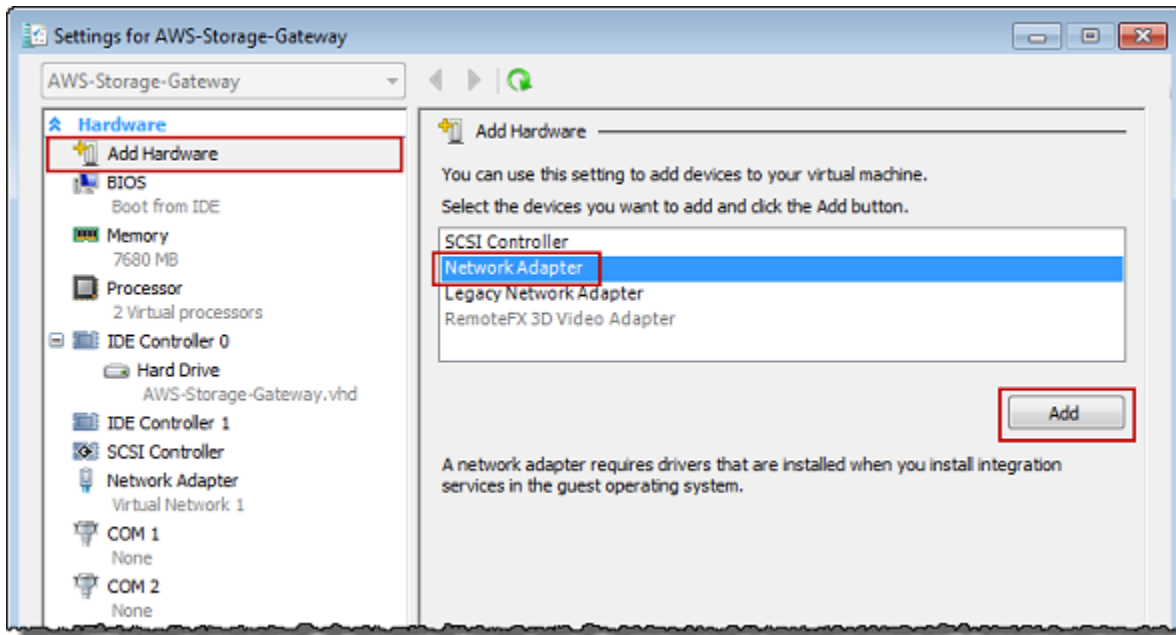
La procedura seguente presuppone che la macchina virtuale del gateway disponga già di una scheda di rete definita e che si aggiunga una seconda scheda. Questa procedura mostra come aggiungere una scheda per un host Microsoft Hyper-V.

Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host Microsoft Hyper-V

1. Nella console Storage Gateway, spegnere il gateway. Per istruzioni, consulta [Per arrestare un gateway di volumi](#).
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).

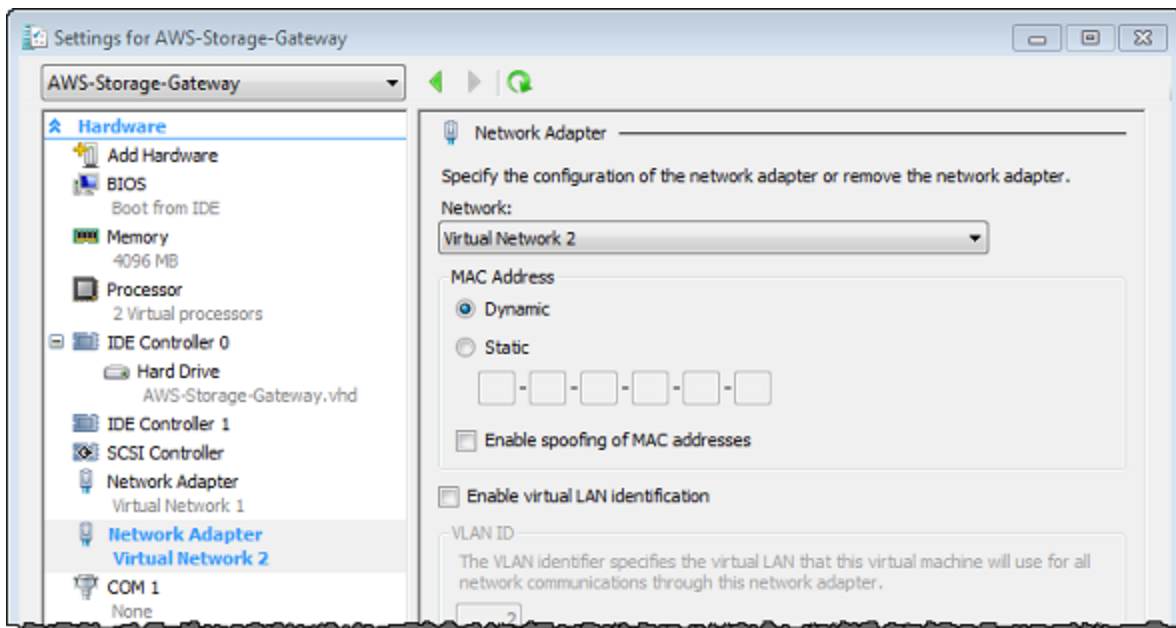


5. Nella finestra di dialogo Settings (Impostazioni) per la macchina virtuale, per Hardware scegliere Add Hardware (Aggiungi hardware).
6. Nel riquadro Add Hardware (Aggiungi hardware) scegliere Network Adapter (Scheda di rete) e quindi Add (Aggiungi) per aggiungere un dispositivo.



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 volumi](#).
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 dell'adattatore di rete che è stato aggiunto più di recente al gateway associato alla condivisione di file.

Per informazioni sulle attività della console locale comuni a Hyper-V VMware e agli host, vedere [KVM Esecuzione delle operazioni sulla console locale della VM di](#)

## Eliminazione del gateway e rimozione delle risorse associate

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

Quando si elimina un gateway, questo non viene più visualizzato nella console di AWS Storage Gateway gestione e la sua SCSI connessione all'iniziatore viene interrotta. Pur essendo la procedura di eliminazione uguale per tutti i tipi di gateway, per la rimozione delle risorse associate occorre seguire istruzioni specifiche, distinte in base al tipo di gateway da eliminare e all'host su cui è distribuito.

Puoi eliminare un gateway a livello di codice oppure utilizzando la console Storage Gateway. Seguono informazioni su come eliminare un gateway utilizzando la console Storage Gateway. [Se desideri eliminare il gateway a livello di codice, consulta Reference.AWS Storage Gateway API](#)

### Argomenti

- [Eliminazione del gateway tramite la console Storage Gateway](#)
- [Rimozione di risorse da un gateway distribuito in locale](#)
- [Rimozione di risorse da un gateway distribuito su un'istanza Amazon EC2](#)

## 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

Per i gateway distribuiti su EC2 un'istanza Amazon, l'istanza continua a esistere finché non la elimini.

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, usa il VMware vSphere client, Microsoft Hyper-V Manager o il client Virtual Machine (KVM) basato su Linux Kernel per connetterti all'host e rimuovere la macchina virtuale. Non è possibile riutilizzare la VM di un gateway eliminato per attivare un nuovo gateway.

### Come eliminare un gateway

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Scegli Gateway, quindi seleziona uno o più gateway da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.

### Warning

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

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



**⚠ Important**

Non paghi più i costi del software dopo aver eliminato un gateway, ma risorse come nastri virtuali, snapshot di Amazon Elastic Block Store (AmazonEBS) e EC2 istanze Amazon persistono. continuano a essere addebitate. Puoi scegliere di rimuovere le EC2 istanze Amazon e EBS gli snapshot Amazon annullando l'abbonamento Amazon. EC2 Se desideri mantenere il tuo EC2 abbonamento Amazon, puoi eliminare le tue EBS istantanee Amazon utilizzando la EC2 console Amazon.

## Rimozione di risorse da un gateway distribuito in locale

Per rimuovere risorse da un gateway distribuito in locale, attieniti alle istruzioni riportate di seguito.

### Rimozione di risorse da un gateway di volumi distribuito su una VM

Se il gateway da eliminare è distribuito su una macchina virtuale (VM), è consigliabile effettuare la pulizia delle risorse compiendo le seguenti azioni:

- Eliminare il gateway. Per istruzioni, consulta [Eliminazione del gateway tramite la console Storage Gateway](#).
- Elimina tutte le EBS istantanee Amazon che non ti servono. Per istruzioni, consulta [Eliminazione di uno EBS snapshot Amazon](#) nella Amazon EC2 User Guide.

## Rimozione di risorse da un gateway distribuito su un'istanza Amazon EC2

Se desideri eliminare un gateway distribuito su un'EC2istanza Amazon, ti consigliamo di ripulire AWS le risorse utilizzate con il gateway, in particolare l'EC2istanza Amazon, eventuali EBS volumi Amazon e anche i nastri se hai distribuito un Tape Gateway. Così facendo, si evita di incorrere in costi di utilizzo indesiderati.

### Rimozione di risorse dai volumi memorizzati nella cache distribuiti su Amazon EC2

Se hai distribuito un gateway con volumi memorizzati nella cache attiviEC2, ti suggeriamo di intraprendere le seguenti azioni per eliminare il gateway e ripulire le sue risorse:

1. Dalla console Storage Gateway, eliminare il gateway come illustrato in [Eliminazione del gateway tramite la console Storage Gateway](#).

2. Nella EC2 console Amazon, interrompi l'EC2istanza se prevedi di riutilizzarla. In alternativa, terminare l'istanza. In vista dell'eliminazione di volumi, annotare, prima di terminare l'istanza, i dispositivi a blocchi collegati alla stessa e gli identificatori dei dispositivi, dati che risulteranno necessari per individuare i volumi da eliminare.
3. Nella EC2 console Amazon, rimuovi tutti i EBS volumi Amazon collegati all'istanza se non intendi riutilizzarli. Per ulteriori informazioni, consulta [Clean Up Your Instance and Volume](#) nella Amazon EC2 User Guide.

# Prestazioni e ottimizzazione per Volume Gateway

Questa sezione descrive le prestazioni di Storage Gateway.

Argomenti

- [Ottimizzazione delle prestazioni del gateway](#)
- [Utilizzo dell'VMware vSphere alta disponibilità con Storage Gateway](#)

## 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 24 core fisici CPU dedicati
- Per Volume Gateway, l'hardware deve dedicare le seguenti quantità di RAM:
  - Almeno 16 GiB di spazio RAM riservato ai gateway con dimensioni della cache fino a 16 TiB
  - Almeno 32 GiB di spazio RAM riservato ai gateway con dimensioni della cache da 16 TiB a 32 TiB
  - Almeno 48 GiB di spazio RAM riservato ai gateway con dimensioni della cache da 32 TiB a 64 TiB
- Disco 1, da utilizzare come cache del gateway come segue:
  - SSD utilizzando un NVMe controller.
- Disco 2, da utilizzare come buffer di caricamento del gateway come segue:
  - SSD utilizzando un controller. NVMe
- Disco 3, da utilizzare come buffer di caricamento del gateway come segue:
  - SSD utilizzando un NVMe controller.
- Adattatore di rete 1 configurato sulla rete macchina virtuale 1:
  - Usa la rete VM 1 e aggiungi VMXnet3 (10 Gbps) da utilizzare per l'ingestione.
- Adattatore di rete 2 configurato sulla rete macchina virtuale 2:
  - Usa la rete VM 2 e aggiungi un VMXnet3 (10 Gbps) da utilizzare per la connessione. AWS

## Aggiungere risorse al gateway

I seguenti colli di bottiglia possono ridurre le prestazioni di al di sotto del throughput massimo teorico sostenuto (larghezza di banda verso il cloud): AWS

- CPU numero di core
- Velocità di trasmissione effettiva del disco del buffer di caricamento/cache
- RAM Importo totale
- Larghezza di banda di rete fino 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:

- Utilizzare uno striped RAID come RAID 10 per migliorare la velocità di trasmissione del disco, idealmente con un controller hardware. RAID

#### Note

RAID (array ridondante di dischi indipendenti), o in particolare RAID le configurazioni con strip su disco come RAID 10, è il processo di divisione di un corpo di dati in blocchi e la distribuzione dei blocchi di dati su più dispositivi di archiviazione. Il RAID livello utilizzato influisce sulla velocità esatta e sulla tolleranza ai guasti che è possibile raggiungere. Distribuendo i carichi di lavoro IO su più dischi, il throughput complessivo del RAID dispositivo è molto più elevato di quello di qualsiasi disco a membro singolo.

- Utilizzo di dischi ad alte prestazioni collegati direttamente

Per ottimizzare le prestazioni del gateway, puoi aggiungere dischi ad alte prestazioni come unità a stato solido (SSD) e un controller. È inoltre possibile collegare dischi virtuali alla macchina virtuale direttamente da una rete di archiviazione (SAN) anziché Microsoft Hyper-V. Il miglioramento delle prestazioni del disco si traduce in genere in una migliore velocità di trasmissione e in un maggior numero di operazioni di input/output al secondo (IOPS).

Per misurare il throughput, utilizza le metriche `WriteBytes` e `ReadBytes` con la statistica di `Samples` Amazon CloudWatch. Ad esempio, la statistica `ReadBytes` su un periodo di campionamento di 5 minuti diviso per 300 secondi fornisce il IOPS. Come regola generale, quando esaminate queste metriche per un gateway, cercate un throughput basso e una IOPS tendenza al ribasso per indicare i colli di bottiglia legati al disco.

#### 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 archiviazione fisica sottostanti sono rappresentate come un archivio dati. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando viene effettuato il provisioning di un disco virtuale (ad esempio, come buffer di caricamento), è possibile archiviare il disco virtuale nello stesso datastore della macchina virtuale o in un datastore differente.

Se si dispone di più di un datastore, è consigliabile scegliere un datastore per ogni tipo di storage locale che si sta creando. Un datastore che è supportato da un solo disco fisico sottostante

può offrire prestazioni non soddisfacenti. Un esempio è quando questo disco viene usato per supportare sia lo storage della cache che il buffer di caricamento in una configurazione del gateway. Analogamente, un data store supportato da una RAID configurazione meno performante come RAID 1 o RAID 6 può portare a prestazioni scadenti.

### Aggiungi CPU risorse al tuo host gateway

Il requisito minimo per un host server gateway è rappresentato da quattro processori virtuali. Per ottimizzare le prestazioni del gateway, verifica che ogni processore virtuale assegnato alla macchina virtuale gateway sia supportato da un CPU core dedicato. Inoltre, conferma che non stai effettuando un numero di sottoscrizioni eccessivo rispetto al CPUs server host.

Quando ne aggiungete altri CPUs al server host del gateway, aumentate la capacità di elaborazione del gateway. In questo modo, il gateway può gestire in parallelo l'archiviazione dei dati dall'applicazione allo storage locale e il caricamento di questi dati in Amazon S3. CPUs inoltre, aiutano a garantire che il gateway riceva CPU risorse sufficienti quando l'host è condiviso con altri VMs. Fornire CPU risorse sufficienti ha l'effetto generale di migliorare la produttività.

### Aumenta la larghezza di banda tra il gateway e il cloud AWS

L'aumento della larghezza di banda da e verso il cloud AWS 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-initiator.

#### Note

Le prestazioni del gateway osservate saranno probabilmente inferiori alla larghezza di banda di rete a causa di altri fattori limitanti elencati qui, come la velocità effettiva del disco nel buffer di cache/upload, il numero di CPU core, la RAM quantità totale 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.

### Modificare la configurazione dei volumi

Per i gateway dei volumi, se ti accorgi che l'aggiunta di ulteriori volumi a un gateway riduce la velocità di trasmissione effettiva per il gateway, puoi aggiungere i volumi a un gateway separato.

In particolare, se un volume viene utilizzato per un'applicazione a throughput elevato, puoi creare un gateway separato per l'applicazione a throughput elevato. Tuttavia, in generale, non è consigliabile utilizzare un gateway per tutte le applicazioni a throughput elevato e un altro gateway per tutte le applicazioni a throughput basso. Per calcolare il throughput del volume, utilizzare i parametri `ReadBytes` e `WriteBytes`.

Per ulteriori informazioni su questi parametri, consulta [Misurazione delle prestazioni tra l'applicazione il gateway](#).

## Ottimizza le impostazioni SCSI

È possibile ottimizzare SCSI le impostazioni i sull'SCSliniziatore i per ottenere prestazioni l/ O più elevate. Si consiglia di scegliere 256 KiB per `MaxReceiveDataSegmentLength` e `FirstBurstLength` e 1 MiB per `MaxBurstLength`. Per ulteriori informazioni sulla configurazione delle SCSI impostazioni i, vedere. [Personalizzazione delle impostazioni SCSI](#)

### Note

Queste impostazioni consigliate possono consentire prestazioni complessive migliori. Tuttavia, le SCSI impostazioni i specifiche necessarie per ottimizzare le prestazioni variano a seconda del software di backup utilizzato. Per ulteriori informazioni, consultare la documentazione del software di backup.

## Aggiungere risorse per l'ambiente applicativo

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

La connessione tra l'SCSliniziatore i e il gateway può limitare le prestazioni di caricamento e download. Se il gateway presenta prestazioni notevolmente peggiori del previsto e avete già migliorato il numero di CPU core e il throughput del disco, considerate:

- Aggiornamento dei cavi di rete per disporre di una maggiore larghezza di banda tra iniziatore e 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 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.

Aggiungete risorse all'ambiente applicativo CPU

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

## Utilizzo dell'VMware vSphere alta disponibilità con Storage Gateway

Storage Gateway offre un'elevata disponibilità VMware attraverso una serie di controlli di integrità a livello di applicazione integrati con VMware vSphere High Availability (VMwareHA). 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 garantire 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 sull' vSphere HA, consulta [vSphere How HA Works](#) nella VMware documentazione.

### Note

Il tempo necessario per riavviare una macchina virtuale guasta e ristabilire la SCSI connessione su un nuovo host dipende da molti fattori, come il sistema operativo e il carico di risorse dell'host, la velocità del disco, la connessione di rete e l'infrastruttura SAN /storage.

Per utilizzare VMware HA con Storage Gateway, segui i passaggi elencati di seguito.

### Argomenti

- [Configura il tuo cluster vSphere VMware HA](#)



- [Scarica l'immagine .ova dalla console Storage Gateway](#)
- [Distribuzione del gateway](#)
- [\(Facoltativo\) Aggiungi opzioni di sovrascrittura per altri utenti del tuo cluster VMs](#)
- [Attivazione del gateway](#)
- [Testa la tua configurazione VMware ad alta disponibilità](#)

## Configura il tuo cluster vSphere VMware HA

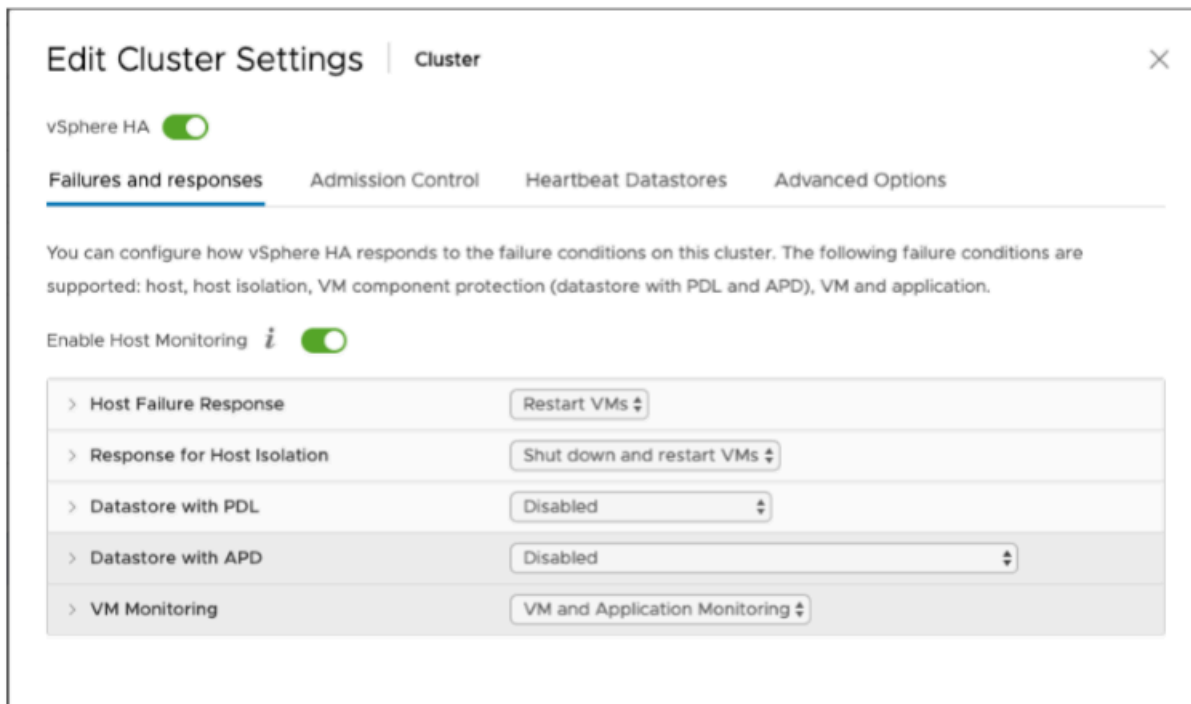
Innanzitutto, se non hai ancora creato un VMware cluster, creane uno. Per informazioni su come creare un VMware cluster, consulta [Creare un cluster vSphere HA](#) nella VMware documentazione.

Successivamente, configura il VMware cluster in modo che funzioni con Storage Gateway.

Per configurare il VMware cluster

1. Nella pagina Modifica impostazioni del cluster VMwarevSphere, assicurati che il monitoraggio delle macchine virtuali sia configurato per il monitoraggio delle macchine virtuali e delle applicazioni. A tale scopo, impostare le seguenti opzioni come indicato:
  - Risposta all'errore dell'host: riavvio VMs
  - Risposta per l'isolamento dell'host: spegnimento e riavvio VMs
  - Datastore con PDL: Disabilitato
  - Datastore con: Disabilitato APD
  - 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 ne hai altre VMs in esecuzione sul cluster, potresti voler impostare questi valori in modo specifico per la tua macchina virtuale. Non è possibile eseguire questa operazione fino a quando non

distribuisce la VM dal file .ova. Per ulteriori informazioni sull'impostazione di questi valori, consulta [\(Facoltativo\) Aggiungi opzioni di sovrascrittura per altri utenti del tuo cluster VMs](#).

## Scarica l'immagine .ova dalla console Storage Gateway

Per scaricare l'immagine .ova per il gateway

- Nella pagina di configurazione del gateway nella console di Storage Gateway, selezionare il tipo di gateway e la piattaforma host, quindi utilizzare il collegamento fornito nella console per scaricare il file .ova, come descritto in Configurazione di un gateway a nastro > [di volume](#).

## Distribuzione del gateway

Nel cluster configurato distribuisce 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 Storage Gateway .ova in un ambiente VMware o in locale, i dischi vengono descritti come dischi paravirtualizzati. SCSI 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 VMware vSphere client, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la tua macchina virtuale gateway, quindi scegli Modifica impostazioni.
2. Nella finestra di dialogo Proprietà della macchina virtuale, scegli la scheda Hardware, seleziona il SCSI controller 0, quindi scegli Cambia tipo.
3. Nella finestra di dialogo Cambia tipo di SCSI controller, selezionate il tipo di SCSI controller VMwareParavirtual, quindi scegliete OK.

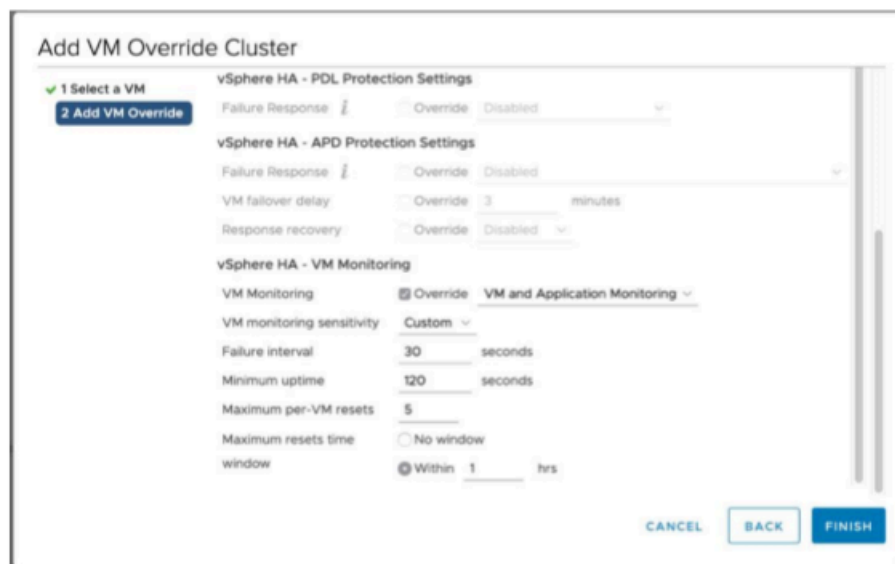
## (Facoltativo) Aggiungi opzioni di sovrascrittura per altri utenti del tuo cluster VMs

Se ne hai altre VMs in esecuzione sul tuo cluster, potresti voler impostare i valori del cluster in modo specifico per ogni macchina virtuale.

Per aggiungere opzioni di override per altre VMs nel cluster

1. Nella pagina di riepilogo VMwarevSphere, scegli il cluster per aprire la pagina del cluster, quindi scegli 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 Volume Gateway a AWS](#)
- b. [Revisione delle impostazioni e attivazione del gateway di volumi](#)
- c. [Configurazione del gateway di volumi](#)

## Testa la tua configurazione VMware ad alta disponibilità

Dopo aver attivato il gateway, esegui il test della configurazione.

Per testare la tua configurazione VMware HA

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway che desideri testare per VMware HA.
3. Per Azioni, scegli Verifica VMware HA.
4. Nella casella Verify VMware High Availability Configuration che appare, scegli OK.

### Note

Il test della configurazione VMware HA riavvia la macchina virtuale del gateway e interrompe la connettività al gateway. L'esecuzione del test potrebbe richiedere alcuni minuti.

Se il test ha esito positivo, lo stato Verified (Verificato) viene visualizzato nella scheda dettagli del gateway nella console.

5. Scegliere Exit (Esci).

Puoi trovare informazioni sugli eventi VMware HA nei gruppi di CloudWatch log di Amazon. Per ulteriori informazioni, vedere [\\_](#).

# 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 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](#)
- [Identity and Access Management per AWS Storage Gateway](#)
- [Registrazione e monitoraggio AWS Storage Gateway](#)
- [Convalida della conformità per AWS Storage Gateway](#)
- [Resilienza nello AWS Storage Gateway](#)
- [Sicurezza dell'infrastruttura in AWS Storage Gateway](#)
- [AWS Best practice per la sicurezza](#)

# Protezione dei dati in AWS Storage Gateway

Il modello di [responsabilità AWS condivisa modello](#) di si applica alla protezione dei dati in AWS Storage Gateway. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o 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 AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e 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 FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere [Federal Information Processing Standard \( \) 140-3. FIPS](#)

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 si lavora con Storage Gateway o altro Servizi AWS utilizzando la console API, AWS CLI, o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Se si fornisce un messaggio URL a un server esterno, si consiglia vivamente di non includere le informazioni sulle credenziali nel modulo URL per convalidare la richiesta a quel 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 le chiavi di crittografia gestite di Amazon S3 (SSE-S3) per crittografare sul lato server tutti i dati archiviati in Amazon S3. È possibile utilizzare Storage Gateway API 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 di file, puoi configurare il gateway per crittografare gli oggetti con chiavi gestite utilizzando AWS KMS-. SSE KMS Per informazioni sull'utilizzo dello Storage Gateway API per crittografare i dati scritti in una condivisione di file, vedere [Create NFS File Share](#) nel AWS Storage Gateway API riferimento.

### 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 Storage Gateway. API È possibile specificare una delle chiavi gestite come chiave. KMS La chiave utilizzata per crittografare il volume non può essere modificata dopo che il volume è stato creato. Per informazioni sull'utilizzo dello Storage Gateway API per crittografare i dati scritti su un volume memorizzato o memorizzato nella cache, vedere [Create Cached iSCSI Volume](#) o [Create Stored iSCSI Volume](#) nel AWS Storage Gateway API Reference.

### 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 Storage Gateway. API È possibile specificare una delle



chiavi gestite come chiave. 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 dello Storage Gateway API per crittografare i dati scritti su un nastro virtuale, vedere [CreateTapes](#) nella Guida AWS Storage Gateway API di riferimento.

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 AmazonS3.
- IAM gli utenti devono disporre delle autorizzazioni necessarie per chiamare le AWS KMS API operazioni. Per ulteriori informazioni, consulta [Using IAM policies with AWS KMS](#) nella AWS Key Management Service Developer Guide.
- Se elimini o disattivi la AWS KMS chiave o revochi il token di concessione, non puoi accedere ai dati sul volume o sul nastro. Per ulteriori informazioni, consulta [Eliminazione delle KMS chiavi](#) nella Guida per gli sviluppatori AWS Key Management Service.
- Se si crea un'istantanea da un volume KMS crittografato, l'istantanea viene crittografata. L'istantanea eredita la chiave del volume. KMS
- Se si crea un nuovo volume da un'istantanea KMS crittografata, il volume viene crittografato. È possibile specificare una KMS chiave diversa per il nuovo volume.

#### Note

Storage Gateway non supporta la creazione di un volume non crittografato da un punto di ripristino di un volume KMS crittografato o di un'istantanea KMS crittografata.

[Per ulteriori informazioni su AWS KMS, consulta What is? AWS Key Management Service](#)

## Configurazione dell'autenticazione CHAP per i volumi

In Storage Gateway, gli iniziatori iSCSI si collegano ai volumi come destinazioni iSCSI. Storage Gateway usa Challenge-Handshake Authentication Protocol (CHAP) per autenticare le connessioni dell'iniziatore e iSCSI. Il protocollo CHAP offre protezione dagli attacchi di riproduzione richiedendo l'autenticazione per accedere alle destinazioni del volume di storage. Per ogni destinazione del volume, è possibile definire una o più credenziali CHAP. È possibile visualizzare e modificare queste credenziali per i diversi iniziatori nella finestra di dialogo Configure CHAP credentials (Configura credenziali CHAP).

## Per configurare le credenziali CHAP

1. Nella console Storage Gateway, scegliere Volumi e selezionare il volume per cui si desidera configurare le credenziali CHAP.
2. Nel menu Actions (Operazioni), selezionare Configure CHAP authentication (Configura autenticazione CHAP).
3. In Initiator Name (Nome iniziatore), digitare il nome dell'iniziatore. Il nome deve essere composto da un minimo di 1 carattere a un massimo di 255 caratteri.
4. In Segreto dell'iniziatore, digitare la frase segreta da utilizzare per autenticare l'iniziatore iSCSI. La frase segreta dell'iniziatore deve essere composta da un minimo di 12 a un massimo di 16 caratteri.
5. In Target secret (Segreto della destinazione), digitare la frase segreta da utilizzare per autenticare la destinazione per il protocollo CHAP reciproco. La frase segreta di destinazione deve essere composta da un minimo di 12 a un massimo di 16 caratteri.
6. Seleziona Save (Salva) per salvare le voci.

Per visualizzare o aggiornare le credenziali CHAP, è necessario disporre delle opportune autorizzazioni per ruolo IAM che consentono di eseguire tale operazione.

## Visualizzazione e modifica delle credenziali CHAP

Puoi aggiungere, rimuovere o aggiornare le credenziali CHAP per ogni utente. È necessario disporre delle opportune autorizzazioni di ruolo IAM per visualizzare o modificare le credenziali CHAP e l'iniziatore target deve essere collegato a un gateway funzionante.

Initiator name	Initiator secret ⓘ	Target secret ⓘ
initiator2	*****	*****
initiator1	*****	*****
Add an initiator name.	Add an initiator secret value.	Add a target secret value.

This volume accepts only connections from authenticated iSCSI initiators. [Learn more](#)

Cancel Save

## Per aggiungere le credenziali CHAP

1. Nella console Storage Gateway, scegliere Volumi e selezionare il volume per cui si desidera aggiungere le credenziali CHAP.
2. Nel menu Actions (Operazioni), selezionare Configure CHAP authentication (Configura autenticazione CHAP).
3. Nella pagina Configure CHAPS (Configura CHAP), fornire Initiator name (Nome iniziatore), Initiator secret (Segreto iniziatore) e Target secret (Segreto destinazione) nelle rispettive finestre, poi selezionare Save (Salva).

## Per rimuovere le credenziali CHAP

1. Nella console Storage Gateway, scegliere Volumi e selezionare il volume per cui si desidera rimuovere le credenziali CHAP.
2. Nel menu Actions (Operazioni), selezionare Configure CHAP authentication (Configura autenticazione CHAP).
3. Fare clic sulla X accanto alle credenziali che si desidera eliminare, quindi scegliere Save (Salva).

## Per aggiornare le credenziali CHAP

1. Nella console Storage Gateway, scegliere Volumi e selezionare il volume per cui si desidera aggiornare le credenziali CHAP.
2. Nel menu Actions (Operazioni), selezionare Configure CHAP authentication (Configura autenticazione CHAP).
3. Nella pagina Configure CHAP credentials (Configura credenziali CHAP), modificare le voci per le credenziali da aggiornare.
4. Selezionare Salva.

# Identity and Access Management per AWS Storage Gateway

AWS Identity and Access Management (IAM) è un dispositivo Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle

autorizzazioni) a utilizzare le risorse. AWS SGW IAM è un dispositivo Servizio AWS che puoi utilizzare senza costi aggiuntivi.

## Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona AWS Storage Gateway con IAM](#)
- [Esempi di policy basate su identità per AWS Storage Gateway](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway](#)

## Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi. AWS SGW

Utente del servizio: se utilizzi il AWS SGW servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS SGW funzionalità 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 in AWS SGW, consulta [Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway](#).

Amministratore del servizio: se sei responsabile delle AWS SGW risorse della tua azienda, probabilmente hai pieno accesso a AWS SGW. È tuo compito determinare a quali AWS SGW funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS SGW, consulta [Come funziona AWS Storage Gateway con IAM](#).

IAM amministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accesso 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. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile 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. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume 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 () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI 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 [Firmare AWS API le richieste](#) nella Guida per l'IAMutente.

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'AWS IAM Identity Center utente e [Utilizzo dell'autenticazione a più fattori \(MFA\) AWS nella Guida per l'IAMutente](#).

### 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 utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'IAMutente.

## 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 informazioni su IAM Identity Center, vedi [Cos'è IAM Identity Center?](#) nella Guida AWS IAM Identity Center per l'utente.

## IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) 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 assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

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 IAM utente \(anziché un ruolo\)](#) nella Guida per l'IAMutente.

## IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console [cambiando ruolo](#). È possibile assumere un ruolo chiamando un' AWS API/operazione AWS CLI or o utilizzando un'operazione personalizzata URL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Utilizzo IAM dei ruoli](#) nella Guida per l'IAMutente.

IAMI ruoli 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 informazioni sui ruoli per la federazione, vedere [Creazione di un ruolo per un provider di identità di terze parti](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in IAM. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo 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 conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM
- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel 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 inoltrato (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FASle richieste 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 azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

- Ruolo di servizio: un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente](#).
- 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 IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida](#) per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta [Quando creare un IAM ruolo \(anziché un utente\)](#) nella Guida per l'IAMutente.

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole 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 JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche 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 IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMLe politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

## Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scelta tra politiche gestite e politiche in linea nella Guida](#) per l'IAMutente.

## Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

## Elenchi di controllo degli accessi (ACLs)

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

## 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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (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 nella Guida per l'utente. IAM](#)
- **Politiche di controllo del servizio (SCPs):** SCPs sono JSON politiche 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 di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP Limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- **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 [le politiche di sessione](#) nella Guida IAM per l'utente.

## Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAMutente.

## Come funziona AWS Storage Gateway con IAM

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

### IAMfunzionalità utilizzabili con AWS Storage Gateway

IAMfunzionalità	AWS SGWsupporto
<a href="#">Policy basate su identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Azioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione della policy (specifica del servizio)</a>	Sì
<a href="#">ACLs</a>	No
<a href="#">ABAC(tag nelle politiche)</a>	Parziale
<a href="#">Credenziali temporanee</a>	Sì
<a href="#">Sessioni di accesso diretto (FAS)</a>	Sì
<a href="#">Ruoli di servizio</a>	Sì
<a href="#">Ruoli collegati al servizio</a>	Sì

Per avere una panoramica generale del funzionamento AWS SGW e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta [AWS i servizi che funzionano con](#) la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

## Politiche basate sull'identità per AWS SGW

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. 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 ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il [riferimento agli elementi IAM JSON della politica](#) nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per AWS SGW

Per visualizzare esempi di politiche basate sull' AWS SGWidentità, vedere. [Esempi di policy basate su identità per AWS Storage Gateway](#)

## Politiche basate sulle risorse all'interno AWS SGW

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica 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 IAM amministratore dell'account fidato 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 la sezione [Cross Account Resource Access IAM nella Guida IAM per l'utente](#).

## Azioni politiche per AWS SGW

Supporta le operazioni di policy: si

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

L'Actionelemento di una JSON policy 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' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS SGW azioni, vedere [Actions Defined by AWS Storage Gateway](#) nel Service Authorization Reference.

Le azioni politiche in AWS SGW uso 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 AWS SGW basate sull'identità, vedere. [Esempi di policy basate su identità per AWS Storage Gateway](#)

## Risorse politiche per AWS SGW

Supporta le risorse di policy: sì

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). 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 AWS SGW risorse e relativi ARNs, vedere [Resources Defined by AWS Storage Gateway](#) nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le ARN risorse, 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 AWS SGW

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le politiche 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, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

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'IAM utente.

Per visualizzare un elenco di chiavi di AWS SGW condizione, 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 policy AWS SGW basate sull'identità, vedere. [Esempi di policy basate su identità per AWS Storage Gateway](#)

## ACLs in AWS SGW

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

## ABAC con AWS SGW

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo di ABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABAC è utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

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, vedere [Cos'è? ABAC](#) nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazione ABAC, consulta [Utilizzare il controllo di accesso basato sugli attributi \(ABAC\)](#) nella Guida per l'IAM utente.

## Utilizzo di credenziali temporanee con AWS SGW

Supporta le credenziali temporanee: sì

Alcuni 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 [Servizi AWS relativa alla funzionalità IAM nella Guida](#) per l'IAM utente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra 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 sul cambio di ruolo, consulta [Passare a un ruolo \(console\)](#) nella Guida per l'IAM utente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere [Credenziali di sicurezza temporanee](#) in IAM.

## Sessioni di accesso diretto per AWS SGW

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FAS



richieste 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 azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

## Ruoli di servizio per AWS SGW

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente](#).

### Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS SGW Modifica i ruoli di servizio solo quando viene AWS SGW fornita una guida in tal senso.

## Ruoli collegati ai servizi per AWS SGW

Supporta 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 IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

[Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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 AWS SGW risorse. Inoltre, non possono eseguire attività utilizzando AWS Management

Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempio JSON, consulta [Creazione di IAM politiche](#) nella Guida per l'IAM utente.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS SGW, incluso il formato di ARNs per ogni tipo di risorsa, vedere [Actions, Resources and Condition Keys for AWS Storage Gateway](#) nel Service Authorization Reference.

## Argomenti

- [Best practice per le policy](#)
- [Utilizzo della AWS SGW console](#)
- [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 AWS SGW risorse nel tuo account. Queste azioni 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 [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAM utente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie 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 per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL.

È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.

- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy ( ) e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere [Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM](#)
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere [Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.](#)

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.](#)

## Utilizzo della AWS SGW console

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 AWS SGW risorse presenti in 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 concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la AWS SGW console, collega anche la policy AWS SGW *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta [Aggiungere autorizzazioni a un utente](#) nella Guida per l'IAMutente.

## Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le

autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI  
AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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 alcuna azione in AWS SGW](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS SGW risorse](#)

## Non sono autorizzato a eseguire alcuna azione in AWS SGW

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'utente `mateojacksonIAMutente` tenta di utilizzare la console per visualizzare i dettagli su una `my-example-widget` risorsa fittizia ma non dispone delle autorizzazioni fittizie `sgw: GetWidget`.

```
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 assistenza, contatta l'amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'azione `iam: PassRole`, le tue politiche devono essere aggiornate per consentirti di assegnare 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 IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione 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 assistenza, contatta AWS l'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 AWS SGW risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS SGW supporta queste funzionalità, consulta [Come funziona AWS Storage Gateway con IAM](#)
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà](#) nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM 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 API chiamate per Storage Gateway come eventi. Le chiamate acquisite includono chiamate dalla console Storage Gateway e chiamate in codice alle API operazioni di 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 percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)
- [Configurazione di Amazon SNS Notifications 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 l'[CloudTrail userIdentityelemento](#).

## 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 stack ordinata delle API chiamate 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": "AIDAI15AUEPBH2M7JTNVC",
        "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": "cloudtrailgatewayv1",
        "gatewayRegion": "us-east-2",
        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
        "gatewayType": "VTL"
    },
    "responseElements": {
        "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
    },
    "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
    "eventType": "AwsApiCall",
    "apiVersion": "20130630",
    "recipientAccountId": "444455556666"
    ]
}

```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' ListGatewaysazione.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUEPBH2M7JTNCV",
      "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 ":"
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QE3KPGG6F0KSTAUU0 ",
        " 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, Fed RAMPHIPAA, MTSC,, C5, K-ISMSOSPAR, ENS High e. HITRUST CSF

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere [AWS Servizi nell'ambito del programma di conformità AWS](#) . 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 HIPAA sicurezza e la conformità: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi.](#) AWS HIPAA
- [AWS Risorse per la conformità](#) [Risorse per AWS](#) : questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.

- [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:

- Utilizza VMware vSphere High Availability (VMwareHA) per proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, consulta [Utilizzo dell'VMware vSphere alta disponibilità con Storage Gateway](#).
- Utilizzatelo AWS Backup per eseguire il backup dei volumi. Per ulteriori informazioni, consulta [Backup dei volumi](#).
- Clona il volume da un punto di ripristino. Per ulteriori informazioni, consulta [Clonazione di un volume](#).

## 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 API chiamate 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 suite di crittografia con perfect forward secrecy (PFS) come Ephemeral Diffie-Hellman () o Elliptic Curve

Ephemeral Diffie-Hellman (E). DHE 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 O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

#### Note

È necessario trattare l'appliance AWS Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare in alcun modo la sua installazione. Il tentativo di installare il software di scansione o di aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del gateway può causare il malfunzionamento del gateway e influire sulla nostra capacità di supportare o correggere il gateway.

AWS esamina, analizza e corregge CVEs regolarmente. Incorporiamo le correzioni di questi problemi in Storage Gateway come parte del nostro normale ciclo di rilascio del software. Queste correzioni vengono in genere applicate come parte del normale processo di aggiornamento del gateway durante le finestre di manutenzione programmata. Per ulteriori informazioni sugli aggiornamenti del gateway, vedere [AWS Security Bulletins](#).

## 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 informazioni sulla risoluzione dei problemi del gateway locale riguardano i gateway distribuiti sia sui client Microsoft Hyper-V che su quelli VMware ESXi Microsoft. 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 delle metriche. CloudWatch Le informazioni sulla risoluzione dei problemi di alta disponibilità riguardano i gateway in esecuzione sulla piattaforma VMware vSphere High Availability (HA).

## Argomenti

- [Risoluzione dei problemi: gateway offline nella console Storage Gateway](#)
- [Risoluzione dei problemi: errore interno durante l'attivazione del gateway](#)
- [Come risolvere i problemi di gateway on-premise](#)
- [Come risolvere i problemi di configurazione di Microsoft Hyper-V](#)
- [Risoluzione dei problemi relativi al EC2 gateway Amazon](#)
- [Risoluzione dei problemi dell'appliance hardware](#)
- [Come risolvere i problemi dei volumi](#)
- [Risoluzione dei problemi relativi alla disponibilità elevata](#)
- [Best practice per il ripristino dei dati](#)

## Risoluzione dei problemi: gateway offline nella console Storage Gateway

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se la AWS Storage Gateway console mostra che il gateway è offline.

È possibile che il gateway venga visualizzato come offline per uno o più dei seguenti motivi:

- Il gateway non può raggiungere gli endpoint del servizio Storage Gateway.
- Il gateway si è spento in modo imprevisto.

- Un disco di cache associato al gateway è stato disconnesso o modificato oppure è guasto.

Per riportare il gateway online, identificate e risolvete il problema che ha causato la disconnessione del gateway.

## Controlla il firewall o il proxy associato

Se hai configurato il gateway per utilizzare un proxy o hai posizionato il gateway protetto da un firewall, consulta le regole di accesso del proxy o del firewall. Il proxy o il firewall devono consentire il traffico da e verso le porte di rete e gli endpoint di servizio richiesti da Storage Gateway. Per ulteriori informazioni, vedere di [di rete e firewall](#).

## Verifica la presenza di un'ispezione continua SSL o approfondita del traffico del gateway

Se è attualmente in corso un'SSLispezione approfondita dei pacchetti sul traffico di rete tra il gateway e il gateway AWS, il gateway potrebbe non essere in grado di comunicare con gli endpoint di servizio richiesti. Per riportare il gateway online, è necessario disattivare l'ispezione.

## Verificare la presenza di un'interruzione dell'alimentazione o di un guasto hardware sull'host dell'hypervisor

Un'interruzione dell'alimentazione o un guasto hardware sull'host hypervisor del gateway può causare lo spegnimento imprevisto del gateway e renderlo irraggiungibile. Dopo aver ripristinato l'alimentazione e la connettività di rete, il gateway sarà nuovamente raggiungibile.

Dopo che il gateway sarà tornato online, assicurati di adottare le misure necessarie per ripristinare i dati. Per ulteriori informazioni, consulta .

## Verifica la presenza di problemi con un disco di cache associato

Il gateway può andare offline se almeno uno dei dischi di cache associati al gateway è stato rimosso, modificato o ridimensionato o se è danneggiato.

Se un disco cache funzionante è stato rimosso dall'host dell'hypervisor:

1. Arresta il gateway.
2. Aggiungere nuovamente il disco.

**Note**

Assicurati di aggiungere il disco allo stesso nodo del disco.

3. Riavviare il gateway.

Se un disco cache è danneggiato, è stato sostituito o è stato ridimensionato:

1. Arresta il gateway.
2. Reimposta il disco della cache.
3. Riconfigurare il disco per l'archiviazione nella cache.
4. Riavviare il gateway.

## Risoluzione dei problemi: errore interno durante l'attivazione del gateway

Le richieste di attivazione dello Storage Gateway attraversano due percorsi di rete. Le richieste di attivazione in entrata inviate da un client si connettono alla macchina virtuale (VM) o all'istanza Amazon Elastic Compute Cloud (AmazonEC2) del gateway tramite la porta 80. Se il gateway riceve correttamente la richiesta di attivazione, comunica con gli endpoint Storage Gateway per ricevere una chiave di attivazione. Se il gateway non riesce a raggiungere gli endpoint Storage Gateway, risponde al client con un messaggio di errore interno.

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se ricevi un messaggio di errore interno quando tenti di attivare il. AWS Storage Gateway

**Note**

- Assicurati di distribuire nuovi gateway utilizzando l'ultimo file di immagine della macchina virtuale o la versione di Amazon Machine Image (AMI). Riceverai un errore interno se tenti di attivare un gateway che utilizza un gateway obsoleto. AMI
- Assicurati di selezionare il tipo di gateway corretto che intendi implementare prima di scaricare il. AMI I file.ova e quelli AMIs per ogni tipo di gateway sono diversi e non sono intercambiabili.

## Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint pubblico, esegui i seguenti controlli e configurazioni.

### Controlla le porte richieste

Per i gateway distribuiti in locale, verifica che le porte sul firewall locale siano aperte. Per i gateway distribuiti su un'EC2istanza Amazon, verifica che le porte siano aperte nel gruppo di sicurezza dell'istanza. Per confermare che le porte siano aperte, esegui un comando telnet sull'endpoint pubblico da un server. Questo server deve trovarsi nella stessa sottorete del gateway. Ad esempio, i seguenti comandi telnet testano la connessione alla porta 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Per confermare che il gateway stesso possa raggiungere l'endpoint, accedi alla console VM locale del gateway (per i gateway distribuiti in locale). In alternativa, puoi accedere SSH all'istanza del gateway (per i gateway distribuiti su AmazonEC2). Quindi, esegui un test di connettività di rete. Conferma che il test ritorni[PASSED]. Per ulteriori informazioni, vedi [Test della connessione del gateway a Internet](#).

#### Note

Il nome utente di accesso predefinito per la console del gateway è `admin`, e la password predefinita è `password`.

Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway agli endpoint pubblici

SSLispezioni, ispezioni approfondite dei pacchetti o altre forme di protezione firewall possono interferire con i pacchetti inviati dal gateway. L'SSLhandshake fallisce se il SSL certificato viene



modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna SSL ispezione, esegui un SSL comando Open sull'endpoint di attivazione principale (anon-cp.storagegateway.region.amazonaws.com) sulla porta 443. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway:

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

### Note

Replace (Sostituisci) *region* con il tuo. Regione AWS

Se non è in corso alcuna SSL ispezione, il comando restituisce una risposta simile alla seguente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, 0 = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, 0 = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
  i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
  i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
  i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Se è in corso un'SSL ispezione, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
$ openssl s_client -connect anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

L'endpoint di attivazione accetta le SSL strette di mano solo se riconosce il certificato. SSL Ciò significa che il traffico in uscita del gateway verso gli endpoint deve essere esente dalle ispezioni eseguite dai firewall della rete. Queste ispezioni possono essere un'ispezione o un'SSLispezione approfondita dei pacchetti.

## Controlla la sincronizzazione dell'ora del gateway

Un eccessivo disallineamento temporale può causare SSL errori di handshake. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi. [Per ulteriori informazioni, vedere del del gateway](#) .

L'opzione System Time Management non è disponibile sui gateway ospitati su EC2 istanze Amazon. Per assicurarti che i EC2 gateway Amazon possano sincronizzare correttamente l'ora, verifica che l'EC2istanza Amazon possa connettersi al seguente elenco di pool di NTP server tramite le porte UDP e TCP 123:

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

## Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint Amazon VPC

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint Amazon Virtual Private Cloud (AmazonVPC), esegui i seguenti controlli e configurazioni.

### Controlla le porte richieste

Assicurati che le porte richieste all'interno del firewall locale (per i gateway distribuiti in locale) o del gruppo di sicurezza (per i gateway distribuiti in Amazon) siano aperte. EC2 Le porte necessarie per connettere un gateway a un VPC endpoint Storage Gateway sono diverse da quelle necessarie per connettere un gateway a endpoint pubblici. Le seguenti porte sono necessarie per la connessione a un VPC endpoint Storage Gateway:

- TCP443
- TCP1026
- TCP1027
- TCP1028
- TCP1031
- TCP2222

Per ulteriori informazioni, vedere .

Inoltre, controlla il gruppo di sicurezza collegato all'VPCendpoint Storage Gateway. Il gruppo di sicurezza predefinito collegato all'endpoint potrebbe non consentire le porte richieste. Crea un nuovo gruppo di sicurezza che consenta il traffico proveniente dall'intervallo di indirizzi IP del gateway sulle porte richieste. Quindi, collega quel gruppo di sicurezza all'VPCendpoint.

#### Note

Utilizza la [VPCconsole Amazon](#) per verificare il gruppo di sicurezza collegato all'VPCendpoint. Visualizza l'VPCendpoint Storage Gateway dalla console, quindi scegli la scheda Security Groups.

Per confermare che le porte richieste siano aperte, è possibile eseguire i comandi telnet sullo Storage Gateway VPC Endpoint. È necessario eseguire questi comandi da un server che si

trova nella stessa sottorete del gateway. È possibile eseguire i test sul primo DNS nome che non specifica una zona di disponibilità. Ad esempio, i seguenti comandi telnet testano le connessioni alle porte richieste utilizzando il DNS nome `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

## Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway al tuo endpoint Amazon VPC Storage Gateway

SSLispezioni, ispezioni approfondite dei pacchetti o altre forme di sicurezza firewall possono interferire con i pacchetti inviati dal gateway. L'SSLhandshake fallisce se il SSL certificato viene modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna SSL ispezione, esegui un SSL comando Open sull'VPCendpoint Storage Gateway. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway. Eseguì il comando per ogni porta richiesta:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:443 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1026 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1028 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1031 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Se non è in corso alcuna SSL ispezione, il comando restituisce una risposta simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
  i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
  i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
  i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---
```

Se è in corso un'SSL ispezione, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
```

```
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-  
east-1.amazonaws.com  
verify error:num=21:unable to verify the first certificate  
verify return:1  
---  
Certificate chain  
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com  
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com  
---
```

L'endpoint di attivazione accetta le SSL strette di mano solo se riconosce il certificato. SSL Ciò significa che il traffico in uscita dal gateway verso l'VPC endpoint attraverso le porte richieste è esente dalle ispezioni eseguite dai firewall di rete. Queste ispezioni possono essere SSL ispezioni o ispezioni approfondite dei pacchetti.

## Controlla la sincronizzazione dell'ora del gateway

Un eccessivo disallineamento temporale può causare SSL errori di handshake. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi. [Per ulteriori informazioni, vedere del del gateway .](#)

L'opzione System Time Management non è disponibile sui gateway ospitati su EC2 istanze Amazon. Per assicurarti che i EC2 gateway Amazon possano sincronizzare correttamente l'ora, verifica che l'EC2 istanza Amazon possa connettersi al seguente elenco di pool di NTP server tramite le porte UDP e TCP 123:

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

## Verifica la presenza di un HTTP proxy e conferma le impostazioni del gruppo di sicurezza associato

Prima dell'attivazione, verifica se hai un HTTP proxy su Amazon EC2 configurato sulla macchina virtuale gateway locale come proxy Squid sulla porta 3128. In questo caso, conferma quanto segue:

- Il gruppo di sicurezza collegato al HTTP proxy su Amazon EC2 deve avere una regola in entrata. Questa regola in entrata deve consentire il traffico proxy Squid sulla porta 3128 dall'indirizzo IP della macchina virtuale del gateway.
- Il gruppo di sicurezza collegato all'EC2VPCendpoint Amazon deve avere regole in entrata. Queste regole in entrata devono consentire il traffico sulle porte 1026-1028, 1031, 2222 e 443 dall'indirizzo IP del proxy su Amazon. HTTP EC2

## Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico e nello stesso è presente un VPC endpoint Storage Gateway VPC

Per risolvere gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico quando nello stesso è presente un endpoint Amazon Virtual Private Cloud VPC (Amazon)VPC, esegui i seguenti controlli e configurazioni.

### Verificare che l'impostazione Enable Private DNS Name non sia abilitata sull'VPCendpoint Storage Gateway

Se l'opzione Enable Private DNS Name è abilitata, non è possibile attivare alcun gateway dall'endpoint pubblico VPC all'endpoint pubblico.

Per disabilitare l'opzione del DNS nome privato:

1. Apri la [VPCconsole Amazon](#).
2. Nel pannello di navigazione, seleziona Endpoint.
3. Scegli il tuo VPC endpoint Storage Gateway.
4. Scegli Azioni.
5. Scegli Gestisci DNS nomi privati.
6. Per Abilita DNS nome privato, deseleziona Abilita per questo endpoint.
7. Scegli Modifica DNS nomi privati per salvare l'impostazione.

## Come risolvere i problemi di gateway on-premise

Di seguito puoi trovare informazioni sui problemi tipici che potresti riscontrare lavorando con i gateway locali e su come AWS Support attivarli per 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
<p>Non è possibile reperire l'indirizzo IP del gateway.</p>	<p>Utilizzare il client dell'hypervisor per connettersi all'host e trovare l'indirizzo IP del gateway.</p> <ul style="list-style-type: none"> <li>• Infatti VMwareESXi, l'indirizzo IP della macchina virtuale è disponibile nel vSphere client nella scheda Riepilogo.</li> <li>• Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale.</li> </ul> <p>Se comunque non si trova l'indirizzo IP del gateway:</p> <ul style="list-style-type: none"> <li>• Controllare che la VM sia attiva. Solo una VM attiva, infatti, consente l'assegnazione di un indirizzo IP al gateway.</li> <li>• 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.</li> </ul>
<p>Si verificano problemi di firewall o rete.</p>	<ul style="list-style-type: none"> <li>• Abilitare le porte necessarie per il gateway.</li> <li>• SSLLa validazione/ispezione dei certificati non devono essere attivate. Storage Gateway utilizza l'TLSautenticazione reciproca che fallirebbe se un'applicazione di terze parti tenta di intercettare/firmare uno dei due certificati.</li> <li>• 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 <a href="#">Requisiti di rete e firewall</a>.</li> </ul>
<p>L'attivazione del gateway non riesce se si fa clic sul pulsante Continua con l'attivazione nella console</p>	<ul style="list-style-type: none"> <li>• Verificare l'accessibilità della VM del gateway eseguendone il ping dal client.</li> <li>• Verificare la connettività di rete a Internet della VM, senza la quale In caso contrario, sarà necessario configurare un proxy.</li> </ul>



Problema	Operazione da eseguire
di gestione Storage Gateway.	<p>SOCKS Per ulteriori informazioni in merito, consulta <a href="#">Instradamento del gateway in locale tramite un proxy</a>.</p> <ul style="list-style-type: none"><li>• Verifica che l'host abbia l'ora corretta, che l'host sia configurato per sincronizzare automaticamente l'ora con un server Network Time Protocol (NTP) e che la VM gateway abbia l'ora corretta. Per informazioni sulla sincronizzazione dell'ora degli host dell'hypervisor e, vedere. VMs <a href="#">Sincronizzazione dell'ora della VM associata al gateway</a></li><li>• Dopo queste fasi, è possibile riprovare l'implementazione del gateway con la console Storage Gateway e la procedura guidata Configura e attiva il gateway.</li><li>• SSLLa convalida/ispezione dei certificati non deve essere attivata. Storage Gateway utilizza l'TLSautenticazione reciproca che fallirebbe se un'applicazione di terze parti tenta di intercettare/ firmare uno dei due certificati.</li><li>• Verifica che la tua macchina virtuale disponga di almeno 7,5 GB di RAM L'allocazione del gateway non riesce se sono presenti meno di 7,5 GB di RAM Per ulteriori informazioni, consulta <a href="#">Requisiti per la configurazione di Volume Gateway</a>.</li></ul>
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 <a href="#">Rimozione di dischi dal gateway</a> .

Problema	Operazione da eseguire
Occorre aumentare la larghezza di banda tra il gateway e AWS.	<p>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 <a href="#">AWS Direct Connect</a> 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 <code>CloudBytesDownloaded</code> e <code>CloudBytesUploaded</code> del gateway. Per ulteriori informazioni su questo argomento, consulta <a href="#">Misurazione delle prestazioni tra il gateway e AWS</a>. Ottimizzando la connettività a Internet si evita il riempimento del buffer di caricamento.</p>

Problema	Operazione da eseguire
<p>Il throughput da o verso il gateway si azzerava.</p>	<ul style="list-style-type: none"><li>• Nella scheda Gateway della console Storage Gateway, verifica che gli indirizzi IP per la macchina virtuale gateway siano gli stessi visualizzati utilizzando il software client dell'hypervisor (ovvero il client VMware vSphere o Microsoft Hyper-V Manager). In caso di mancata corrispondenza, riavviare il gateway dalla console Storage Gateway, come illustrato in <a href="#">Spegnimento della macchina virtuale gateway</a>. 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.</li><li>• Infatti VMware ESXi, l'indirizzo IP della macchina virtuale è disponibile nel client nella scheda Riepilogo. vSphere</li><li>• Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale.</li><li>• Verifica la connettività del gateway a AWS come descritto in <a href="#">Verifica della connessione del gateway a Internet</a>.</li><li>• 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 <a href="#">Configurazione di rete del gateway</a> e selezionare l'opzione inerente alla visualizzazione della configurazione di rete del gateway.</li></ul> <p>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 <a href="#">Misurazione delle prestazioni tra il gateway e AWS</a></p>
<p>Si sono verificati problemi durante l'importazione (distribuzione) di Storage Gateway su Microsoft Hyper-V.</p>	<p>Consultare <a href="#">Come risolvere i problemi di configurazione di Microsoft Hyper-V</a>, documento dedicato ai problemi che più comunemente possono verificarsi distribuendo un gateway su Microsoft Hyper-V.</p>

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.
  - VMwareESXi— per ulteriori informazioni, vedere [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 AVAILABLECOMMANDSfinestra, inserisci **open-support-channel** per connetterti all'assistenza clienti per Storage Gateway. Consenti la TCP porta 22 in modo da poter aprire un canale di supporto per 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 VPC endpoint, nella AVAILABLECOMMANDSfinestra, inserisci **open-support-channel**. Se il gateway non è attivato, fornisci l'VPCendpoint o l'indirizzo IP per connetterti all'assistenza clienti per Storage Gateway. Consenti la TCP porta 22 in modo da poter aprire un canale di supporto a AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

### Note

Il numero di canale non è un numero di porta Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Invece, il gateway effettua una connessione Secure Shell (SSH) (TCP22) ai server Storage Gateway e fornisce il canale di supporto per la connessione.

5. Dopo aver stabilito il canale di supporto, fornite il numero del servizio di supporto AWS Support in modo da AWS Support poter fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **q** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Immetti **exit** per disconnetterti dalla console gateway.
8. Seguire le istruzioni per uscire dalla console locale.

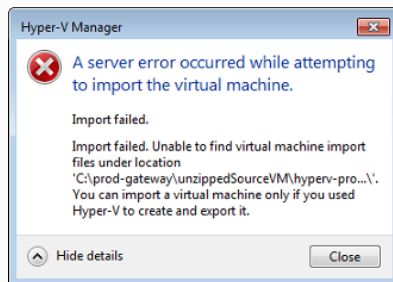
## Come risolvere i problemi di configurazione di Microsoft Hyper-V

Nella tabella seguente sono elencati i problemi che più comunemente possono verificarsi quando si implementa Storage Gateway sulla piattaforma Microsoft Hyper-V.

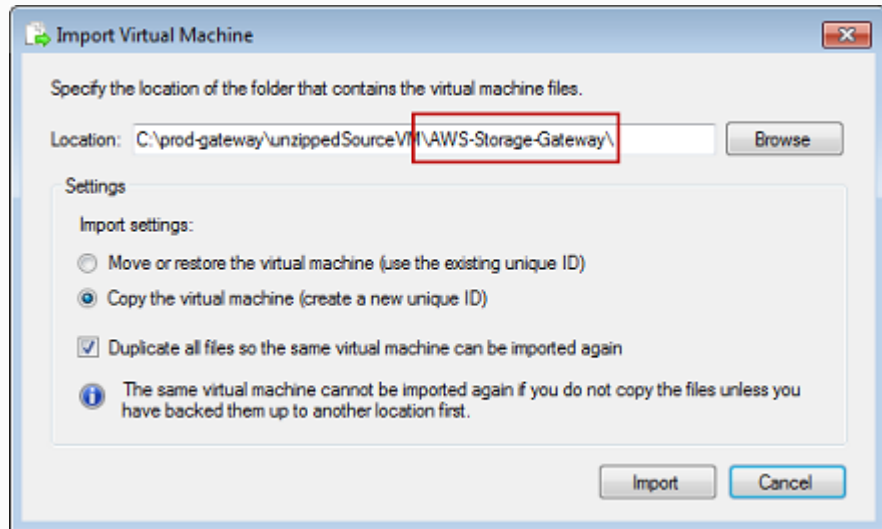
Problema	Operazione da eseguire
Nel tentativo di importare un gateway si riceve il messaggio di errore "Importazione non riuscita. Impossibile trovare il file di importazione della	<p>Ci si può imbattere in questo errore per i seguenti motivi:</p> <ul style="list-style-type: none"> <li>• Se non si specifica 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 <code>AWS-Storage-Gateway</code> , come nell'esempio seguente:</li> </ul>

## Problema

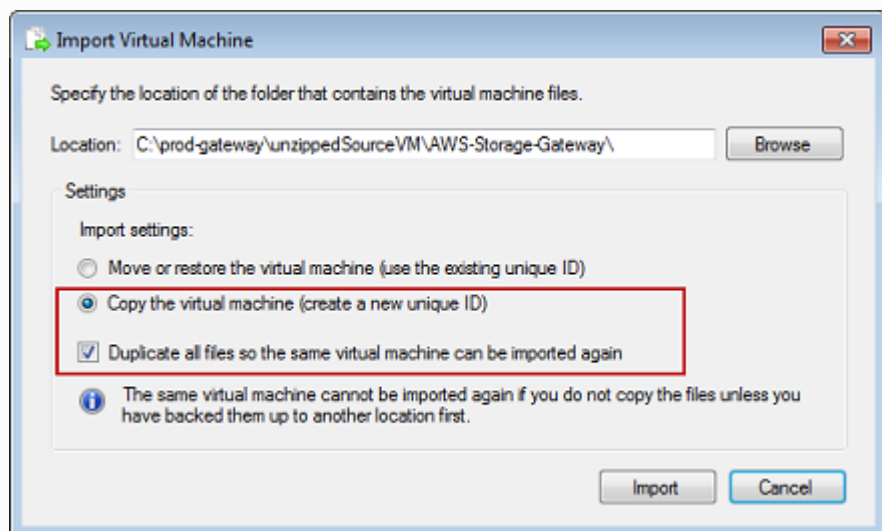
macchina virtuale nella sede...".



## Operazione da eseguire

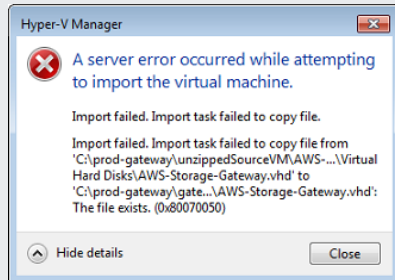


- Se è già stato distribuito un gateway senza selezionare le opzioni Copy the virtual machine (Copia la macchina virtuale) e Duplicate all files (Duplica tutti i file) nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale), la VM è stata già creata nella sede dove si trovano i file 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.



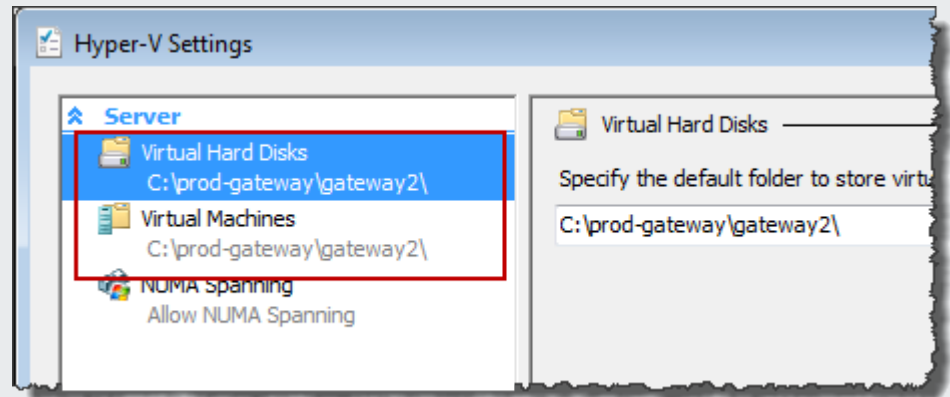
## Problema

Nel tentativo di importare un gateway si riceve il messaggio di errore "Importazione non riuscita. Impossibile copiare file".

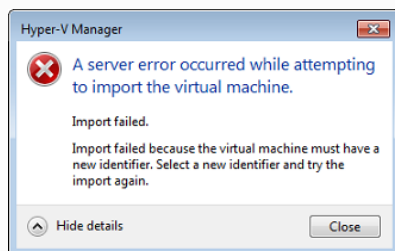


## Operazione da eseguire

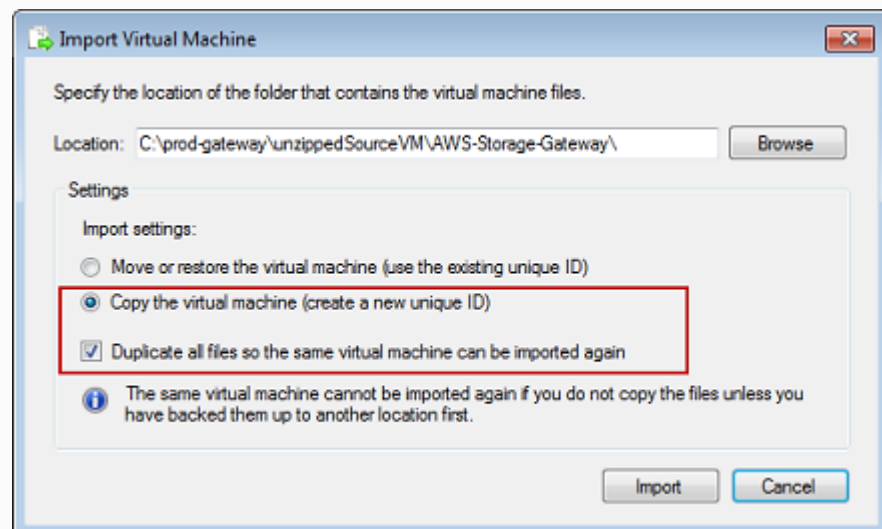
Questo errore si verifica quando, con un gateway già distribuito, si tenta di riutilizzare le cartelle predefinite che includono i file del disco rigido virtuale e quelli di configurazione della macchina virtuale. Per risolvere questo problema, bisogna specificare nuove sedi nella finestra di dialogo Hyper-V Settings (Impostazioni di Hyper-V).

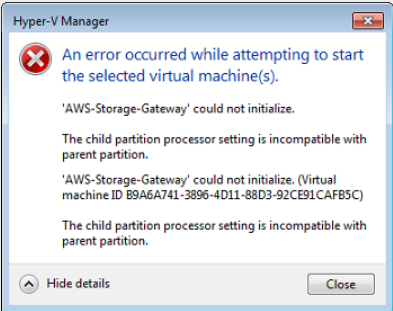


Nel tentativo di importare un gateway si riceve un messaggio di errore: "Importazione non riuscita. Per importare, assegna alla macchina virtuale un nuovo identificatore. Seleziona il nuovo identificatore e riprova."

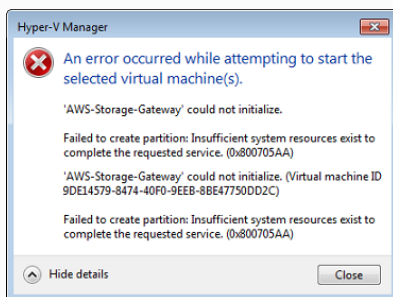


Quando si importa il gateway, assicurarsi di selezionare le opzioni Copy the virtual machine (Copia la macchina virtuale) e Duplicate all files (Duplica tutti i file) nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale) per creare un nuovo ID univoco per la VM. L'esempio seguente mostra le opzioni da utilizzare nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale).



Problema	Operazione da eseguire
<p>Nel tentativo di avviare una VM del gateway viene visualizzato il messaggio di errore "La configurazione dell'elaboratore di partizione secondario non è compatibile con la partizione principale".</p> 	<p>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'hypervisor sottostante.</p> <p>Per ulteriori informazioni sui requisiti per Storage Gateway, consulta <a href="#">Requisiti per la configurazione di Volume Gateway</a>.</p>

Tentando di avviare una VM del gateway si visualizza il messaggio di errore "Impossibile creare la partizione: risorse insufficienti 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 per la configurazione di Volume Gateway](#).



Problema	Operazione da eseguire
<p>Gli aggiornamenti di software di gateway e snapshot si verificano con tempistiche leggermente diverse da quelle previste.</p>	<p>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 sincronizzazione oraria della console del gateway locale. Per ulteriori informazioni, consulta <a href="#">Sincronizzazione dell'ora della VM associata al gateway</a>.</p>
<p>Bisogna inserire i file decompressi di Storage Gateway con Microsoft Hyper-V nel file system dell'host.</p>	<p>Accedere all'host come si fa generalmente con un server Microsoft Windows. Ad esempio, se il nome dell'host dell'hypervisor è <code>hyperv-server</code>, si può utilizzare il percorso UNC <code>\\hyperv-server\c\$</code>, presupponendo che il nome <code>hyperv-server</code> possa essere risolto o sia definito nel file degli host in locale.</p>
<p>Nel connettersi all'hypervisor viene richiesto di immettere le credenziali.</p> 	<p>Aggiungere le credenziali utente da amministratore locale per l'host dell'hypervisor, avvalendosi dello strumento Sconfig.cmd.</p>
<p>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.</p>	<p>Per informazioni su una soluzione alternativa, consulta la documentazione Microsoft, vedi <a href="#">Scarse prestazioni di rete sulle macchine virtuali su un host Hyper-V Windows Server 2012 se VMQ è attivato</a>.</p>

# Risoluzione dei problemi relativi al EC2 gateway Amazon

Nelle sezioni seguenti, puoi trovare i problemi tipici che potresti riscontrare lavorando con il tuo gateway distribuito su AmazonEC2. Per ulteriori informazioni sulla differenza tra un gateway locale e un gateway distribuito in AmazonEC2, consulta [Implementazione di un'EC2istanza Amazon per ospitare Volume Gateway](#)

## Argomenti

- [Dopo qualche secondo, il gateway ancora non si attiva](#)
- [Non riesci a trovare l'istanza del EC2 gateway nell'elenco delle istanze](#)
- [Hai creato un EBS volume Amazon ma non riesci a collegarlo alla tua istanza EC2 gateway](#)
- [Non puoi collegare un iniziatore a un target di volume del tuo gateway EC2](#)
- [Viene visualizzato un messaggio che denuncia l'indisponibilità di dischi quando si tenta di aggiungere volumi di archiviazione](#)
- [Occorre rimuovere un disco allocato per ridurre lo spazio del buffer di caricamento](#)
- [La velocità effettiva da o verso il EC2 gateway scende a zero](#)
- [Vuoi aiutarci AWS Support a risolvere i problemi del tuo gateway EC2](#)
- [Vuoi connetterti alla tua istanza gateway utilizzando la console EC2 seriale Amazon](#)

## Dopo qualche secondo, il gateway ancora non si attiva

Controlla quanto segue nella EC2 console Amazon:

- La porta 80 è attivata nel gruppo di sicurezza associato all'istanza. Per ulteriori informazioni sull'aggiunta di una regola del gruppo di sicurezza, consulta [Adding a security group rule](#) nella Amazon EC2 User Guide.
- L'istanza del gateway è contrassegnata come in esecuzione. Nella EC2 console Amazon, il valore State per l'istanza dovrebbe essere RUNNING.
- Assicurati che il tuo tipo di EC2 istanza Amazon soddisfi i requisiti minimi, come descritto in [Requisiti di storage](#).

Dopo aver risolto il problema, provare di nuovo ad attivare il gateway. A tale scopo, apri la console Storage Gateway, scegli Implementa un nuovo gateway su Amazon EC2 e inserisci nuovamente l'indirizzo IP dell'istanza.

## Non riesci a trovare l'istanza del EC2 gateway 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:

- Controlla il nome di Amazon Machine Image (AMI) nella scheda Descrizione dell'istanza. Un'istanza basata sullo Storage Gateway AMI deve iniziare con il testo **aws-storage-gateway-ami**.
- Se hai diverse istanze basate sullo Storage Gateway AMI, controlla l'ora di avvio dell'istanza per trovare l'istanza corretta.

## Hai creato un EBS volume Amazon ma non riesci a collegarlo alla tua istanza EC2 gateway

Verifica che il EBS volume Amazon in questione si trovi nella stessa zona di disponibilità dell'istanza gateway. In caso di discrepanza nelle zone di disponibilità, crea un nuovo EBS volume Amazon nella stessa zona di disponibilità dell'istanza.

## Non puoi collegare un iniziatore a un target di volume del tuo gateway EC2

Verifica che il gruppo di sicurezza con cui hai avviato l'istanza includa una regola che consenta l'accesso alla porta che stai utilizzando. La porta è in genere impostata su 3260. Per ulteriori informazioni sulla connessione ai volumi, consulta [Connessione ai volumi in un client Windows](#).

## Viene visualizzato un messaggio che denuncia l'indisponibilità di dischi quando si tenta di aggiungere volumi di archiviazione

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 AmazonEC2, i dischi locali sono EBS volumi Amazon collegati all'istanza. Questo messaggio di errore si verifica probabilmente perché non è stato definito alcun EBS volume Amazon per l'istanza.

Controlla i dispositivi a blocchi definiti per l'istanza che esegue il gateway. Se sono presenti solo due dispositivi a blocchi (i dispositivi predefiniti forniti con AMI), è necessario aggiungere spazio di archiviazione. Per ulteriori informazioni in merito, consulta [Implementazione di un'EC2 istanza](#)

[Amazon per ospitare Volume Gateway](#). Dopo aver collegato due o più EBS volumi Amazon, prova a creare uno storage di volume sul 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 effettiva da o verso il EC2 gateway scende a zero

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 il 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. Fornisci questo accesso tramite la console EC2 locale di Amazon. Accedi alla console EC2 locale di Amazon tramite Secure Shell (SSH). Per effettuare correttamente l'accessoSSH, il gruppo di sicurezza dell'istanza deve disporre di una regola che apra la TCP porta 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 per i gruppi di sicurezza, consulta [i gruppi EC2 di sicurezza Amazon](#) nella Amazon EC2 User Guide.

Per consentire la AWS Support connessione al gateway, devi prima accedere alla console locale dell'EC2istanza Amazon, 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. Accedi alla console locale per la tua EC2 istanza Amazon. Per istruzioni, consulta [Connect to your instance](#) nella Amazon EC2 User Guide.

Puoi usare il seguente comando per accedere alla console locale dell'EC2istanza.

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

#### Note

Il *PRIVATE-KEY* è il `.pem` file contenente il certificato privato della coppia di EC2 chiavi che hai usato per avviare l'EC2istanza Amazon. Per ulteriori informazioni, consulta [Recupero della chiave pubblica per la tua coppia di chiavi](#) nella Amazon EC2 User Guide.

Il *INSTANCE-PUBLIC-DNS-NAME* è il nome pubblico Domain Name System (DNS) dell'EC2istanza Amazon su cui è in esecuzione il gateway. Puoi ottenere questo DNS nome pubblico selezionando l'EC2istanza Amazon nella EC2 console e facendo clic sulla scheda Descrizione.

2. Quando richiesto, immettere **6 - Command Prompt** per aprire la console del canale AWS Support .
3. Entra **h** per aprire la AVAILABLECOMMANDSfinestra.
4. Esegui una di queste operazioni:
  - Se il gateway utilizza un endpoint pubblico, nella AVAILABLECOMMANDSfinestra, inserisci **open-support-channel** per connetterti all'assistenza clienti per Storage Gateway. Consenti la TCP porta 22 in modo da poter aprire un canale di supporto per 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 VPC endpoint, nella AVAILABLECOMMANDSfinestra, inserisci **open-support-channel**. Se il gateway non è attivato, fornisci l'VPCendpoint o l'indirizzo IP per connetterti all'assistenza clienti per Storage Gateway. Consenti la TCP porta 22 in modo da poter aprire un canale di supporto a AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

**Note**

Il numero di canale non è un numero di porta Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Invece, il gateway effettua una connessione Secure Shell (SSH) (TCP22) ai server Storage Gateway e fornisce il canale di supporto per la connessione.

5. Dopo aver stabilito il canale di supporto, fornite il numero del servizio di supporto AWS Support in modo da AWS Support poter 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. Inserisci **exit** per uscire dalla console Storage Gateway.
8. Segui i menu della console per uscire dall'istanza Storage Gateway.

## Vuoi connetterti alla tua istanza gateway utilizzando la console EC2 seriale Amazon

Puoi utilizzare la console EC2 seriale di Amazon per risolvere problemi di avvio, configurazione di rete e altri problemi. Per istruzioni e suggerimenti per la risoluzione dei problemi, consulta [Amazon EC2 Serial Console](#) nella Amazon Elastic Compute Cloud User Guide.

## Risoluzione dei problemi dell'appliance hardware

I seguenti argomenti illustrano i problemi che possono verificarsi con l'appliance hardware 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 dell'appliance, è possibile farlo utilizzando l'interfaccia di gestione Dell iDRAC. Per ulteriori informazioni, consulta [i DRAC9 Virtual Power Cycle: accensione remota dei EMC PowerEdge server Dell sul sito Web](#) di Dell Technologies InfoHub .

## Dove è possibile ottenere il DRAC supporto Dell i?

Il server Dell PowerEdge R640 è dotato dell'interfaccia di DRAC gestione Dell i. Consigliamo quanto segue:

- Se si utilizza l'interfaccia di DRAC gestione i, è necessario modificare la password predefinita. Per ulteriori informazioni sulle DRAC credenziali i, consulta [Dell PowerEdge - Quali sono le credenziali di accesso predefinite](#) per i? DRAC .
- Assicurati che il firmware up-to-date serva a prevenire violazioni della sicurezza.
- Lo spostamento dell'interfaccia di DRAC rete i su una porta normale (em) può causare problemi di prestazioni o impedire 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 del dispositivo hardware nella console Storage Gateway, come illustrato di seguito.

Scheda hardware della console Storage Gateway con l'appliance selezionata e i dettagli visualizzati.

Storage Gateway

Gateways

File shares

Volumes

Tapes

Hardware

Successfully launched File Gateway on praksuji-bh

Order appliance Quotes and orders Activate appliance Actions

Filter by hardware appliance name, ID or launched gateway type.

Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
praksuji-bh	v15loueix9yotyn5	Dell PowerEdge R640	File Gateway
praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Details

Name	praksuji-bh	Vendor	Dell
ID	v15loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

Scheda hardware della console Storage Gateway con l'appliance selezionata e i dettagli visualizzati.

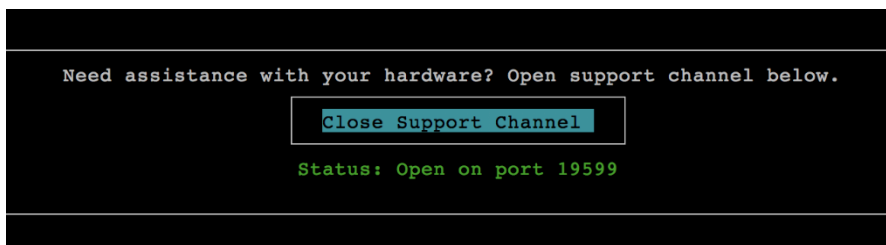
## Dove ottenere supporto per l'appliance hardware

Per contattare il supporto per i dispositivi hardware Storage Gateway, consulta [AWS Support](#).

Il AWS Support team potrebbe chiederti di attivare il canale di supporto per risolvere i problemi del 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 volumi

I paragrafi seguenti illustrano i problemi più comuni che possono verificarsi nell'utilizzo dei volumi e le operazioni suggerite per risolverli.

### Argomenti

- [Secondo la console il volume non è configurato](#)
- [Secondo la console il volume è irrecuperabile](#)
- [Il gateway nella cache è irraggiungibile e occorre recuperare i dati](#)
- [Secondo la console il volume è nello stato TRANSITO](#)
- [Occorre controllare l'integrità del volume e correggere possibili errori](#)
- [La destinazione iSCSI del volume non compare nella console di gestione del disco Windows](#)
- [Occorre modificare il nome della destinazione iSCSI del volume](#)
- [Lo snapshot programmato per un volume non viene eseguito](#)
- [È necessario rimuovere o sostituire un disco non riuscito](#)
- [Il throughput dall'applicazione a un volume si è azzerato](#)
- [Un disco della cache nel gateway rileva un errore](#)
- [Lo snapshot di un volume resta allo stato IN ATTESA più del previsto](#)
- [Notifiche di stato della disponibilità elevata](#)

### Secondo la console il volume non è configurato

Se la console Storage Gateway contrassegna il volume con lo stato BUFFER DI CARICAMENTO NON CONFIGURATO, occorre ampliare la capacità del buffer di caricamento del gateway. Senza un buffer di caricamento configurato, non è possibile utilizzare il gateway per archiviare i dati di un'applicazione. Per ulteriori informazioni, consulta [Per configurare un buffer di caricamento o l'archiviazione della cache per il gateway](#).

### Secondo la console il volume è irrecuperabile

Un volume nello storage contrassegnato dalla console Storage Gateway con lo stato IRRECUPERABILE non può essere più utilizzato. Puoi provare quindi a eliminarlo nella console

Storage Gateway. Se però contiene dei dati utili, per recuperarli basta creare un nuovo volume basato sul disco locale della VM già utilizzato per la creazione del volume in origine. Quando si crea un nuovo volume, selezionare *Preserve existing data* (Conserva i dati esistenti). Prima di rimuovere il volume, inoltre, bisogna eliminarne gli snapshot in sospeso. Per ulteriori informazioni, consulta [Eliminazione di uno snapshot](#). Se l'eliminazione del volume nella console Storage Gateway non riesce, probabilmente il disco allocato per lo stesso è stato impropriamente rimosso dalla VM e non può quindi essere eliminato dall'appliance.

Un volume nella cache contrassegnato dalla console Storage Gateway con lo stato **IRRECUPERABILE** non può essere più utilizzato. Se però contiene dei dati utili, occorre creare uno snapshot del volume dal quale recuperarli o clonare il volume dall'ultimo punto di ripristino. Dopo aver recuperato i dati, è possibile procedere all'eliminazione del volume. Per ulteriori informazioni, consulta [Il gateway nella cache è irraggiungibile e occorre recuperare i dati](#).

Per quel che riguarda i volumi archiviati, è possibile creare un nuovo volume dal disco usato per creare il volume irrecuperabile. Per ulteriori informazioni, consulta [Creazione di un volume](#). Per informazioni sullo stato di un volume, consulta [Informazioni su stati e transizioni dei volumi](#).

## Il gateway nella cache è irraggiungibile e occorre recuperare i dati

Quando il gateway diventa irraggiungibile (perché, ad esempio, viene spento), si può, sempre da un punto di ripristino del volume, sia creare uno snapshot adoperabile sia clonare un nuovo volume. Tuttavia, la clonazione da un punto di ripristino di un volume è più rapida ed economica rispetto alla creazione di uno snapshot. Per ulteriori informazioni sulla clonazione dei volumi, consulta [Clonazione di un volume](#).

Storage Gateway identifica dei punti di ripristino per ciascun volume inserito nell'architettura del gateway di volumi nella cache. Un punto di ripristino del volume è un punto temporale in cui tutti i dati del volume sono coerenti e da cui è possibile creare una snapshot o clonare un volume.

## Secondo la console il volume è nello stato TRANSITO

In alcuni casi, la console Storage Gateway può contrassegnare il volume con lo stato **TRANSITO**. A un volume può essere assegnato lo stato **TRANSITO** per vari motivi, alcuni dei quali richiedono un intervento.

Si deve intervenire, ad esempio, se lo stato **TRANSITO** del volume è dovuto all'esaurimento da parte del gateway dello spazio per il buffer di caricamento. Per verificare se il buffer di caricamento è stato

superato in passato, puoi visualizzare la `UploadBufferPercentUsed` metrica nella CloudWatch console Amazon; per ulteriori informazioni, consulta [Monitoraggio del buffer di caricamento](#). Se il gateway ha lo stato TRANSITO perché ha esaurito lo spazio nel buffer di caricamento, è necessario allocare più spazio nel buffer di caricamento al gateway. L'aggiunta di altro spazio nel buffer farà passare automaticamente il volume da TRANSITO a PROCESSO DI BOOTSTRAP a DISPONIBILE. Mentre il volume è allo stato PROCESSO DI BOOTSTRAP, il gateway legge i dati dal disco del volume, li carica su Amazon S3 e li recupera in base alle esigenze. Una volta che il gateway ha recuperato e salvato i dati del volume su Amazon S3, lo stato del volume diventa DISPONIBILE e gli snapshot vengono riavviati. Tieni presente che quando il volume è contrassegnato dallo stato PASS THROUGH (TRANSITO) o BOOTSTRAPPING (PROCESSO DI BOOTSTRAP) puoi continuare a leggere e scrivere dati dal suo disco. Per ulteriori informazioni sull'aggiunta di spazio per il buffer di caricamento, consulta [Determinazione delle dimensioni del buffer di caricamento da allocare](#).

Per intervenire tempestivamente, ancora prima che si esaurisca lo spazio, basta impostare un allarme soglia per il buffer di caricamento del gateway. Per ulteriori informazioni, consulta [Per impostare un allarme soglia superiore allarme per un buffer di caricamento del gateway](#).

Non occorre intervenire, invece, quando un volume resta allo stato PASS THROUGH (TRANSITO) perché semplicemente attende che un altro volume concluda l'operazione di bootstrap. Il gateway, infatti, esegue il bootstrap dei volumi uno alla volta.

Lo stato PASS THROUGH (TRANSITO), infine, sebbene di rado, può indicare che un disco allocato per un buffer di caricamento è inutilizzabile. In tal caso, è necessario rimuovere il disco. Per ulteriori informazioni, consulta [Gateway di volumi](#). Per informazioni sullo stato di un volume, consulta [Informazioni su stati e transizioni dei volumi](#).

## Occorre controllare l'integrità del volume e correggere possibili errori

Se il gateway utilizza gli iniziatori Microsoft Windows per connettersi ai propri volumi, per controllare l'integrità di un volume e correggere eventuali errori a esso correlati è possibile adoperare l'utilità Windows CHKDSK. Lo strumento CHKDSK può essere avviato manualmente o automaticamente da parte di Windows se viene rilevato un danneggiamento del volume.

## La destinazione iSCSI del volume non compare nella console di gestione del disco Windows

Se la destinazione iSCSI del volume non viene visualizzata nella console di gestione del disco Windows, occorre verificare di aver configurato il buffer di caricamento per il gateway. Per ulteriori

informazioni, consulta [Per configurare un buffer di caricamento o l'archiviazione della cache per il gateway](#).

## Occorre modificare il nome della destinazione iSCSI del volume

Per modificare il nome della destinazione iSCSI di un volume, è necessario eliminare il volume per poi riaggiungerlo con un nuovo nome di destinazione. Così facendo, è possibile conservare i dati nel volume.

## Lo snapshot programmato per un volume non viene eseguito

La mancata esecuzione di uno snapshot programmato per un volume può dipendere da un volume ancora allo stato TRANSITO o da un buffer di caricamento del gateway già pieno prima dell'operazione. Puoi controllare la `UploadBufferPercentUsed` metrica per il gateway nella CloudWatch console Amazon e creare un allarme per questa metrica. Per ulteriori informazioni, consultare [Monitoraggio del buffer di caricamento](#) e [Per impostare un allarme soglia superiore allarme per un buffer di caricamento del gateway](#).

## È necessario rimuovere o sostituire un disco non riuscito

Per sostituire il disco di un volume non riuscito o un volume inutile, bisogna innanzitutto rimuovere il volume utilizzando la console Storage Gateway. Per ulteriori informazioni, consulta [Per eliminare un volume](#). In un secondo momento, si può procedere alla rimozione dello storage di backup, avvalendosi del client dell'hypervisor:

- Con VMware ESXi, rimuovi lo storage di backup come descritto in [Eliminazione di un volume](#).
- Con Microsoft Hyper-V, rimuovi lo storage di backup.

## Il throughput dall'applicazione a un volume si è azzerato

Se il throughput dall'applicazione a un volume si azzerava, occorre procedere come segue:

- Se si utilizza il client VMware vSphere, verificare che l'indirizzo Host IP (IP host) del volume corrisponda a uno degli indirizzi elencati nel client vSphere nella scheda Summary (Riepilogo). Nella console Storage Gateway, l'indirizzo IP host di un volume di storage si trova nella scheda Dettagli relativa al volume stesso. Può risultare una discrepanza d'indirizzo IP quando, ad esempio, si assegna un nuovo indirizzo IP al gateway. In caso di discrepanza, occorre riavviare il gateway

dalla console Storage Gateway, come illustrato in [Spegnimento della macchina virtuale gateway](#). Dopo il riavvio, l'indirizzo Host IP (IP host) riportato nella scheda iSCSI Target Info (Informazioni destinazione iSCSI) di un volume di storage dovrebbe corrispondere a un indirizzo IP specificato nel client vSphere nella scheda Summary (Riepilogo) del gateway.

- Non vi è alcun indirizzo IP nella casella Host IP (IP host) del volume e il gateway è online. Questa situazione può verificarsi se, ad esempio, si crea un volume associato a un indirizzo IP di una scheda di rete inclusa in un gateway con due o più schede di rete. Se si rimuove o disattiva la scheda di rete alla quale è associato il volume, l'indirizzo IP potrebbe non apparire nella casella IP host. Per risolvere questo problema, bisogna eliminare il volume e ricrearlo conservandone i dati esistenti.
- Verificare che l'iniziatore iSCSI utilizzato dall'applicazione sia correttamente mappato alla destinazione iSCSI per il volume di storage. Per ulteriori informazioni sulla connessione ai volumi di storage, consulta [Connessione ai volumi in un client Windows](#).

Puoi visualizzare la velocità effettiva per i volumi e creare allarmi dalla console Amazon CloudWatch. Per ulteriori informazioni sulla misurazione del throughput dall'applicazione a un volume, consulta [Misurazione delle prestazioni tra l'applicazione il gateway](#).

## 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.

## Lo snapshot di un volume resta allo stato IN ATTESA più del previsto

La permanenza prolungata dello snapshot di un volume nello stato IN ATTESA può dipendere dall'arresto anomalo della VM del gateway così come dal cambiamento di stato del volume in TRANSITO o IRRECUPERABILE. In questi casi, in cui lo snapshot resta allo stato IN ATTESA e non viene completato correttamente, consigliamo di eliminare lo snapshot. Per ulteriori informazioni, consulta [Eliminazione di uno snapshot](#).

Quando il volume torna allo stato DISPONIBILE, è possibile crearne un nuovo snapshot. Per informazioni sullo stato di un volume, consulta [Informazioni su stati e transizioni dei volumi](#).

## 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](#)
- [Metriche](#)

## 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](#)
- [Notifica: HardReboot](#)
- [Notifica: HealthCheckFailure](#)
- [Notifica: AvailabilityMonitorTest](#)

### 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](#)
- [Ripristino dei dati da un gateway o una macchina virtuale malfunzionante](#)
- [Ripristino dei dati da un volume irrecuperabile](#)
- [Ripristino dei dati da un disco della cache malfunzionante](#)
- [Ripristino dei dati da un file system danneggiato](#)
- [Ripristino dei dati da un data center inaccessibile](#)

## 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 volumi nella cache e , quando il gateway diventa raggiungibile i volumi o i 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 [Informazioni su stati e transizioni dei volumi](#).
- 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

In caso di malfunzionamento del gateway o della macchina virtuale, puoi recuperare i dati che sono stati caricati AWS e archiviati su un volume in Amazon S3. Per i gateway di volumi nella cache, è possibile ripristinare i dati da uno snapshot di ripristino. Per i gateway di volumi archiviati, è possibile ripristinare i dati dal più recente snapshot Amazon EBS del volume. Per i gateway di nastri virtuali, è possibile ripristinare uno o più nastri da un punto di ripristino in un nuovo gateway di nastri virtuali.

Se il gateway di volumi nella cache diventa irraggiungibile, puoi usare le fasi seguenti per ripristinare i dati da uno snapshot di ripristino:

1. In AWS Management Console, scegli il gateway malfunzionante, scegli il volume che desideri ripristinare e quindi crea uno snapshot di ripristino da esso.
2. Distribuire e attivare un nuovo gateway di volumi. In alternativa, se è disponibile un gateway di volumi funzionante, è possibile usarlo per ripristinare i dati del volume.
3. Individuare lo snapshot creato e ripristinarlo in un nuovo volume nel gateway funzionante.
4. Montare il nuovo volume come dispositivo iSCSI nel server applicazioni locale.

Per informazioni dettagliate su come ripristinare i volumi nella cache da uno snapshot di ripristino, consulta [Il gateway nella cache è irraggiungibile e occorre recuperare i dati](#).

## Ripristino dei dati da un volume irrecuperabile

Se lo stato del volume è IRRECUPERABILE, non è più possibile usare il volume.

Per i volumi archiviati, è possibile recuperare i dati dal volume irrecuperabile e spostarli in un nuovo volume usando le fasi seguenti:

1. Creare un nuovo volume dal disco usato per creare il volume irrecuperabile.
2. Conservare i dati esistenti mentre si crea il nuovo volume.
3. Eliminare tutti i processi di snapshot in sospeso per il volume irrecuperabile.
4. Eliminare il volume irrecuperabile dal gateway.

Per i volumi nella cache, è consigliabile usare l'ultimo punto di ripristino per clonare un nuovo volume.

Per informazioni dettagliate su come recuperare i dati da un volume irrecuperabile e spostarli in un nuovo volume, consulta [Secondo la console il volume è irrecuperabile](#).

## 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.

## Ripristino dei dati da un file system danneggiato

Se il file system si danneggia, è possibile utilizzare il comando **fsck** per verificare la presenza di errori nel file system e correggerli. Se riesci a ripristinare il file system, puoi quindi ripristinare i dati dai volumi nel file system, come descritto di seguito:

1. Arrestare la macchina virtuale e usare la console di gestione Storage Gateway per creare uno snapshot di ripristino. Questa istantanea rappresenta i dati più recenti archiviati in AWS

### Note

È possibile usare questo snapshot come fallback se il file system non può essere ripristinato oppure se il processo di creazione dello snapshot non può essere completato.

Per informazioni su come creare uno snapshot di ripristino, consulta [Il gateway nella cache è irraggiungibile e occorre recuperare i dati](#).

2. Utilizzare il comando **fsck** per verificare la presenza di errori nel file system e cercare di correggerli.
3. Riavviare la macchina virtuale del gateway.
4. Quando l'host hypervisor inizia il processo di avvio, premere e tenere premuto il tasto MAIUSC per passare al menu di avvio di grub.
5. Dal menu, premere **e** per modificare.
6. Scegliere la riga del kernel (seconda riga) e quindi premere **e** per modificare.
7. Aggiungere l'opzione seguente alla riga di comando del kernel: **init=/bin/bash**. Usare uno spazio per separare l'opzione precedente dall'opzione appena aggiunta.
8. Eliminare entrambe le righe `console=`, assicurandosi di eliminare tutti i valori che seguono il simbolo `=`, compresi quelli separati da virgole.
9. Premere **Return** per salvare le modifiche.
10. Premere **b** per avviare il computer con l'opzione del kernel modificata. Il computer si avvierà in un prompt di `bash#`.
11. Immettere **`/sbin/fsck -f /dev/sda1`** per eseguire il comando manualmente dal prompt, per controllare e ripristinare il file system. Se il comando non funziona con il percorso `/dev/sda1`, è possibile usare **`lsblk`** per determinare il dispositivo root del filesystem di `/` e utilizzare invece quel percorso.

12. Quando il processo di controllo e ripristino del file system è completato, riavviare l'istanza.

Verranno ripristinati i valori originali per le impostazioni di grub e il gateway si avvierà normalmente.

13. Attendere il completamento degli snapshot in corso dal gateway originale e quindi convalidare i dati degli snapshot.

È possibile continuare a usare il volume originale così come è oppure è possibile creare un nuovo gateway con un nuovo volume basato sullo snapshot di ripristino o sullo snapshot completato. In alternativa, è possibile creare un nuovo volume da qualsiasi snapshot completato da questo volume.

## 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 volumi in un data center inaccessibile

1. Creare e attivare un nuovo gateway di volumi in un host Amazon EC2. Per ulteriori informazioni, consulta [Implementazione di un'istanza Amazon per ospitare Volume Gateway](#).

### Note

I volumi archiviati del gateway non possono essere ospitati nell'istanza Amazon EC2.

2. Creare un nuovo volume e scegliere il gateway EC2 come gateway di destinazione. Per ulteriori informazioni, consulta [Creazione di un volume](#).

Creare il volume in base a uno snapshot Amazon EBS o a un clone dall'ultimo punto di ripristino del volume da ripristinare.

Se il volume è basato su uno snapshot, fornire l'ID dello snapshot.

Se si sta clonando un volume da un punto di ripristino, scegliere il volume di origine.

# 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

- [Implementazione e configurazione dell'host VM gateway](#)
- [Gateway di volumi](#)
- [Ottenimento di una chiave di attivazione per il gateway](#)
- [Connessione degli SCSI iniziatori](#)
- [Utilizzo AWS Direct Connect con Storage Gateway](#)
- [Requisiti delle porte di rete per Volume Gateway](#)
- [Connessione al gateway](#)
- [Informazioni sulle risorse e sulle risorse dello Storage Gateway IDs](#)
- [Tagging per risorse Storage Gateway](#)
- [Uso di componenti open source per AWS Storage Gateway](#)
- [AWS Storage Gateway quote](#)

# Implementazione e configurazione dell'host VM gateway

## Argomenti

- [Configurazione VMware per Storage Gateway](#)
- [Sincronizzazione dell'ora della VM associata al gateway](#)
- [Implementazione di un'EC2istanza Amazon per ospitare Volume Gateway](#)
- [Implementazione di Amazon EC2 con impostazioni predefinite](#)
- [Modifica le opzioni dei metadati delle EC2 istanze Amazon](#)

# Configurazione VMware per Storage Gateway

Durante VMware la configurazione per Storage Gateway, assicurati di sincronizzare l'ora della macchina virtuale con l'ora dell'host, configura la VM per utilizzare controller di disco paravirtualizzati

durante il provisioning dello storage e fornisca protezione dai guasti nel livello di infrastruttura che supporta una macchina virtuale gateway.

## Argomenti

- [Sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host](#)
- [Configurazione della macchina virtuale per l'utilizzo di controller di AWS Storage Gateway disco paravirtualizzati](#)
- [Utilizzo di Storage Gateway con disponibilità VMware elevata](#)

## 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. Quindi si controlla l'ora dell'host e, se necessario, si imposta l'ora dell'host e si configura l'host in modo che sincronizzi automaticamente l'ora con un server Network Time Protocol (NTP).

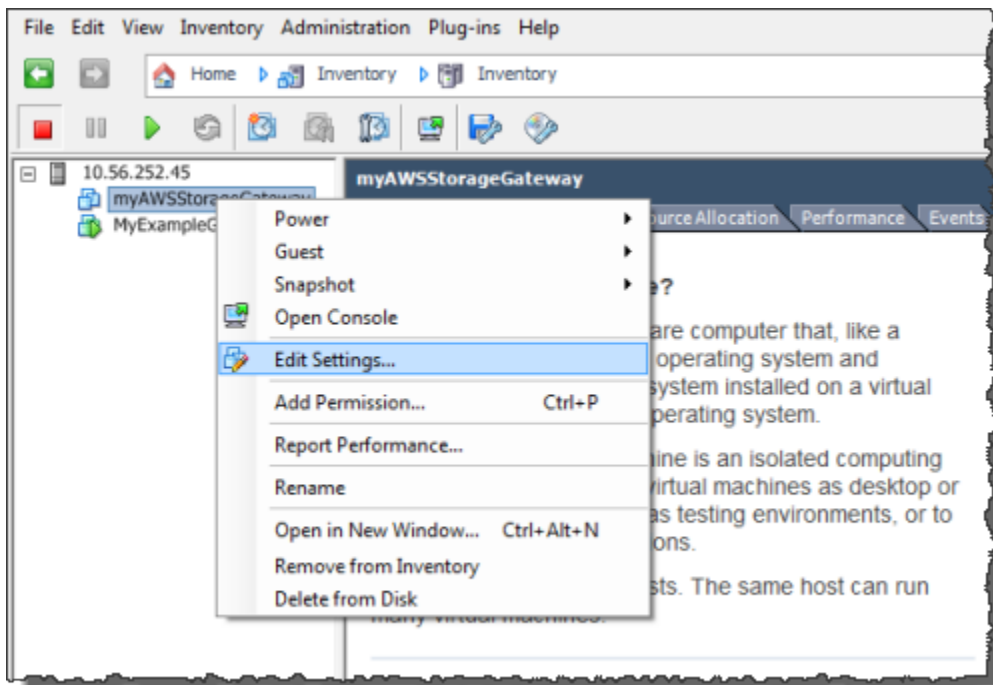
### Important

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

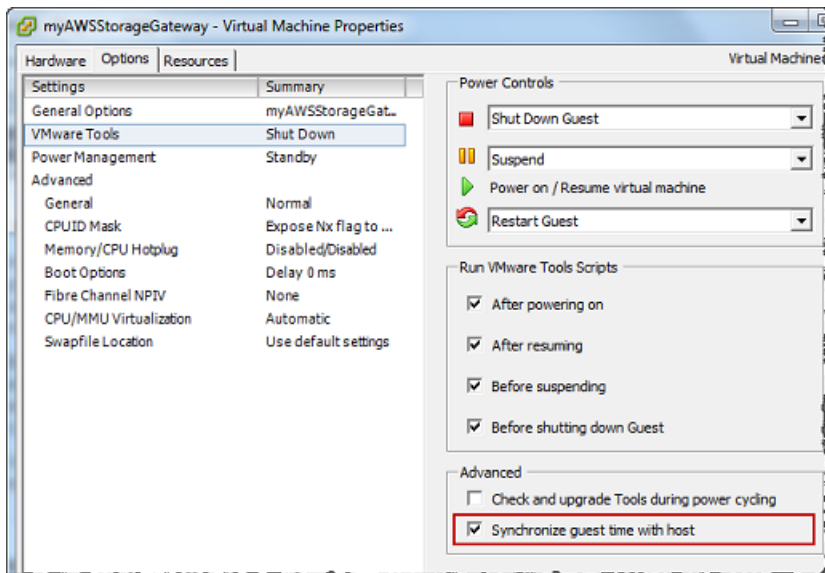
1. Configurare la data e l'ora della macchina virtuale.
  - a. Nel vSphere client, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la tua macchina virtuale gateway e scegli Modifica impostazioni.

Viene visualizzata la finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale).



- b. Scegli la scheda Opzioni e scegli VMwareStrumenti 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.

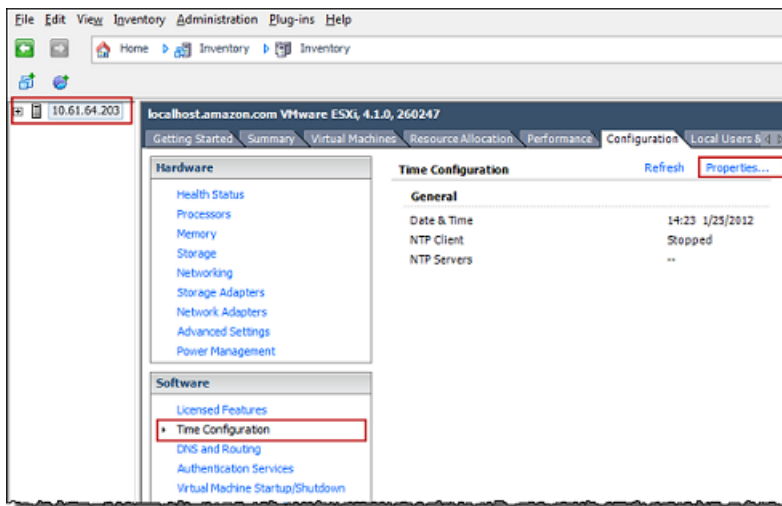


2. Configurare la data e l'ora dell'host.

È importante verificare che l'orologio dell'host sia impostato sulla data e sull'ora corrette. Se non avete configurato l'orologio dell'host, effettuate le seguenti operazioni per impostarlo e sincronizzarlo con un NTP server.

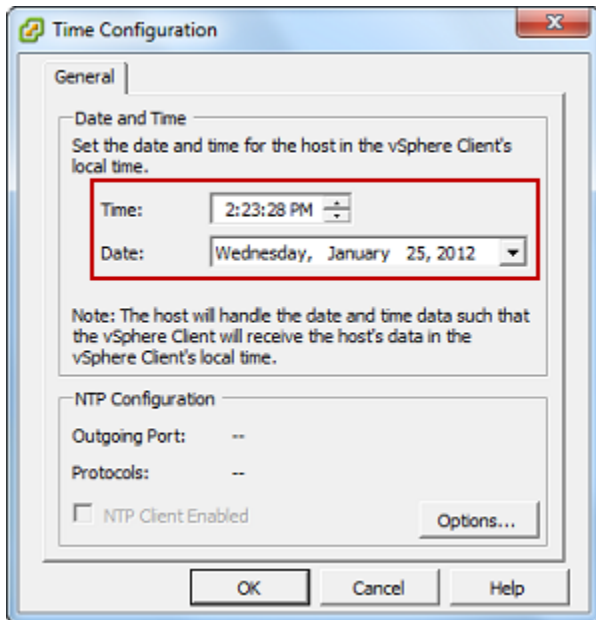
- a. Nel VMware vSphere client, seleziona il nodo vSphere host nel riquadro a sinistra, quindi scegli la scheda Configurazione.
- b. Selezionare Time Configuration (Configurazione data e ora) nel pannello Software e quindi scegliere il collegamento Properties (Proprietà).

Viene visualizzata la finestra di dialogo Time Configuration (Configurazione data e ora).

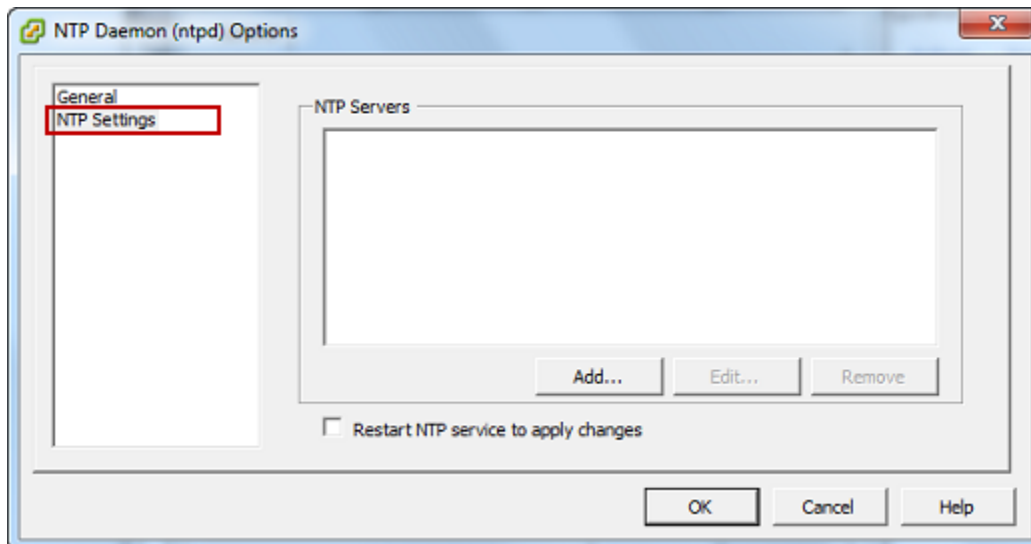


- c. Nel pannello Date and Time (Data e ora) impostare la data e l'ora.





- d. Configura l'host per sincronizzare automaticamente l'ora con un NTP server.
  - i. Scegliete Opzioni nella finestra di dialogo Time Configuration, quindi nella finestra di dialogo Opzioni NTP Daemon (ntpd), scegliete NTPImpostazioni nel riquadro sinistro.



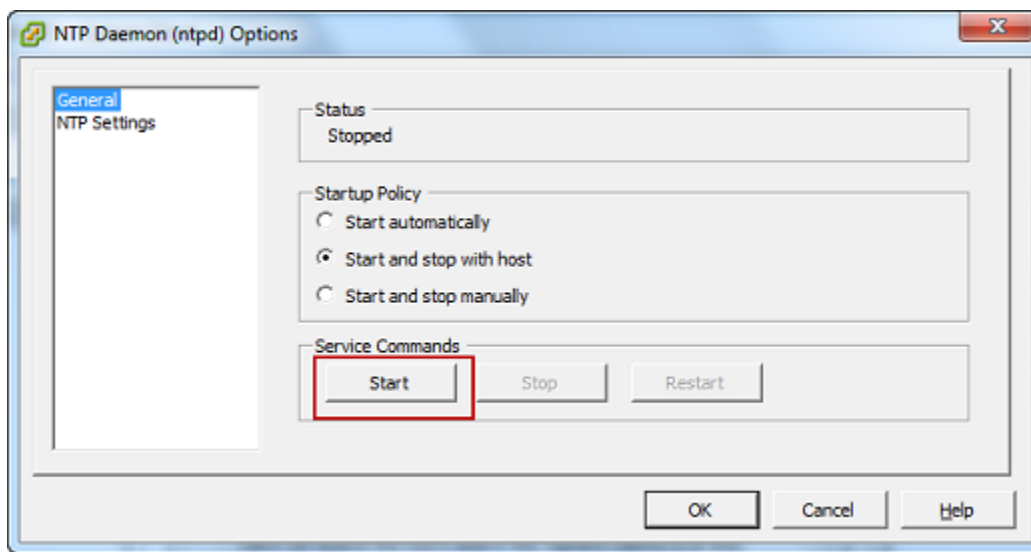
- ii. Scegli Aggiungi per aggiungere un nuovo server. NTP
    - iii. Nella finestra di dialogo Aggiungi NTP server, digitate l'indirizzo IP o il nome di dominio completo di un NTP server, quindi scegliete OK.

È possibile usare `pool.ntp.org` come mostrato nell'esempio seguente.



- iv. Nella finestra di dialogo Opzioni NTP Daemon (ntpd), scegliete Generale nel riquadro a sinistra.
- v. Nel riquadro Service Commands (Comandi servizio) scegliere Start (Avvia) per avviare il servizio.

Nota che se modifichi questo riferimento NTP al server o ne aggiungi un altro in un secondo momento, dovrai riavviare il servizio per utilizzare il nuovo server.



- e. Scegliete OK per chiudere la finestra di NTPdialogo Opzioni Daemon (ntpd).
- f. Scegliere OK per chiudere la finestra di dialogo Time Configuration (Configurazione data e ora).

## Configurazione della macchina virtuale per l'utilizzo di controller di AWS Storage Gateway disco paravirtualizzati

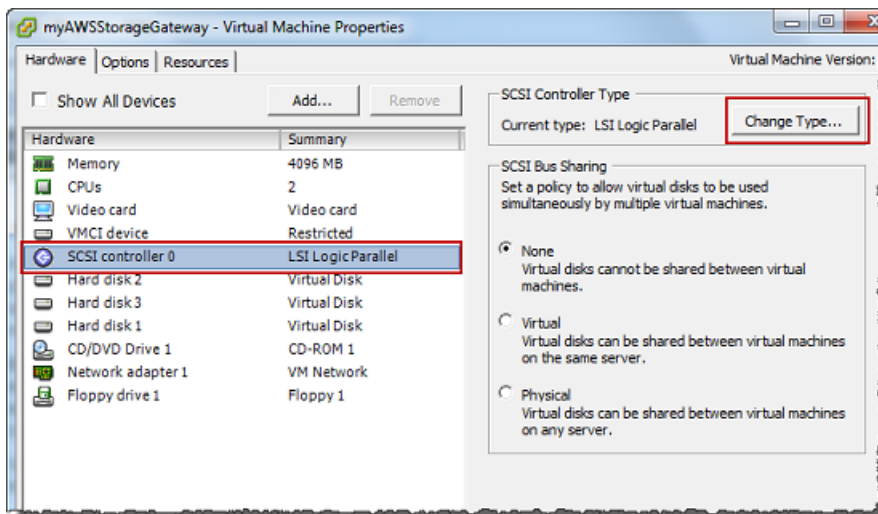
In questa attività, si imposta il SCSI controller i in modo che la macchina virtuale utilizzi la paravirtualizzazione. La paravirtualizzazione è una modalità in cui la macchina virtuale del gateway opera con il sistema operativo host in modo che la console possa identificare i dischi aggiunti alla macchina virtuale.

**Note**

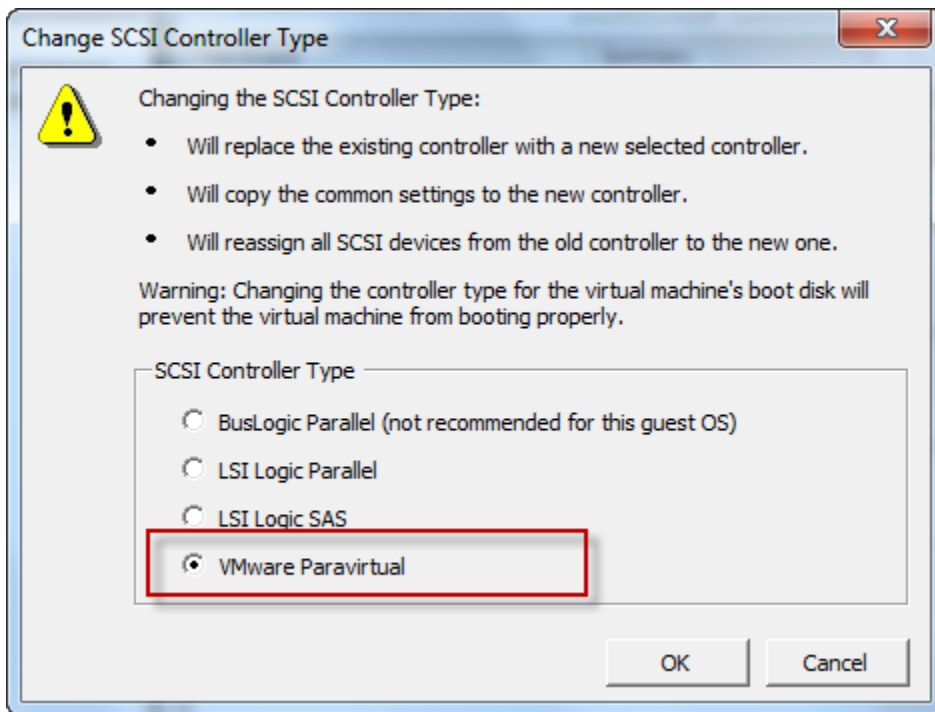
Devi completare questa procedura per evitare problemi di identificazione dei dischi quando li configuri nella console del gateway.

Per configurare la macchina virtuale per l'uso di controller paravirtualizzati

1. Nel VMware vSphere client, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la tua VM gateway, quindi scegli Modifica impostazioni.
2. Nella finestra di dialogo Proprietà della macchina virtuale, scegli la scheda Hardware, seleziona il SCSI controller 0, quindi scegli Cambia tipo.



3. Nella finestra di dialogo Cambia tipo di SCSI controller, seleziona il tipo di SCSI controller VMwareParavirtual, quindi scegli OK.



## Utilizzo di Storage Gateway con disponibilità VMware elevata

VMware High Availability (HA) è un componente in vSphere grado di fornire protezione dai guasti a livello di infrastruttura che supporta una macchina virtuale gateway. VMware a tale scopo, HA utilizza più host configurati come cluster, in modo che, in caso di guasto di un host che esegue una macchina virtuale gateway, la macchina virtuale gateway possa essere riavviata automaticamente su un altro host all'interno del cluster. Per ulteriori informazioni su VMware HA, consulta [Best Practices for VMware vSphere High Availability Clusters](#) sul sito Web. VMware

Per utilizzare Storage Gateway con VMware HA, si consiglia di effettuare le seguenti operazioni:

- Implementa il pacchetto VMware ESX .ova scaricabile 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 evitare che l'iniziatore si disconnetta dalle destinazioni dei volumi di archiviazione durante il failover, segui le impostazioni consigliate per il tuo sistema operativo. SCSI 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 SCSI timeout i consigliati per i client Windows e Linux sono superiori al tempo tipico necessario per il failover. Per ulteriori informazioni sulla personalizzazione delle impostazioni del timeout dei client Windows, consulta [Personalizzazione delle impostazioni di Windows i SCSI](#). Per ulteriori informazioni sulla personalizzazione delle impostazioni del timeout dei client Linux, consulta [Personalizzazione delle impostazioni di Linux i SCSI](#).

- Con il clustering, se distribuisce 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

Per un gateway distribuito su VMware ESXi, l'impostazione dell'ora dell'host dell'hypervisor e la sincronizzazione dell'ora della macchina virtuale con l'host sono sufficienti per evitare la deriva temporale. 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 gateway hypervisor con un server Network Time Protocol (NTP)

1. Accedere alla console locale del gateway:
  - Per ulteriori informazioni sull'accesso alla console locale, vedere. VMware ESXi [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 Virtuam Machine basata su kernel Linux (), vedere. KVM [Accesso alla console locale del gateway con Linux KVM](#)
2. Nel menu principale Configurazione di Storage Gateway digitare **4** per Gestione ora di sistema.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. Nel menu System Time Management (Gestione ora di sistema), digitare **1** per View and Synchronize System Time (Visualizza e sincronizza ora di sistema).

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

4. Se il risultato indica che è necessario sincronizzare l'ora della macchina virtuale con l'ora, immettere. **NTP 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.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Lo screenshot seguente mostra una macchina virtuale che richiede la sincronizzazione dell'ora.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

## Implementazione di un'EC2istanza Amazon per ospitare Volume Gateway

Puoi distribuire e attivare un su un'istanza Amazon Elastic Compute Cloud EC2 (Amazon). AWS Storage Gateway Amazon Machine Image (AMI) è disponibile come communityAMI.

### Note


La community AMIs di Storage Gateway è pubblicata e completamente supportata da AWS. Come si può vedere AWS, l'editore è un fornitore verificato.

Volume Gateway AMIs utilizza la seguente convenzione di denominazione. Il numero di versione aggiunto al AMI nome cambia con ogni versione rilasciata.

`aws-storage-gateway-CLASSIC-2.9.0`

Per distribuire un'EC2istanza Amazon per ospitare il tuo Volume Gateway

1. Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta [Configurare un gateway di volumi](#). Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi segui i passaggi seguenti per avviare l'EC2istanza Amazon che ospiterà il tuo .

 Note

La piattaforma EC2 host Amazon supporta solo volumi in cache. Gli Stored Volume Gateway non possono essere implementati su istanze. EC2

2. Scegli Launch instance per aprire il AWS Storage Gateway AMI modello nella EC2 console Amazon, dove puoi configurare impostazioni aggiuntive.

Usa Quicklaunch per avviare l'EC2istanza Amazon con le impostazioni predefinite. Per ulteriori informazioni sulle specifiche predefinite di Amazon EC2 Quicklaunch, consulta le specifiche di per Amazon. EC2 [Specifiche di configurazione Quicklaunch per AmazonEC2](#).

3. In Nome, inserisci un nome per l'EC2istanza Amazon. Dopo aver distribuito l'istanza, puoi cercare questo nome per trovare l'istanza nelle pagine di elenco nella EC2 console Amazon.
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 EC2 istanze Amazon](#).

È possibile ridimensionare l'istanza dopo l'avvio, se necessario. Per ulteriori informazioni, consulta [Ridimensionamento dell'istanza nella](#) Amazon EC2 User Guide.

 Note

Alcuni tipi di istanze, in particolare i3EC2, utilizzano dischi. NVMe SSD Questi possono causare problemi all'avvio o all'arresto del gateway di volumi; 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 è 0. Per ulteriori informazioni sui parametri di monitoraggio per il gateway, consulta [Metriche e dimensioni dello Storage Gateway](#) nella CloudWatch documentazione.

5. Nella sezione Coppia di chiavi (accesso), in Nome coppia di chiavi: obbligatorio, seleziona la coppia di chiavi che desideri utilizzare per connetterti in modo sicuro alla tua istanza. Se necessario, è possibile creare una nuova coppia di chiavi. Per ulteriori informazioni, consulta [Creazione di una coppia di chiavi](#) nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux.
6. Nella sezione Impostazioni di rete, rivedi le impostazioni preconfigurate e scegli Modifica per apportare modifiche ai seguenti campi:
  - a. Se VPC: obbligatorio, scegli VPC dove vuoi lanciare la tua EC2 istanza Amazon. Per ulteriori informazioni, consulta [Come VPC funziona Amazon](#) nella Guida per l'utente di Amazon Virtual Private Cloud.
  - b. (Facoltativo) Per Subnet, scegli la sottorete in cui vuoi lanciare l'istanza AmazonEC2.
  - c. Per Assegna automaticamente IP pubblico, scegli Abilita.
7. Nella sottosezione Firewall (gruppi di sicurezza), rivedi le impostazioni preconfigurate. Se lo desideri, puoi modificare il nome e la descrizione predefiniti del nuovo gruppo di sicurezza da creare per la tua EC2 istanza Amazon, oppure scegliere di applicare le regole firewall di un gruppo di sicurezza esistente.
8. Nella sottosezione Regole dei gruppi di sicurezza in ingresso, aggiungi le regole firewall per aprire le porte che i client utilizzeranno per connettersi alla tua istanza. Per ulteriori informazioni sulle porte richieste per il gateway di volumi, 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

Volume Gateway richiede che la TCP porta 80 sia aperta per il traffico in entrata e per HTTP l'accesso singolo durante l'attivazione del gateway. Dopo l'attivazione, è possibile chiudere questa porta.

Inoltre, è necessario aprire la TCP porta 3260 per l'accesso. SCSI

9. Nella sottosezione Configurazione di rete avanzata, rivedere le impostazioni preconfigurate e, se necessario, apportare modifiche.
10. Nella sezione Configura archiviazione scegliere Aggiungi nuovo volume per aggiungere spazio di archiviazione all'istanza del gateway.

 Important

È necessario aggiungere almeno un EBS volume Amazon con almeno 165 GiB di capacità per lo storage della cache e almeno un EBS volume Amazon con almeno 150 GiB di capacità per il buffer di caricamento, oltre al volume Root preconfigurato. Per migliorare le prestazioni, si consiglia di allocare più EBS volumi per l'archiviazione della cache con almeno 150 GiB ciascuno.

11. Nella sezione Dettagli avanzati, rivedi le impostazioni preconfigurate e apporta le modifiche se necessario.
12. Scegli Launch instance per avviare la tua nuova istanza Amazon EC2 gateway con le impostazioni configurate.
13. Per verificare che la tua nuova istanza sia stata lanciata correttamente, vai alla pagina Istanze nella EC2 console Amazon e cerca la tua nuova istanza per nome. Assicurati che in Stato dell'istanza sia visualizzato In esecuzione con un segno di spunta verde e che il Controllo dello stato sia completo e mostri un segno di spunta verde.
14. Seleziona l'istanza dalla pagina dei dettagli. Copia l'IPv4 indirizzo pubblico dalla sezione di riepilogo dell'istanza, quindi torna alla pagina Configura gateway nella console Storage Gateway per riprendere la configurazione del .

È possibile determinare l'AMIID da utilizzare per avviare un utilizzando la console Storage Gateway o interrogando l'archivio AWS Systems Manager dei parametri.

Per determinare l'AMIID, esegui una delle seguenti operazioni:

- Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta [Configurare un gateway di volumi](#). Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi scegli Launch instance per aprire il AWS Storage Gateway AMI modello nella EC2 console Amazon.

Verrai reindirizzato alla AMI pagina della EC2 community, dove puoi vedere l'AMIID della tua AWS regione in. URL

- Esegui una query sull'archivio dei parametri Systems Manager. È possibile utilizzare AWS CLI o Storage Gateway API per interrogare il parametro pubblico Systems Manager nello spazio dei nomi `/aws/service/storagegateway/ami/CACHED/latest` per i gateway di volume cache o `/aws/service/storagegateway/ami/STORED/latest` per gli Stored Volume Gateway. Ad esempio, l'utilizzo del CLI comando seguente restituisce l'ID della corrente AMI nel campo specificato. Regione AWS

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/STORED/latest
```

Il CLI comando 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/STORED/latest",
    "Name": "/aws/service/storagegateway/ami/STORED/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

## Implementazione di Amazon EC2 con impostazioni predefinite

Questo argomento elenca i passaggi per implementare un host Amazon EC2 utilizzando le specifiche predefinite.

Puoi implementare e attivare un gateway di volumi 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 volumi](#).
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 implementare un'istanza Amazon EC2 con la configurazione predefinita.

L'istanza Amazon EC2 creata da Usa le impostazioni predefinite ha le seguenti specifiche predefinite:

- Tipo di istanza: m5.xlarge
- Impostazioni di rete
  - Per VPC, seleziona il VPC nel quale desideri che venga eseguita l'istanza EC2.
  - Per Sottorete, specifica la sottorete in cui deve essere avviata l'istanza EC2.

#### Note

Le sottoreti VPC verranno visualizzate nel menu a discesa solo se hanno l'impostazione di assegnazione automatica dell'indirizzo 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			

Impostazioni predefinite	Volume root AMI	Cache del volume 2	Cache del volume 3			
Prestazioni	125	125	125			

## Modifica le opzioni dei metadati delle EC2 istanze Amazon

Il servizio di metadati dell'istanza (IMDS) è un componente su istanza che fornisce un accesso sicuro ai metadati delle EC2 istanze Amazon. Un'istanza può essere configurata per accettare richieste di metadati in entrata che utilizzano la IMDS versione 1 (IMDSv1) o richiedere che tutte le richieste di metadati utilizzino la versione 2 (). IMDS IMDSv2 IMDSv2utilizza richieste orientate alla sessione e mitiga diversi tipi di vulnerabilità che potrebbero essere utilizzate per tentare di accedere a. IMDS Per informazioni sulIMDSv2, consulta [Come funziona Instance Metadata Service versione 2](#) nella Amazon Elastic Compute Cloud User Guide.

Ti consigliamo di richiederlo IMDSv2 per tutte le EC2 istanze Amazon che ospitano Storage Gateway. IMDSv2è obbligatorio per impostazione predefinita su tutte le istanze gateway appena lanciate. Se disponi di istanze esistenti che sono ancora configurate per accettare richieste di IMDSv1 metadati, consulta [Require the use of IMDSv2](#) nella Amazon Elastic Compute Cloud User Guide per istruzioni su come modificare le opzioni di metadati dell'istanza di cui richiedere l'uso. IMDSv2 L'applicazione di questa modifica non richiede il riavvio dell'istanza.

## Gateway di volumi

### Argomenti

- [Rimozione di dischi dal gateway](#)
- [Aggiungere e rimuovere EBS volumi Amazon per i EC2 gateway Amazon](#)

### 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.

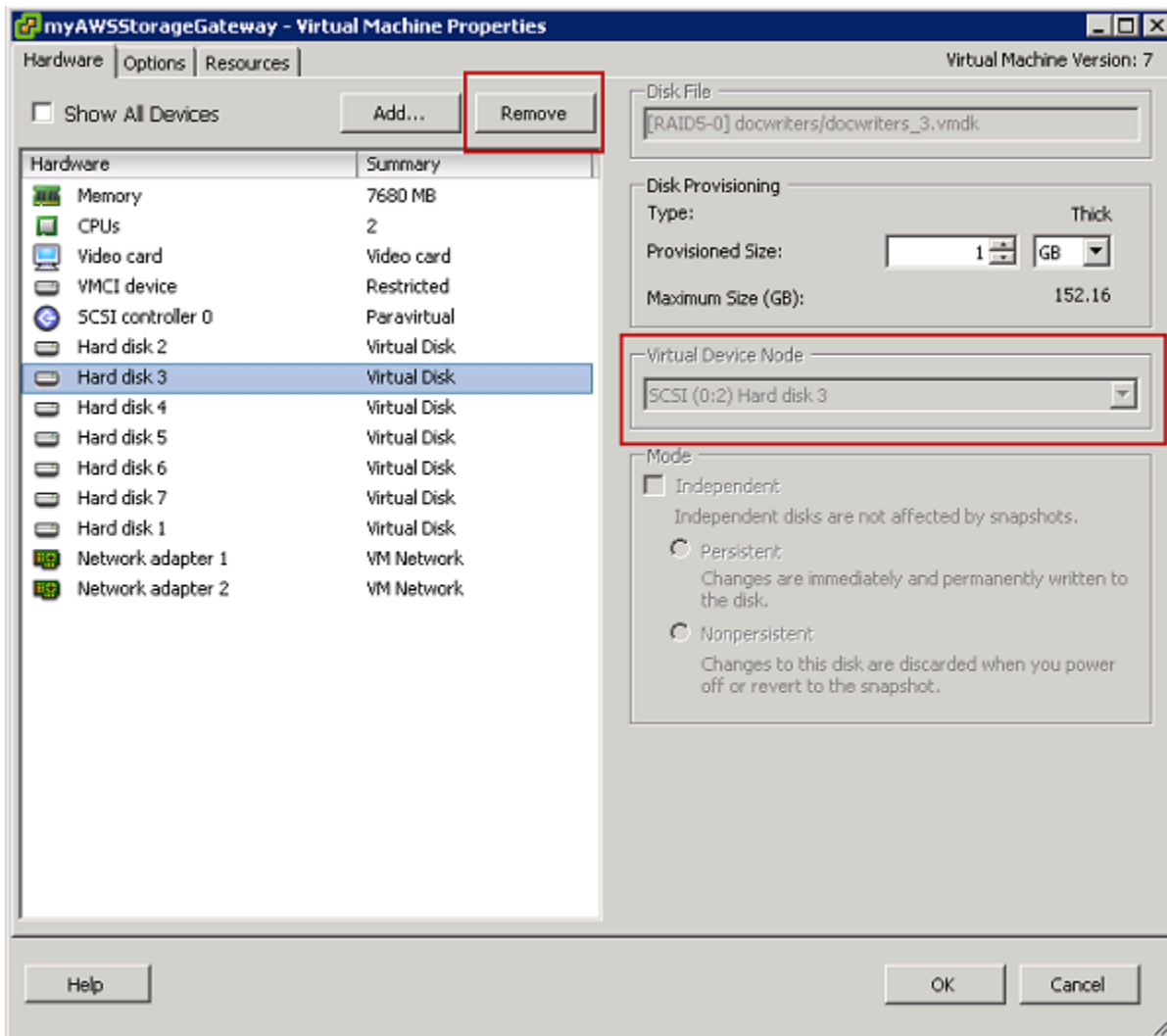
## Rimozione di un disco da un gateway ospitato su VMware ESXi

È possibile utilizzare la procedura seguente per rimuovere un disco dal gateway ospitato sull'VMwarehypervisor.

Per rimuovere un disco allocato per il buffer di caricamento ( ) VMware ESXi

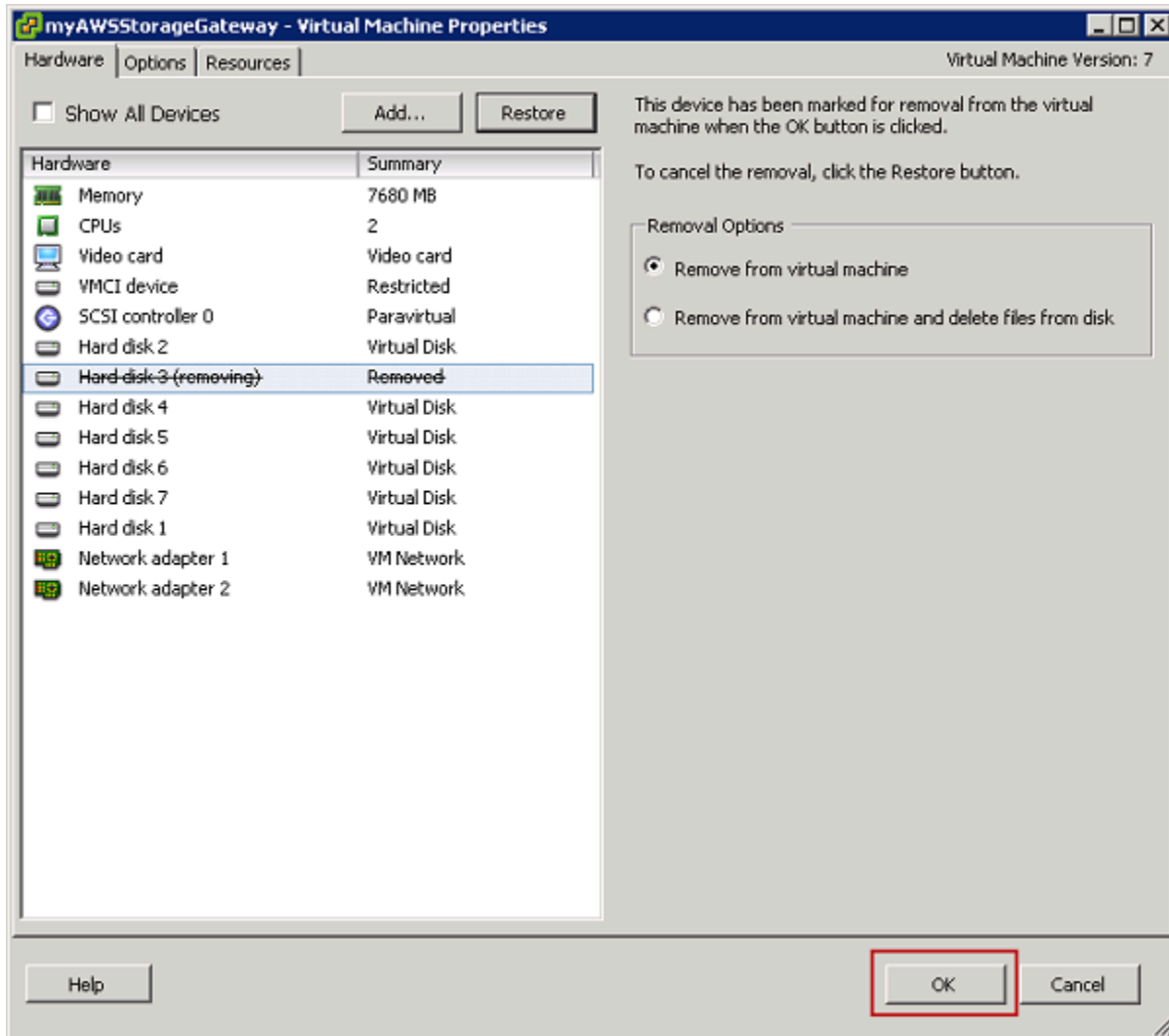
1. Nel vSphere client, apri il menu contestuale (fai clic con il pulsante destro del mouse), scegli il nome della tua macchina virtuale gateway, quindi scegli Modifica impostazioni.
2. Sulla scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), selezionare 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

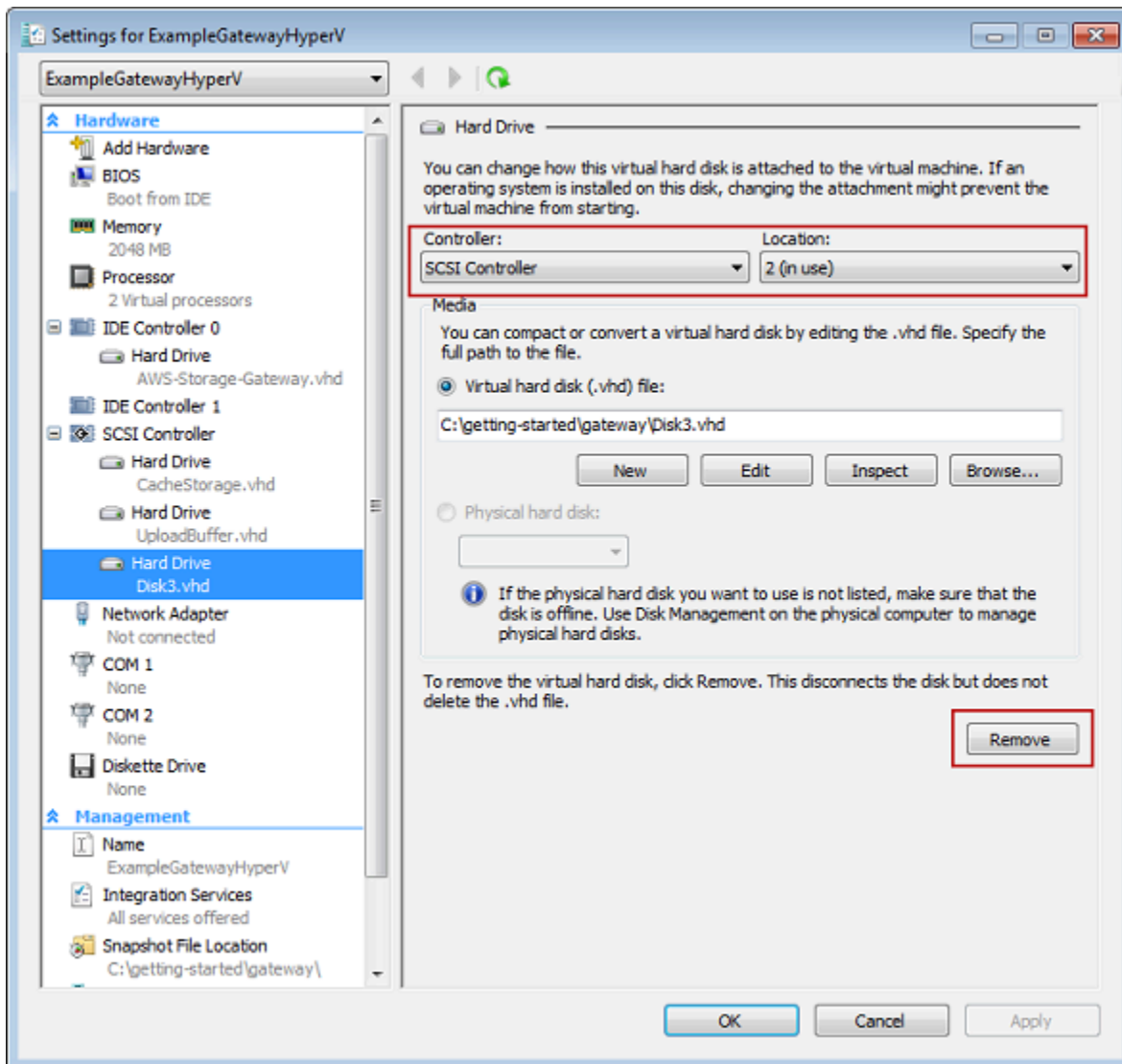
Utilizzando la seguente procedura, puoi rimuovere un disco dal gateway ospitato su un hypervisor Microsoft Hyper-V.

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 a un gateway vengono visualizzati sotto la voce SCSIController 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 SCSI controller 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 Virtual Machine (KVM) basato su Linux Kernel, puoi usare un `virsh` comando simile al seguente.

```
$ virsh detach-disk domain_name /device/path
```

Per ulteriori dettagli sulla gestione dei KVM dischi, consultate la documentazione della distribuzione Linux in uso.

## Aggiungere e rimuovere EBS volumi Amazon per i EC2 gateway Amazon

Quando hai inizialmente configurato il gateway per l'esecuzione come EC2 istanza Amazon, hai allocato EBS i volumi Amazon da utilizzare come buffer di caricamento e archiviazione cache. Nel tempo, man mano che le esigenze delle tue applicazioni cambiano, puoi allocare EBS volumi Amazon aggiuntivi per questo uso. Puoi anche ridurre lo spazio di archiviazione allocato rimuovendo i volumi Amazon EBS precedentemente allocati. Per ulteriori informazioni su AmazonEBS, consulta [Amazon Elastic Block Store \(AmazonEBS\)](#) nella Amazon EC2 User Guide.

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. Puoi allegare alla tua istanza tutti i EBS volumi Amazon che desideri, ma puoi configurare questi volumi solo come buffer di caricamento e spazio di archiviazione cache fino a queste quote di archiviazione. Per ulteriori informazioni, consulta [AWS Storage Gateway quote](#).

Per aggiungere un EBS volume Amazon e configurarlo per il tuo gateway

1. Crea un EBS volume Amazon. Per istruzioni, consulta [Creazione o ripristino di un EBS volume Amazon](#) nella Amazon EC2 User Guide.
2. Collega il EBS volume Amazon alla tua EC2 istanza Amazon. Per istruzioni, consulta [Allegare un EBS volume Amazon a un'istanza](#) nella Amazon EC2 User Guide.
3. Configura il EBS volume Amazon che hai aggiunto come buffer di caricamento o archiviazione 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 EBS volume Amazon

### Warning

Questi passaggi si applicano solo ai EBS volumi Amazon allocati come spazio buffer di caricamento, non ai volumi allocati alla cache.

1. Arrestare il gateway seguendo la procedura descritta nella sezione [Spegnimento della macchina virtuale gateway](#).
2. Scollega il EBS volume Amazon dalla tua EC2 istanza Amazon. Per istruzioni, consulta [Scollegare un EBS volume Amazon da un'istanza](#) nella Amazon EC2 User Guide.
3. Elimina il EBS volume Amazon. Per istruzioni, consulta [Eliminazione di un EBS volume Amazon](#) nella Amazon EC2 User Guide.
4. Avviare il gateway seguendo la procedura descritta nella sezione [Spegnimento della macchina virtuale gateway](#).

## Ottenimento di una chiave di attivazione per il gateway

Per ricevere una chiave di attivazione per il gateway, effettua una richiesta Web alla macchina virtuale (VM) del gateway. La macchina virtuale restituisce un reindirizzamento che contiene la chiave di attivazione, che viene passata come uno dei parametri dell'opzione `ActivateGateway` API per specificare la configurazione del gateway. Per ulteriori informazioni, vedere [ActivateGateway](#) lo Storage Gateway API Reference.

### Note

Le chiavi di attivazione del gateway scadono dopo 30 minuti se non vengono utilizzate.

La richiesta effettuata alla macchina virtuale gateway include la AWS regione in cui avviene l'attivazione. L'URL restituito dal reindirizzamento nella risposta contiene un parametro della stringa di query denominato `activationkey`. Questo parametro della stringa di query è la chiave di attivazione. Il formato della stringa di query ha un aspetto simile a questo: `http://gateway_ip_address?activationRegion=activation_region`. L'output di questa query restituisce sia la regione che la chiave di attivazione.

L'URL include anche `vpcEndpoint`, l'ID dell'endpoint VPC per i gateway che si connettono utilizzando il tipo di endpoint VPC.

### Note

L'appliance hardware Storage Gateway, i modelli di immagini VM e le Amazon Machine Images (AMI) di Amazon EC2 sono preconfigurati con i servizi HTTP necessari per ricevere e rispondere alle richieste Web descritte in questa pagina. Non è richiesta né consigliata l'installazione di servizi aggiuntivi sul gateway.

## Argomenti

- [Linux \(curl\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [Utilizzo della console locale](#)

## Linux (curl)

Gli esempi seguenti mostrano come recuperare una chiave di attivazione utilizzando Linux (curl).

### Note

Sostituisci le variabili evidenziate con i valori effettivi per il gateway. I valori accettabili sono i seguenti:

- *gateway\_ip\_address* - L'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. Consulta [Endpoint regionali nella Guida di riferimento](#) generale.AWS Se questo parametro non è specificato o se il valore fornito è digitato in modo errato o non corrisponde a una regione valida, il comando utilizzerà per impostazione predefinita la regione. `us-east-1`

- *vpc\_endpoint* - Il nome dell'endpoint VPC per il gateway, ad esempio.  
vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com

Per ottenere la chiave di attivazione per un endpoint pubblico:

```
curl "http://gateway_ip_address?activationRegion=region_code&no_redirect"
```

Per ottenere la chiave di attivazione per un endpoint VPC:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

## Linux (bash/zsh)

L'esempio seguente mostra come usare Linux (bash/zsh) per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function get-activation-key() {  
  local ip_address=$1  
  local activation_region=$2  
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then  
    echo "Usage: get-activation-key ip_address activation_region gateway_type"  
    return 1  
  fi  
  
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?  
activationRegion=$activation_region&gatewayType=$gateway_type"); then  
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')  
    echo "$activation_key_param" | cut -f2 -d=  
  else  
    return 1  
  fi  
}
```

## Microsoft Windows PowerShell

L'esempio seguente mostra come utilizzare Microsoft Windows PowerShell per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion,
        [parameter(Mandatory=$true)][string]$GatewayType
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=([A-Z0-9-]+)"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}
```

## Utilizzo della console locale

Nell'esempio seguente viene illustrato come utilizzare la console locale per generare e visualizzare una chiave di attivazione.

Come ottenere una chiave di attivazione per il gateway dalla console locale

1. 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 per scegliere Ottieni chiave di attivazione.
3. Seleziona Storage Gateway come opzione di famiglia di gateway.
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 per Standard o 2 per Federal Information Processing Standard (FIPS) come tipo di endpoint.

## Connessione degli SCSI iniziatori

Quando si gestisce il gateway, si lavora con volumi o dispositivi Virtual Tape Library (VTL) esposti come obiettivi di Internet Small Computer System Interface (iSCSI). Per i Volume Gateway, le SCSI destinazioni i sono volumi. Per i Tape Gateway, i target sono VTL i dispositivi. Nell'ambito di questo lavoro, svolgete attività come la connessione a tali destinazioni, la personalizzazione SCSI delle impostazioni i, la connessione da un client Red Hat Linux e la configurazione del Challenge-Handshake Authentication Protocol (). CHAP

### Argomenti

- [Connessione ai volumi in un client Windows](#)
- [Connessione di volumi o VTL dispositivi a un client Linux](#)
- [Personalizzazione delle impostazioni SCSI](#)
- [Configurazione dell'CHAPautenticazione per i tuoi obiettivi i SCSI](#)

Lo SCSI standard i è uno standard di rete di storage basato su IP (Internet Protocol) per l'avvio e la gestione delle connessioni tra dispositivi di storage e client basati su IP. L'elenco seguente definisce alcuni dei termini utilizzati per descrivere la SCSI connessione i e i componenti coinvolti.

### SCSIiniziatore i

Il componente client di una SCSI rete i. L'inziatore invia richieste al SCSI target i. Gli iniziatori possono essere implementati nel software o nell'hardware. Storage Gateway supporta solo gli iniziatori software.

### bersaglio i SCSI

Il componente server della SCSI rete i che riceve e risponde alle richieste degli iniziatori. Ciascuno dei tuoi volumi è esposto come target iSCSI. Connect un solo SCSI iniziatore i a ciascun SCSI target i.

### SCSIInziatore Microsoft i

Il programma software su computer Microsoft Windows che consente di connettere un computer client (ovvero il computer su cui è in esecuzione l'applicazione di cui si desidera scrivere i dati



sul gateway) a un array esterno SCSI basato su i (ovvero il gateway). La connessione viene effettuata usando la scheda di rete Ethernet del computer host. L'SCSIinizzatore Microsoft i 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.

Red Hat è un iniziatore SCSI

Il pacchetto `iscsi-initiator-utils` Resource Package Manager (RPM) fornisce un SCSI iniziatore i implementato nel software per Red Hat Linux. Il pacchetto include un demone server per il protocollo i. SCSI

Ogni tipo di gateway può connettersi ai SCSI dispositivi i ed è possibile personalizzare tali connessioni, come descritto di seguito.

## Connessione ai volumi in un client Windows

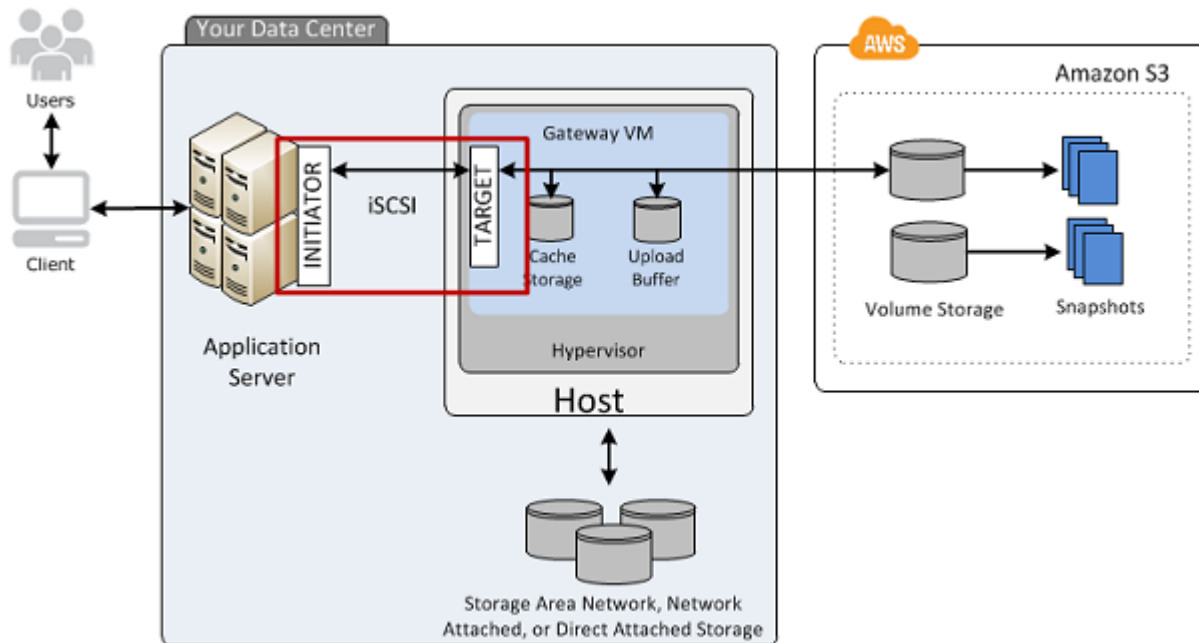
Un Volume Gateway espone i volumi creati per il gateway come destinazioni iSCSI. Per ulteriori informazioni, consulta [Collegamento dei volumi al tuo client](#).

### Note

Per la connessione al volume di destinazione, il gateway deve disporre di un buffer di caricamento configurato. Se un buffer di caricamento non è configurato per il gateway, lo stato dei volumi viene visualizzato come. `UPLOAD BUFFER NOT CONFIGURED`

Per configurare un buffer di caricamento per un gateway in una configurazione di volumi archiviati, consulta [Per configurare un buffer di caricamento o l'archiviazione della cache per il gateway](#). Per configurare un buffer di caricamento per un gateway in una configurazione di volumi nella cache, consulta [Per configurare un buffer di caricamento o l'archiviazione della cache per il gateway](#).

Il diagramma seguente evidenzia l'SCSlobiettivo i nel quadro più ampio dell'architettura Storage Gateway. Per ulteriori informazioni, consulta [Come funziona il gateway di volumi \(architettura\)](#).



È possibile connettersi al volume da un client Windows o Red Hat Linux. Facoltativamente, è possibile configurare CHAP per entrambi i tipi di client.

Il gateway espone il volume come SCSI destinazione i con un nome specificato dall'utente, preceduto da `iqn.1997-05.com.amazon:`. Ad esempio, se specifichi un nome di destinazione `dimyvolume`, il SCSI target i che usi per connetterti al volume è `iqn.1997-05.com.amazon:myvolume`. Per ulteriori informazioni su come configurare le applicazioni per montare volumi su iSCSI, vedere [Connessione ai volumi in un client Windows](#).

Per	See
Eeguire la connessione al volume da Windows.	<a href="#">Connessione a un client Microsoft Windows</a>
Eeguire la connessione al volume da Red Hat Linux.	<a href="#">Connessione a un client Red Hat Enterprise Linux</a>
Configura CHAP l'autenticazione per Windows e Red Hat Linux.	<a href="#">Configurazione dell'CHAPautenticazione per i tuoi obiettivi i SCSI</a>

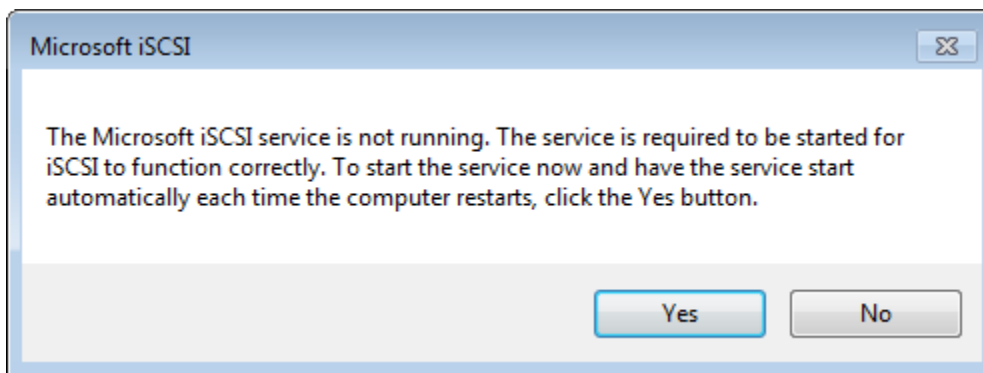
## Per connettere il client Windows a un volume di storage

1. Nel menu Start del computer client Windows, immettete **iscsicpl.exe** nella casella Cerca programmi e file, individuate il programma i SCSI initiator, quindi eseguitelo.

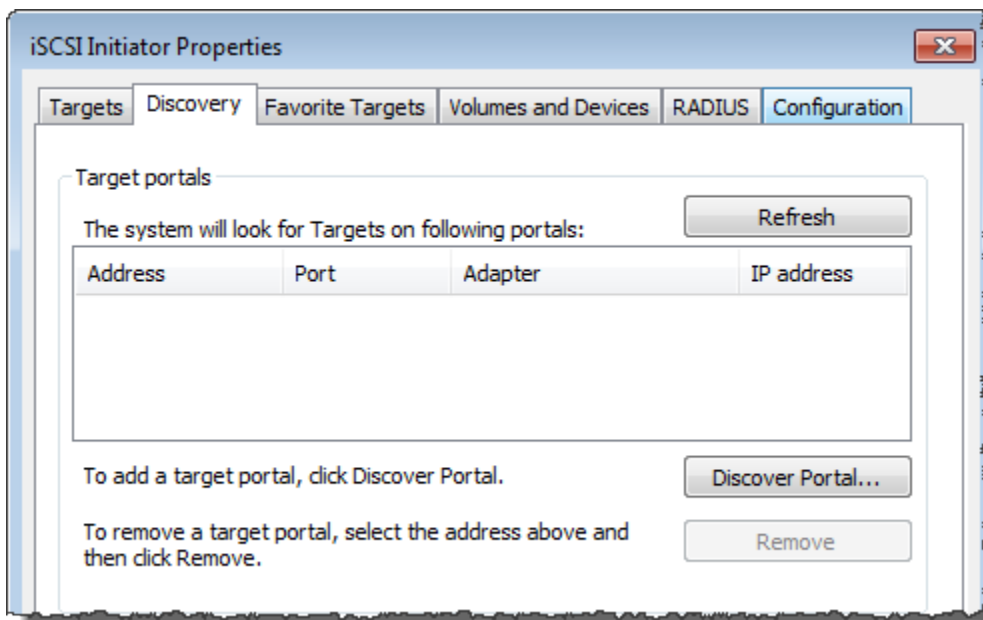
### Note

È necessario disporre dei diritti di amministratore sul computer client per eseguire l'iSCSI iniziatore i.

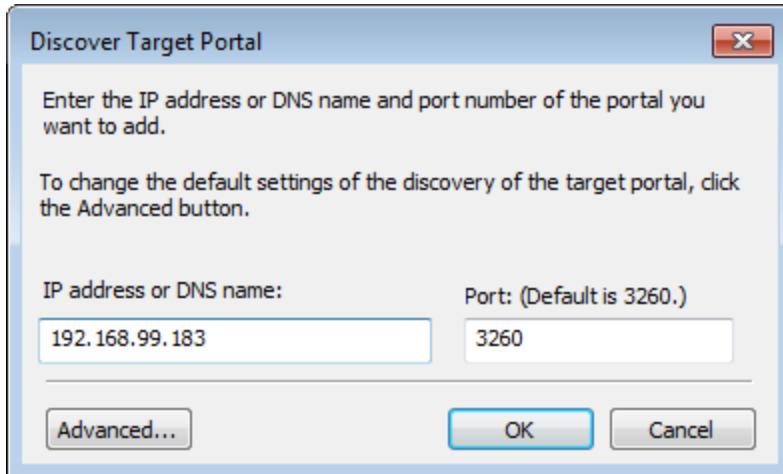
2. Se richiesto, scegli Sì per avviare il servizio Microsoft i SCSI Initiator.



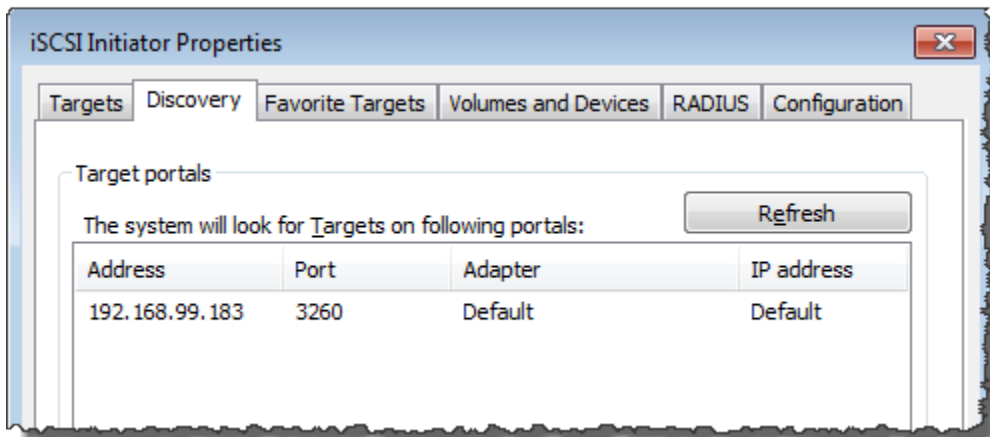
3. Nella finestra di dialogo i SCSI Initiator Properties, scegli la scheda Discovery, quindi scegli Discover Portal.



4. Nella finestra di dialogo Discover Target Portal, inserisci l'indirizzo IP del tuo iSCSI target come indirizzo IP o DNS nome, quindi scegli OK. Per ottenere l'indirizzo IP del gateway, fare riferimento alla scheda Gateway nella console Storage Gateway. Se hai distribuito il gateway su un'EC2istanza Amazon, puoi trovare l'IP o l'DNSindirizzo pubblico nella scheda Descrizione della EC2 console Amazon.



L'indirizzo IP verrà ora visualizzato nell'elenco Target portals (Portali destinazione) nella scheda Discovery (Individuazione).

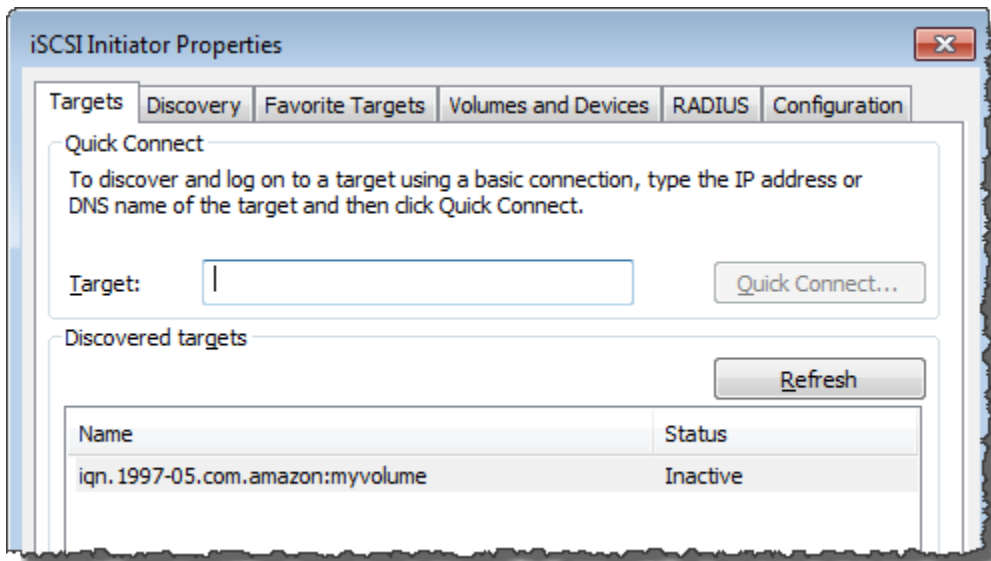


**Warning**

Per i gateway distribuiti su EC2 un'istanza Amazon, l'accesso al gateway tramite una connessione Internet pubblica non è supportato. L'indirizzo IP elastico dell'EC2istanza Amazon non può essere utilizzato come indirizzo di destinazione.

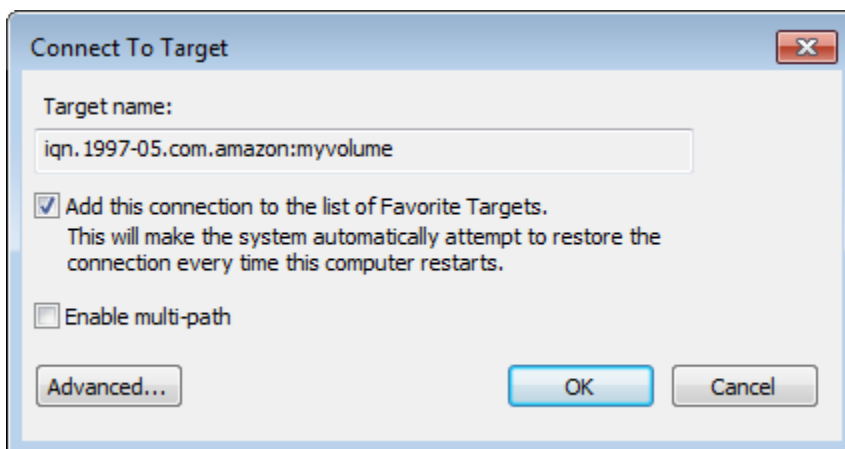
5. Connettere il nuovo portale di destinazione al volume di storage di destinazione nel gateway:
  - a. Scegliere la scheda Destinazioni.

Il nuovo portale di destinazione viene visualizzato con uno stato inattivo. Il nome della destinazione visualizzato deve corrispondere al nome specificato per il volume di storage nella fase 1.

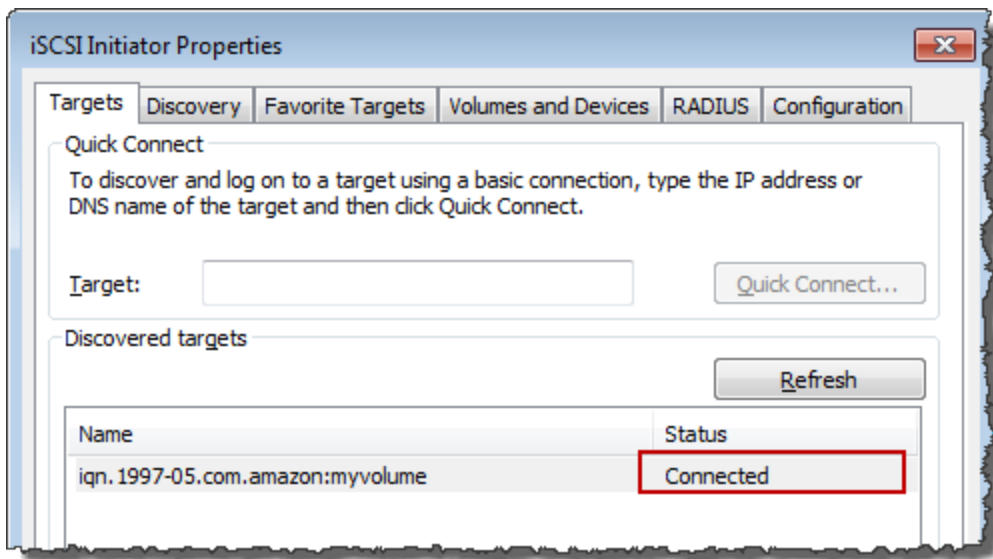


- b. Selezionare la destinazione e quindi scegliere Connect (Connetti).

Se il nome della destinazione non è già compilato, immettere il nome della destinazione come mostrato nel passaggio 1. Nella finestra di dialogo Connetti alla destinazione, seleziona Aggiungi questa connessione all'elenco delle destinazioni preferite, quindi scegli OK.



- c. Nella scheda Destinazioni assicurarsi che nella colonna Stato per la destinazione sia presente il valore Connesso, che indica che la destinazione è connessa, quindi scegliere OK.



È ora possibile inizializzare e formattare il volume di storage per Windows, in modo da poter iniziare a salvare i dati al suo interno. A tale scopo, usa lo strumento Gestione disco di Windows.

#### Note

Sebbene non sia necessario per questo esercizio, si consiglia vivamente di personalizzare SCSI le impostazioni i per un'applicazione reale, come illustrato in [Personalizzazione delle impostazioni di Windows i SCSI](#)

## Connessione di volumi o VTL dispositivi a un client Linux

Quando si utilizza Red Hat Enterprise Linux (RHEL), si utilizza il `iscsi-initiator-utils` RPM pacchetto per connettersi ai SCSI target gateway i (volumi o VTL dispositivi).

Per connettere un client Linux ai SCSI target i

1. Installa il `iscsi-initiator-utils` RPM pacchetto, se non è già installato sul tuo client.

Puoi utilizzare il seguente comando per installare il pacchetto.

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

2. Assicurati che il SCSI demone i sia in esecuzione.

- a. Verificate che il SCSI demone i sia in esecuzione utilizzando uno dei seguenti comandi.

Per RHEL 5 o 6, usate il seguente comando.

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

Per RHEL 7, usa il seguente comando.

```
sudo service iscsid status
```

- b. Se il comando status non restituisce uno stato in esecuzione, avviare il daemon usando uno dei comandi seguenti.

Per RHEL 5 o 6, usa il seguente comando.

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

Per RHEL 7, usa il seguente comando. Per RHEL 7, di solito non è necessario avviare esplicitamente il `iscsid` servizio.

```
sudo service iscsid start
```

3. Per scoprire le destinazioni del volume o VTL del dispositivo definite per un gateway, utilizzate il seguente comando `discovery`.

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

Sostituisci l'indirizzo IP del gateway con `[GATEWAY_IP]` variabile nel comando precedente. È possibile trovare l'IP del gateway nelle proprietà i SCSI Target Info di un volume sulla 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 SCSI qualificato i (IQN) sarà diverso da quello mostrato in precedenza, perché IQN i valori sono unici per un'organizzazione. Il nome della destinazione è il nome specificato quando viene creato il volume. È inoltre possibile trovare questo nome di destinazione nel riquadro delle proprietà i SCSI Target Info quando si seleziona un volume sulla console Storage Gateway.

4. Per connettersi a una destinazione, utilizzare il seguente comando.

Si noti che è necessario specificare il valore corretto `[GATEWAY_IP]` e IQN nel comando `connect`.

 Warning

Per i gateway distribuiti su EC2 un'istanza Amazon, l'accesso al gateway tramite una connessione Internet pubblica non è supportato. L'indirizzo IP elastico dell'EC2istanza Amazon non può essere utilizzato 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
```

Ti consigliamo vivamente di personalizzare le SCSI impostazioni i dopo aver configurato l'iniziatore, come illustrato in [Personalizzazione delle impostazioni di Linux i SCSI](#).



## Personalizzazione delle impostazioni SCSI

Dopo aver configurato l'iniziatore, si consiglia vivamente di personalizzare SCSI le impostazioni i per evitare che l'iniziatore si disconnetta dalle destinazioni.

Aumentando i valori di SCSI timeout i come illustrato nei passaggi seguenti, migliorate la capacità dell'applicazione di gestire meglio le operazioni di scrittura che richiedono molto tempo e altri problemi transitori 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 di Windows i SCSI](#)
- [Personalizzazione delle impostazioni di Linux i SCSI](#)
- [Personalizzazione delle impostazioni di timeout del disco di Linux per i gateway di volumi](#)

## Personalizzazione delle impostazioni di Windows i SCSI


Quando si utilizza un client Windows, si utilizza l'SCSIiniziatore Microsoft i per connettersi al volume del gateway. Per istruzioni su come connetterti ai volumi, consulta [Collegamento dei volumi al tuo client](#).

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.

### Per personalizzare le impostazioni di Windows i SCSI

1. Aumentare il tempo massimo durante il quale lasciare in coda le richieste.
  - a. Avviare l'editor del Registro di sistema (`Regedit.exe`).

- b. Passa alla chiave identificatore univoco globale (GUID) per la classe di dispositivo che contiene le impostazioni SCSI del controller i, mostrata di seguito.

 Warning

Accertatevi di utilizzare la `CurrentControlSet` sottochiave e non un altro set di controlli, ad esempio `ControlSet001` o `ControlSet 002`.

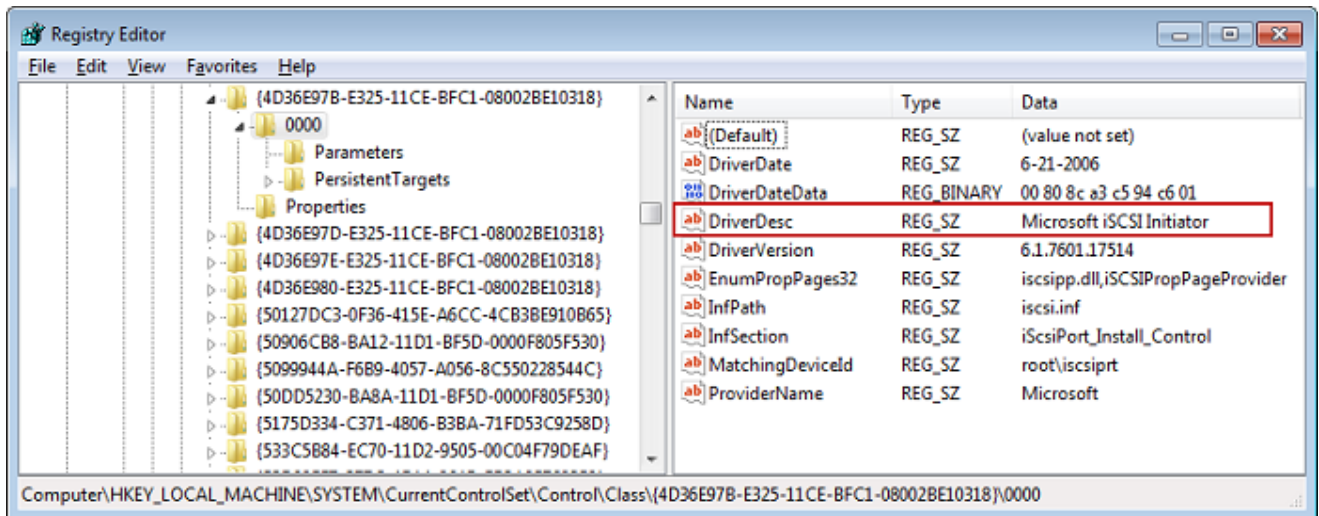
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. Trova la sottochiave per l'SCSI iniziatore Microsoft i, mostrata di seguito come [*<Instance Number>*].

La chiave è rappresentata da un numero a quattro cifre, ad esempio `0000`.

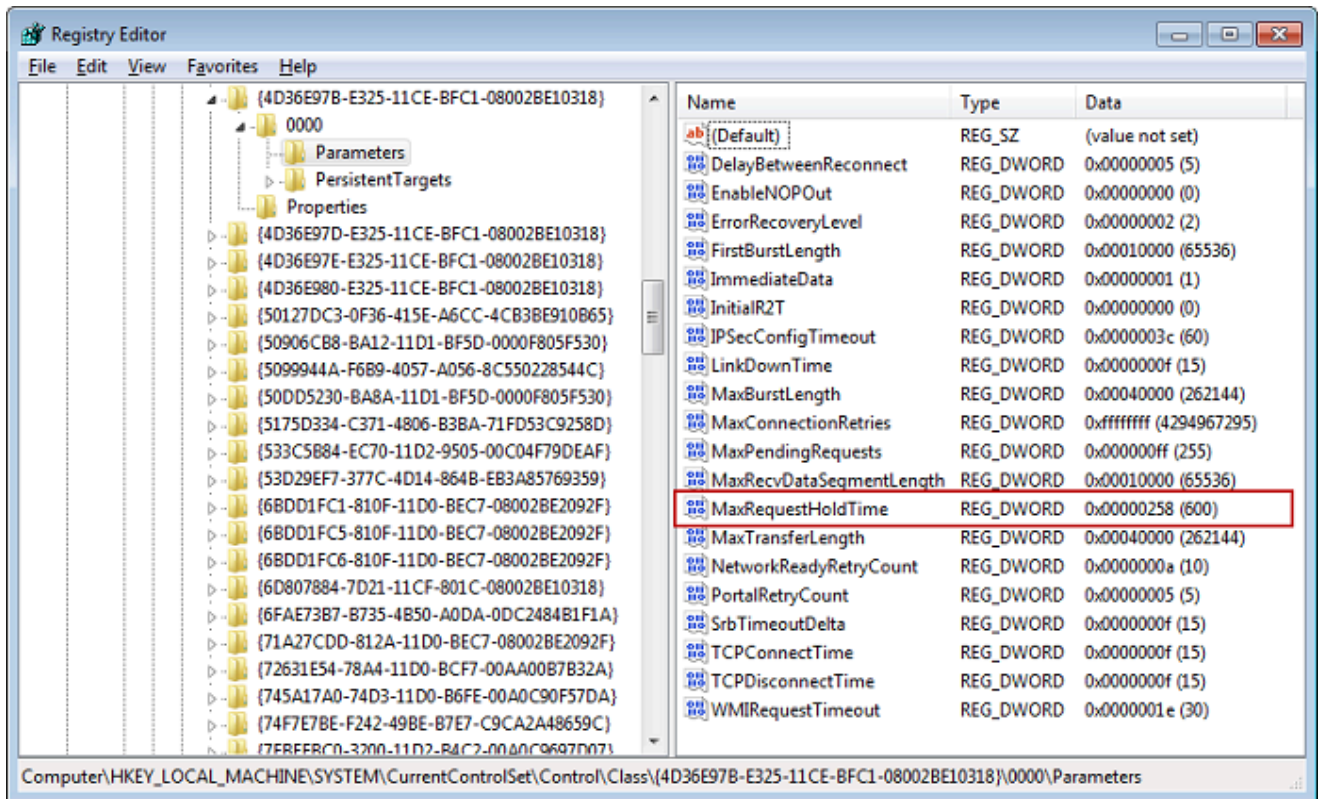
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number>]
```

A seconda del dispositivo installato nel computer, l'SCSI iniziatore Microsoft i potrebbe non essere la `0000` sottochiave. 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.

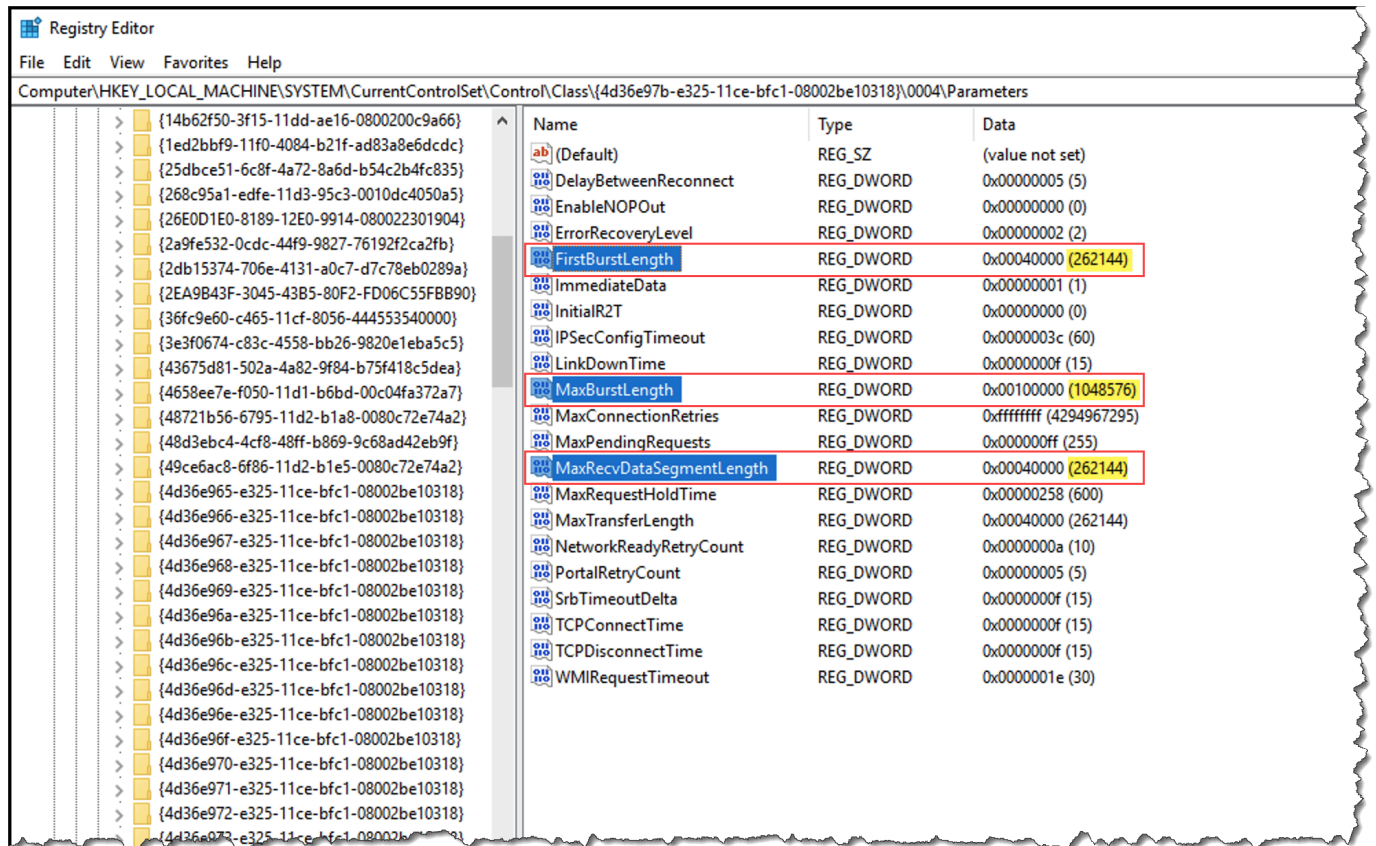


- d. Per mostrare SCSI le impostazioni i, selezionare la sottochiave Parameters.
- e. Aprite il menu contestuale (fate clic con il pulsante destro del mouse) per il valore MaxRequestHoldTimeDWORD(32 bit), scegliete Modifica, quindi modificate il valore in. **600**

MaxRequestHoldTimespecifica per quanti secondi Microsoft i SCSI initiator deve tenere premuti 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 in SCSI pacchetti i modificando i parametri seguenti:
- **FirstBurstLength** controlla 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.
  - **MaxBurstLength** è 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.
  - **MaxRecvDataSegmentLength** controlla 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:

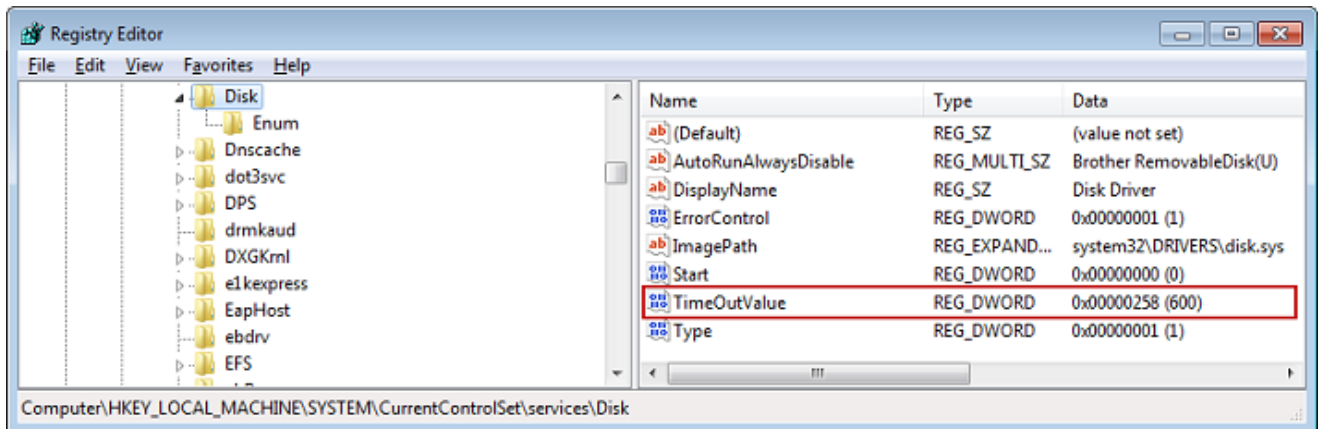
- a. Se non è già stato fatto, avviare l'editor del Registro di sistema (Regedit.exe).
- b. Accedere alla sottochiave Disk nella sottochiave Services di CurrentControlSet, illustrata di seguito.

HKEY\_Local\_Machine\SYSTEM\CurrentControlSet\Services\Disk

- c. Aprite il menu contestuale (fate clic con il pulsante destro del mouse) per il valore TimeoutValueDWORD(32 bit), scegliete Modifica, quindi modificate il valore in **600**

TimeoutValue specifica per quanti secondi l'ISCSIniziatore 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 di Linux i SCSI

Dopo aver configurato l'initiator per il gateway, si consiglia vivamente di personalizzare SCSI le impostazioni i per evitare che l'initiator si disconnetta dalle destinazioni. Aumentando i valori di SCSI timeout i come illustrato di seguito, migliorate la capacità dell'applicazione di gestire meglio le operazioni di scrittura che richiedono molto tempo e altri problemi transitori 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 di Linux i SCSI

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. Impostazione della proprietà `[replacement_timeout_value]` valore per **600**.

Impostazione della proprietà `[noop_out_interval_value]` valore per **60**.

Impostazione della proprietà `[noop_out_timeout_value]` valore per **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.

Impostazione della proprietà `[replacement_first_burst_length_value]` value to **262144** o l'impostazione predefinita del sistema operativo Linux, a seconda di quale sia il più alto.

Impostazione della proprietà `[replacement_max_burst_length_value]` value to **1048576** o il valore predefinito del sistema operativo Linux, a seconda di quale sia il più alto.

Impostazione della proprietà `[replacement_segment_length_value]` value to **262144** o il valore predefinito del sistema operativo Linux, a seconda di quale sia il più alto.

 Note

È possibile ottimizzare diversi software di backup per funzionare al meglio utilizzando diverse SCSI impostazioni. 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, accertarsi che i risultati di tutte le operazioni di scrittura nei nastri vengano scaricate. A tale scopo, smonta i nastri prima di riavviarle.

## Personalizzazione delle impostazioni di timeout del disco di Linux per i gateway di volumi

Se si utilizza un Volume Gateway, è possibile personalizzare le seguenti impostazioni di timeout del disco Linux oltre alle SCSI impostazioni i descritte nella sezione precedente.

Per personalizzare le impostazioni di timeout del disco di Linux

1. Aumentare il valore di timeout del disco nel file delle regole.
  - a. Se utilizzate l'iniziatore RHEL 5, aprite il `/etc/udev/rules.d/50-udev.rules` file e cercate la riga seguente.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$DEVPATH/timeout'"
```

Questo file di regole non esiste in RHEL 6 o 7 iniziatori, quindi è necessario crearlo utilizzando la seguente regola.



```
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, utilizzate il comando seguente e aggiungete le righe di codice mostrate in precedenza.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Per modificare il valore di timeout in RHEL 7, utilizzate il comando seguente e aggiungete le righe di codice mostrate in precedenza.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

- b. Impostazione della proprietà *[timeout]* valore a. **600**

Questo valore rappresenta un timeout di 600 secondi.

2. Riavviare il sistema perché i nuovi valori di configurazione vengano applicati.

Prima di riavviare, accertarsi che i risultati di tutte le operazioni di scrittura nei volumi vengano scaricati. 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 SCSI dispositivo i.

## Configurazione dell'CHAPautenticazione per i tuoi obiettivi i SCSI

Storage Gateway supporta l'autenticazione tra il gateway e SCSI gli initiator utilizzando Challenge-Handshake Authentication Protocol (). CHAP CHAPfornisce protezione dagli attacchi di riproduzione verificando periodicamente l'identità di un SCSI iniziatore i autenticato per accedere a un volume e a un dispositivo di destinazione. VTL

### Note

CHAPla configurazione è facoltativa ma altamente consigliata.

Per eseguire la configurazione CHAP, è necessario configurarla sia nella console Storage Gateway che nel software i SCSI initiator utilizzato per la connessione alla destinazione. Storage Gateway utilizza mutuo CHAP, ovvero quando l'iniziatore autentica la destinazione e la destinazione autentica l'iniziatore.

Per configurare Mutual per i tuoi obiettivi CHAP

1. Effettuare la configurazione CHAP sulla console Storage Gateway, come descritto in [CHAPPer configurare una destinazione di volume sulla console Storage Gateway](#).
2. Nel software Client Initiator, completa la CHAP configurazione:
  - Per configurare mutuo CHAP su un client Windows, vedi [Per configurare mutuo CHAP su un client Windows](#).
  - Per configurare mutuo CHAP su un client Red Hat Linux, vedi [Per configurare mutuo CHAP su un client Red Hat Linux](#).

CHAPPer configurare una destinazione di volume sulla console Storage Gateway

In questa procedura è necessario specificare due chiavi segrete che vengono usate per leggere e scrivere in un volume. Le stesse chiavi vengono usate nella procedura per configurare l'iniziatore client.

1. Dalla console Storage Gateway, scegliere Volumi nel pannello di navigazione.
2. Per Azioni, selezionare Configura CHAP autenticazione.
3. Fornite le informazioni richieste nella finestra di dialogo Configura CHAP autenticazione.
  - a. Per il nome dell'iniziatore, immettete il nome dell'iSCSIiniziatore i. Questo nome è un nome SCSI qualificato Amazon i (IQN) preceduto da `iqn.1997-05.com.amazon:` un nome di destinazione. Di seguito è riportato un esempio.

`iqn.1997-05.com.amazon:your-volume-name`

Puoi trovare il nome dell'iniziatore usando il tuo software i SCSI Initiator. Ad esempio, per i client Windows, il nome è il valore nella scheda Configurazione dell'iniziatore iSCSI. Per ulteriori informazioni, consulta [Per configurare mutuo CHAP su un client Windows](#).

**Note**

Per modificare il nome di un iniziatore, è necessario innanzitutto disattivarlo CHAP, modificare il nome dell'iniziatore nel software i SCSI Initiator e quindi eseguire l'attivazione CHAP con il nuovo nome.

- b. Per Segreto utilizzato per autenticare l'iniziatore, immettere 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 alla destinazione. CHAP

- c. Per Secret used to Authenticate Target (MutualCHAP), inserisci 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 il target deve conoscere per partecipare CHAP con l'iniziatore.

**Note**

Il segreto usato per autenticare la destinazione deve essere diverso dal segreto usato per autenticare l'iniziatore.

- d. Seleziona Salva.

4. Scegli la scheda Dettagli e conferma che SCSI CHAP l'autenticazione i sia impostata su true.



Per configurare mutuo CHAP su un client Windows

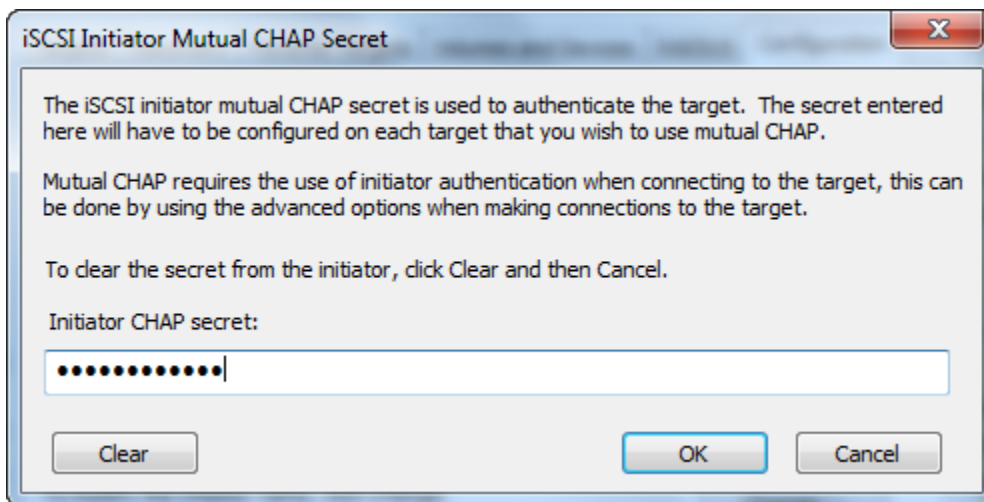
In questa procedura, si esegue la configurazione CHAP nell'SCSI iniziatore Microsoft i utilizzando gli stessi tasti utilizzati CHAP per configurare il volume sulla console.

1. Se l'iSCSI iniziatore non è già avviato, nel menu Start del computer client Windows, scegli Esegui **iscsicpl.exe**, invio e quindi scegli OK per eseguire il programma.
2. Configurate la CHAP configurazione reciproca per l'iniziatore (ovvero il 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 è il valore utilizzato nella finestra di dialogo Configura CHAP autenticazione della console Storage Gateway.  
Il nome visualizzato nell'immagine di esempio è solo per scopo dimostrativo.

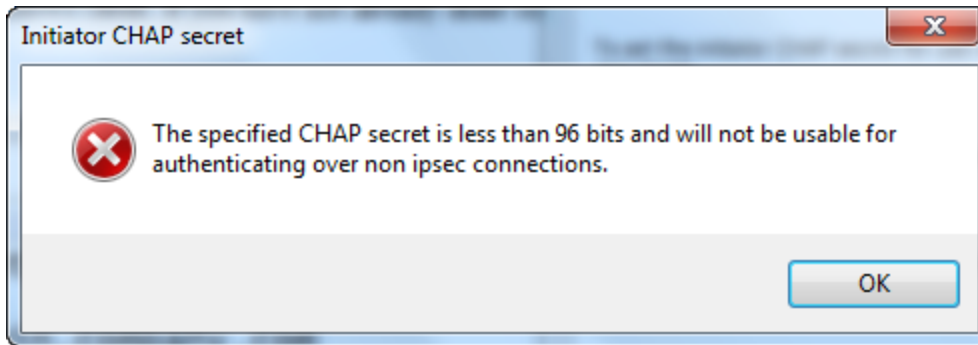
- b. Scegli CHAP.
- c. Nella finestra di dialogo iSCSI Initiator Mutual Chap Secret, immettere il valore del CHAP segreto reciproco.



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 è uguale a quello inserito nella casella Segreto usato per autenticare Target (MutualCHAP) nella finestra di dialogo Configura CHAP autenticazione. Per ulteriori informazioni, consulta [Configurazione dell'CHAP autenticazione per i tuoi obiettivi iSCSI](#).

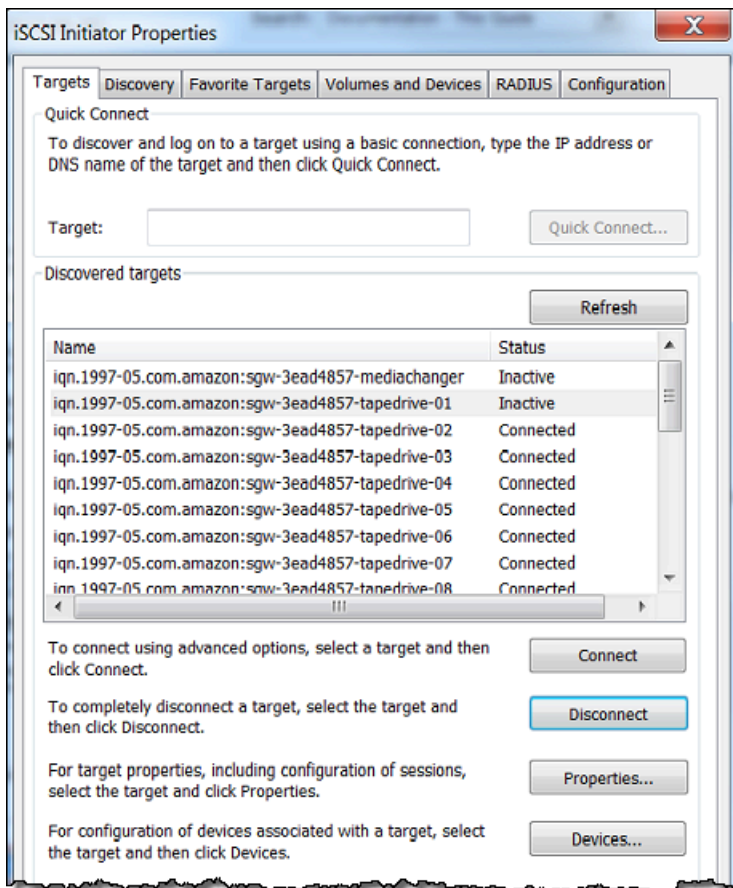
- d. Se la chiave inserita è inferiore a 12 caratteri o superiore a 16 caratteri, viene visualizzata una finestra di dialogo di errore CHAP segreto dell'iniziatore.

Scegliere OK e quindi immettere di nuovo la chiave.



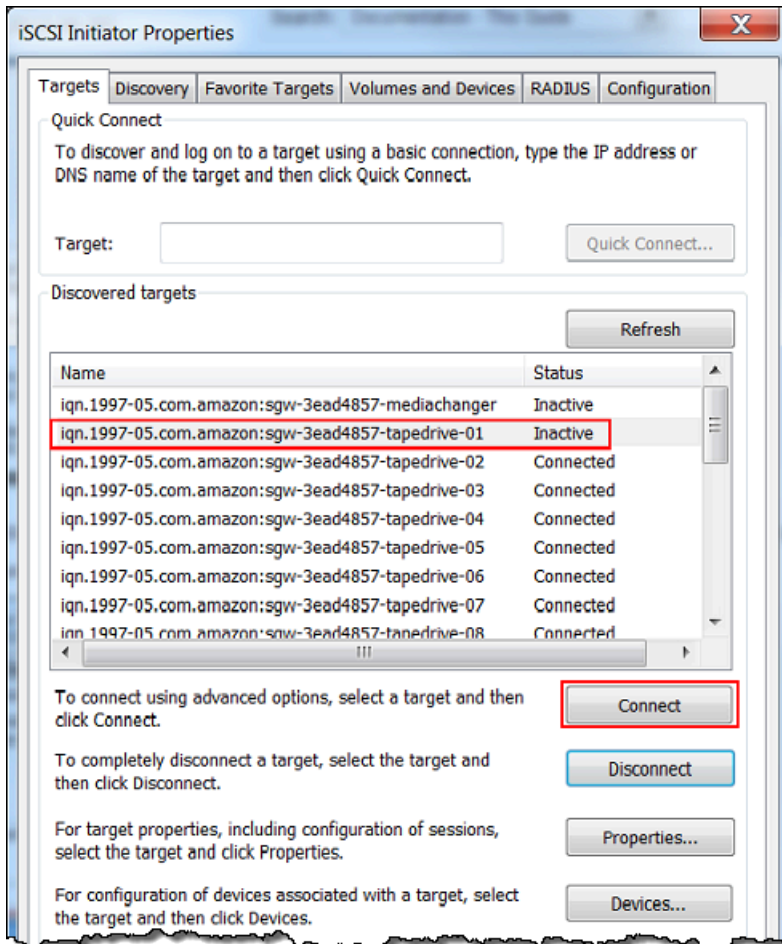
3. Configura la destinazione con il segreto dell'iniziatore per completare la configurazione reciproca CHAP

a. Scegliere la scheda Destinazioni.

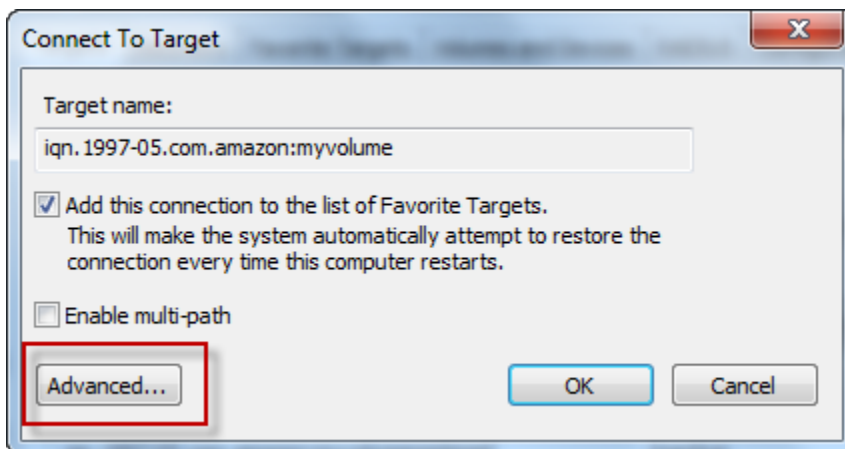


b. Se la destinazione per cui desideri configurare CHAP è attualmente connessa, disconnetti la destinazione selezionandola e scegliendo Disconnetti.

- c. Seleziona la destinazione per cui desideri configurare CHAP, quindi scegli Connect.

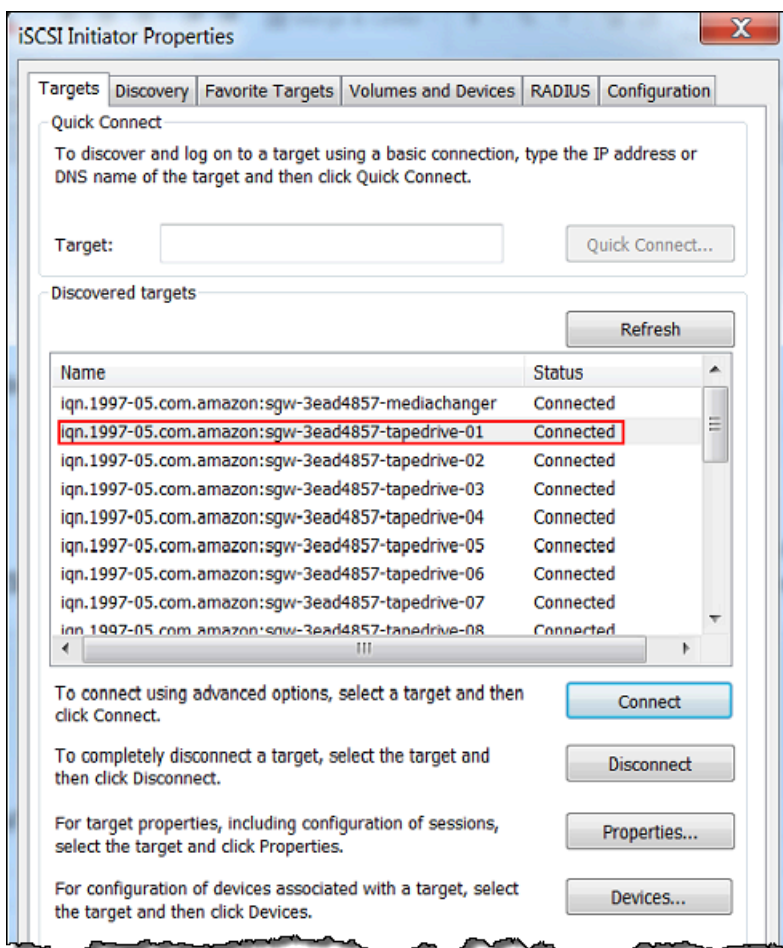


- d. Nella finestra di dialogo Connect to Target (Connetti a destinazione) scegliere Advanced (Avanzate).



- e. Nella finestra di dialogo Impostazioni avanzate, configura CHAP.

- i. Seleziona Attiva CHAP accesso.
  - ii. Digitare il segreto necessario per autenticare l'inziatore. Questo segreto è uguale a quello immesso nella casella Segreto usato per autenticare l'inziatore nella finestra di dialogo Configura l'CHAPautenticazione. Per ulteriori informazioni, consulta [Configurazione dell'CHAPautenticazione per i tuoi obiettivi i SCSI](#).
  - 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 mutuo CHAP su un client Red Hat Linux

In questa procedura, si configura CHAP nell'SCSIinziatore Linux i utilizzando le stesse chiavi utilizzate CHAP per configurare il volume sulla console Storage Gateway.

1. Assicuratevi che il SCSI demone i sia in esecuzione e che vi siate già connessi a una destinazione. Se non hai completato queste due attività, consulta [Connessione a un client Red Hat Enterprise Linux](#) .
2. Disconnettete e rimuovete qualsiasi configurazione esistente per la destinazione per la quale state per configurarla. 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 si disconnette dalla destinazione denominata **myvolume** definita in Amazon i SCSI qualified name (IQN). Cambia il nome del bersaglio e IQN come richiesto dalla tua situazione.

```
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. Modifica il file SCSI di configurazione i per attivarloCHAP.

- a. Ottenere il nome dell'inziatore, ovvero il client in uso.

Il comando seguente ottiene il nome dell'inziatore 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. Decomentate le seguenti righe del file e specificate 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
<i>username</i>	Nome dell'inziatore individuato in una fase precedente in questa procedura. Il valore inizia con iqn. Ad esempio, <b>iqn.1994-05.com.redhat:8e89b27b5b8</b> è valido <i>username</i> valore.
<i>password</i>	Chiave segreta usata per autenticare l'inziatore (il client in uso) quando comunica con il volume.
<i>username_in</i>	Il volume IQN di destinazione. Il valore inizia con iqn e termina con il nome della destinazione. Ad esempio, <b>iqn.1997-05.com.amazon:myvolume</b> è valido <i>username_in</i> valore.
<i>password_in</i>	Chiave segreta usata per autenticare la destinazione (il volume) quando comunica con l'inziatore.

- d. Salvare le modifiche nel file di configurazione e quindi chiudere il file.
4. Individuare la destinazione e accedervi. Per farlo, segui i passaggi descritti in [Connessione a un client Red Hat Enterprise 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 VPC endpoint devono essere creati con. HAProxy Per ulteriori informazioni, consulta [Creazione di un'interfaccia virtuale](#) nella Guida per l'utente di AWS Direct Connect .

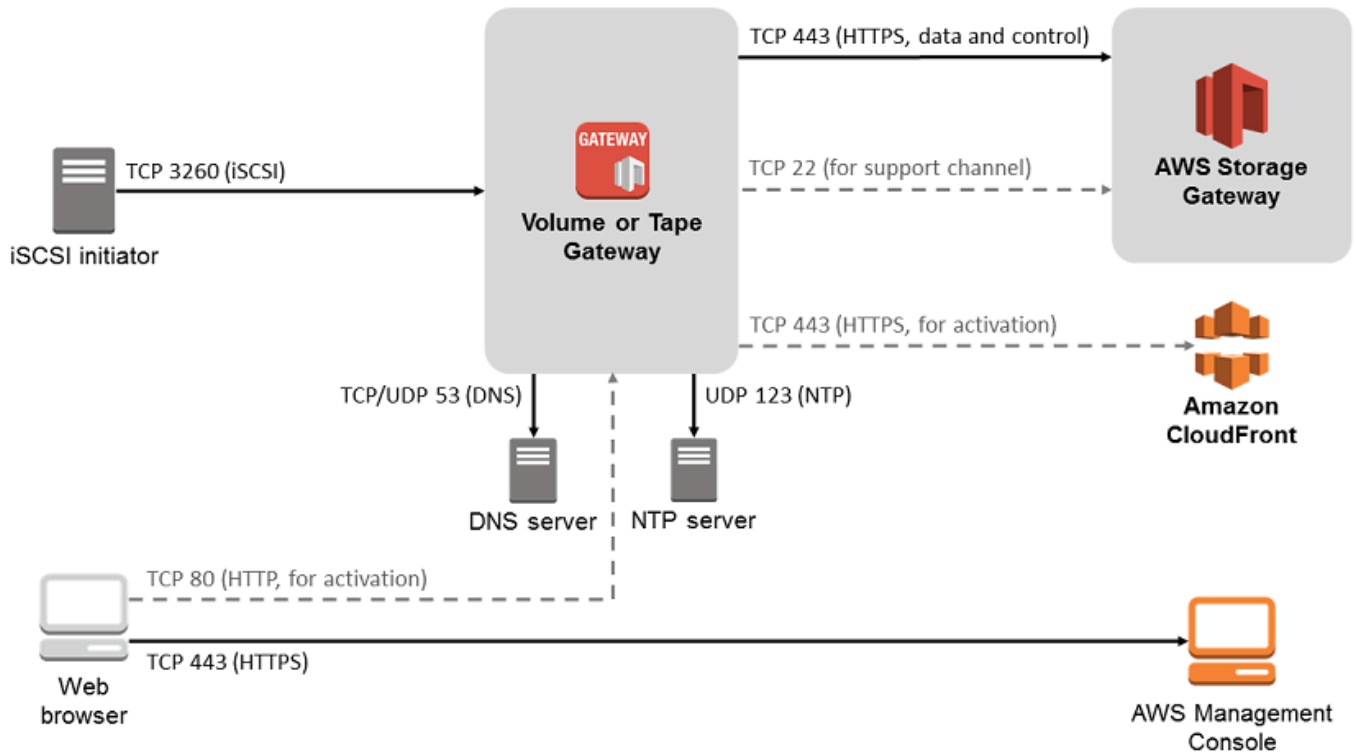
Per ulteriori informazioni AWS Direct Connect, consulta [Cos'è AWS Direct Connect?](#) nella Guida AWS Direct Connect per l'utente.

## Requisiti delle porte di rete per Volume Gateway

Per il corretto funzionamento di Storage Gateway, sono necessarie le porte seguenti. Alcune porte sono comuni e sono 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 volumi.

Gateway di volumi

La figura seguente mostra tutte le porte che devi aprire per il funzionamento dei gateway di volumi.



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

Da	Per	Protocollo	Porta	Modalità di utilizzo
Macchina virtuale Storage Gateway	AWS	Protocollo di controllo della trasmissione (TCP)	43 () HTTPS	Per la comunicazione da una macchina virtuale in uscita dello Storage Gateway a un endpoint di AWS servizio. Per informazioni sugli endpoint

Da	Per	Protocollo	Porta	Modalità di utilizzo	
				del servizio, consulta <a href="#">Consentire AWS Storage Gateway l'accesso tramite firewall e router.</a>	

Da	Per	Protocollo	Porta	Modalità di utilizzo
Browser	Macchina virtuale Storage Gateway	TCP	80 () HTTP	<p>Dai sistemi locali per ottenere la chiave di attivazione di Storage Gateway. La porta 80 viene usata solo durante l'attivazione di un'appliance Storage Gateway.</p> <p>Per una macchina virtuale Storage Gateway la porta 80 non deve essere accessibile pubblicamente. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. Se attivi il gateway dalla console di</p>

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 Domain Name Service (DNS)	User Datagram Protocol ()/ UDPUDP	53 () DNS	Per la comunicazione tra una macchina virtuale Storage Gateway e il DNS server.

Da	Per	Protocollo	Porta	Modalità di utilizzo	
Macchina virtuale Storage Gateway	AWS	TCP	22 (Canale di supporto)	Consente di accedere 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 Network Time Protocol (NTP)	UDP	123 (NTP)	<p>Utilizzato dai sistemi locale per sincronizzare l'ora della VM con quella dell'host. Una macchina virtuale Storage Gateway è configurata per utilizzare i seguenti NTP server:</p> <ul style="list-style-type: none"><li>• 0.amazon.pool.ntp.org</li><li>• 1.amazon.pool.ntp.org</li><li>• 2.amazon.pool.ntp.org</li><li>• 3.amazon.pool.ntp.org</li></ul>



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 volumi richiedono le seguenti porte.

Da	Per	Protocollo	Porta	Modalità di utilizzo
i SCSI iniziatori	Macchina virtuale Storage Gateway	TCP	3260 (i) SCSI	Tramite sistemi locali per la connessione a i SCSI target esposti 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 EC2 gateway Amazon, puoi anche ottenere l'indirizzo IP della tua EC2 istanza Amazon dalla Console di EC2 gestione Amazon. Per informazioni su come ottenere l'indirizzo IP del gateway, consulta:

- VMwareospitante: [Accesso alla console locale del Gateway con VMware ESXi](#)
- Host HyperV: [Accesso alla console locale del gateway con Microsoft Hyper-V](#)

- Host Virtual Machine (KVM) basato su kernel Linux: [Accesso alla console locale del gateway con Linux KVM](#)
- EC2host: [Ottenere un indirizzo IP da un EC2 host Amazon](#)

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 EC2 host Amazon

Per ottenere l'indirizzo IP dell'EC2istanza Amazon su cui è distribuito il gateway, accedi alla console locale dell'EC2istanza. Quindi ottenere l'indirizzo IP nella parte superiore della pagina della console. Per istruzioni, consulta [Accesso alla console locale di Amazon EC2 Gateway](#).

Puoi anche ottenere l'indirizzo IP dalla Console di EC2 gestione Amazon. 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 EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, scegli Istanze, quindi seleziona l'EC2istanza su cui 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 EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, scegli Istanze, quindi seleziona l'EC2istanza su cui 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, scegli il gateway che hai appena attivato, quindi scegli la scheda VTLdispositivi nel pannello inferiore.
5. Ottieni i nomi di tutti i tuoi VTL dispositivi.
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'EC2istanza.

## Informazioni sulle risorse e sulle risorse dello Storage Gateway IDs

In Storage Gateway, la risorsa principale è un gateway, ma altri tipi di risorse includono: volume, nastro virtuale, i SCSI target e dispositivo vtl. In questo caso, si parla di risorse secondarie, che non esistono a meno che non siano state associate a un gateway.

A queste risorse e sottorisorse sono associati Amazon Resource Names (ARNs) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	ARNFormato
Gateway ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
Volume ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
Obiettivo ARN (SCSIobiettivo I)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSItarget</i>

Storage Gateway supporta anche l'uso di EC2 istanze, EBS volumi e istantanee. Queste risorse sono EC2 risorse Amazon utilizzate in Storage Gateway.

## Lavorare con Resource IDs

Quando crei una risorsa, Storage Gateway assegna a tale risorsa un ID risorsa univoco. Questo ID di risorsa fa parte della risorsaARN. 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.

**IDs**Le risorse Storage Gateway sono in lettere maiuscole. Tuttavia, quando utilizzi queste risorse IDs con Amazon EC2API, Amazon EC2 si aspetta che le risorse siano IDs in lettere minuscole. È necessario modificare l'ID della risorsa in minuscolo per utilizzarla con EC2 API. Ad esempio, in Storage Gateway l'ID per un volume può essere `vol-1122AABB`. Quando si utilizza questo ID con EC2API, è necessario modificarlo in `vol-1122aabb`. In caso contrario, EC2 API 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 per l'uso di AWS .
- I caratteri validi per la proprietà key sono UTF -8 lettere e numeri, spazi e caratteri speciali `+ - = . _ /` e `@`.

## Lavorare con i tag

È possibile utilizzare i tag utilizzando la console Storage Gateway, lo Storage Gateway API o [l'interfaccia a riga di comando di Storage Gateway \(CLI\)](#). Le procedure seguenti illustrano come aggiungere, modificare ed eliminare un tag dalla console.

Per aggiungere un tag

1. Apri la console Storage Gateway a <https://console.aws.amazon.com/storagegateway/casa>.
2. Nel riquadro di navigazione, scegliere la risorsa a cui vuoi applicare un tag.

Ad esempio, per applicare tag a un gateway, scegliere Gateways (Gateway), quindi scegliere il gateway che si desidera contrassegnare con dei tag dall'elenco di gateway.

3. Scegliere Tags (Tag), quindi Add tag (Aggiungi tag).
4. Nella finestra di dialogo Add/edit tags (Aggiungi/Modifica tag), selezionare Add New Volume (Aggiungi nuovo volume).
5. Digita una chiave per Key (Chiave) e un valore per Value (Valore). Ad esempio, è possibile digitare **Department** per la chiave e **Accounting** per il valore.

### Note

È possibile lasciare la casella Value (Valore) vuota.

6. Per aggiungere altri tag, scegliere Create Tag (Crea tag). È possibile aggiungere più tag a una risorsa.
7. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Per modificare un tag

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

2. Scegliere la risorsa con il tag da modificare.
3. Scegliere Tags (Tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. 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 a <https://console.aws.amazon.com/storagegateway/casa>.
2. Scegliere la risorsa con il tag da eliminare.
3. Scegliere Tags (Tag), quindi scegliere Add/edit tags (Aggiungi/modifica tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. Scegliere l'icona X accanto al tag che si desidera eliminare, poi scegliere Save (Salva).

## 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 VMwareESXi, scarica sources.tar](#)
- Per i gateway distribuiti su Microsoft Hyper-V, scaricare [sources\\_hyperv.tar](#)
- [Per i gateway distribuiti su una macchina virtuale basata su kernel Linux \(\), scarica sources\\_ .tar KVM KVM](#)

[Questo prodotto include software sviluppato da Open SSL Project per l'uso in Open Toolkit \(http://www.openssl.org/\). SSL](#) 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 i volumi](#)
- [Dimensioni disco locale consigliate per il gateway](#)

## Quote per i volumi

La tabella seguente elenca le quote per i volumi.

Descrizione	Volumi nella cache	Volumi archiviati
Dimensione massima di un volume	32 TiB	16 TiB
<div data-bbox="142 785 266 823">  Note         </div> <div data-bbox="185 840 628 1209"> <p>Se crei uno snapshot da un volume memorizzato nella cache di dimensioni superiori a 16 TiB, puoi ripristinarlo su un volume Storage Gateway ma non su un volume Amazon Elastic Block Store (Amazon) EBS.</p> </div>		
Numero massimo di volumi per gateway	32	32
Le dimensioni totali di tutti i volumi per un gateway	1,024 TiB	512 TiB

## 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 (massimo)	Altri dischi locali richiesti
Gateway di volumi memorizzato nella cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway di volumi archiviato	—	—	150 GiB	2 TiB	1 o più per il volume o i volumi archiviati

#### Note

È possibile configurare una o più unità locali per la cache e il buffer di caricamento, fino alla capacità massima.

Quando si aggiunge cache o buffer di caricamento a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza AmazonEC2). Non modificare la dimensione dei dischi esistenti se i dischi sono stati allocati in precedenza come cache o come buffer di caricamento.



# API Riferimento per Storage Gateway

Oltre a utilizzare la console, è possibile utilizzarla per configurare e AWS Storage Gateway API 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 [Endpoint e quote AWS Storage Gateway](#) nella Riferimenti generali di AWS.

## Note

È inoltre possibile utilizzare AWS SDKs il per sviluppare applicazioni con AWS Storage Gateway. Il AWS SDKs per Java, .NET e PHP racchiude le informazioni sottostanti AWS Storage Gateway API, semplificando le attività di programmazione. Per informazioni sul download delle SDK librerie, vedete [Sample Code Libraries](#).

## Argomenti

- [Intestazioni obbligatorie delle richieste in Storage Gateway](#)
- [Firmare le richieste](#)
- [Risposte agli errori](#)
- [Azioni](#)

## Intestazioni obbligatorie delle richieste in Storage Gateway

Questa sezione descrive le intestazioni richieste da inviare con ogni POST richiesta a Storage Gateway. Sono incluse HTTP intestazioni per identificare le informazioni chiave sulla richiesta, tra cui l'operazione che si desidera richiamare, la data della richiesta e le informazioni che indicano l'autorizzazione dell'utente 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
```

Di seguito sono riportate le intestazioni da includere nelle POST richieste 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 utilizzate nelle transazioni. HTTP

Header	Descrizione
Authorization	<p>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):</p> <pre data-bbox="472 1052 1507 1329">Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyymmdd/region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>Nella sintassi precedente, si specificano l'anno <i>YourAccessKey</i>, il mese e il giorno (<i>aaaammgg</i>), la regione e il <i>CalculatedSignature</i>. Il formato dell'intestazione di autorizzazione è dettato dai requisiti del processo di firma V4. AWS I dettagli sulla firma vengono approfonditi nell'argomento <a href="#">Firmare le richieste</a>.</p>
Content-Type	<p>Usa <code>application/x-amz-json-1.1</code> come tipo di contenuto per tutte le richieste a Storage Gateway.</p> <pre data-bbox="472 1787 1507 1866">Content-Type: application/x-amz-json-1.1</pre>

Header	Descrizione
Host	<p>Usa l'intestazione host per specificare l'endpoint Storage Gateway in cui invii la richiesta. Ad esempio, <code>storagegateway.us-east-2.amazonaws.com</code> è l'endpoint per la regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili per Storage Gateway, consulta <a href="#">Endpoint e quote AWS Storage Gateway</a> nella Riferimenti generali di AWS.</p> <div data-bbox="472 569 1507 646" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>Host: <code>storagegateway. <i>region</i>.amazonaws.com</code></p> </div>
x-amz-date	<p>È necessario fornire il timestamp nell'intestazione o nell'HTTP Date intestazione. AWS x-amz-date (Alcune librerie HTTP client non consentono di impostare l'Date intestazione.) Quando è presente un'intestazione x-amz-date, Storage Gateway ignora qualsiasi intestazione Date durante l'autenticazione della richiesta. Il x-amz-date formato deve essere ISO8601 Basic nel formato YYYYMMDD'T'HHMMSS'Z'. Se vengono utilizzati Date sia l'x-amz-date intestazione che l'intestazione Date, il formato dell'intestazione Date non deve essere ISO8601.</p> <div data-bbox="472 1178 1507 1255" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>x-amz-date: <code>YYYYMMDD'T'HHMMSS'Z'</code></p> </div>
x-amz-target	<p>Questa intestazione specifica la versione API e l'operazione richiesta. I valori di intestazione di destinazione sono formati concatenando la API versione con il API nome e sono nel seguente formato.</p> <div data-bbox="472 1493 1507 1570" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>x-amz-target: <code>StorageGateway_ <i>APIversion</i> .<i>operationName</i></code></p> </div> <p>Il operationName valore (ad esempio "ActivateGateway") può essere trovato dall'elenco API <a href="#">API Riferimento per Storage Gateway</a></p>

## 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 tua HTTP richiesta in un formato canonico. L'utilizzo di un formato canonico è necessario in quanto Storage Gateway utilizza quel formato quando ricalcola una firma da confrontare con quella che hai inviato.

- [Fase 2: creazione di una stringa di firma](#)

Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata stringa di firma, è una concatenazione del nome dell'algoritmo hash, della data della richiesta, di una stringa di ambito credenziali e della richiesta in formato canonico creata nella fase precedente. La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

- [Fase 3. Creazione di una firma](#)

Crea una firma per la tua richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input: la tua stringa di firma e una chiave derivata. La chiave derivata viene calcolata partendo dalla chiave di accesso segreta e utilizzando la stringa `Credential Scope` per creare una serie di codici di autenticazione dei messaggi basati su Hash (`()`). HMACs

## Esempio di calcolo di firma

L'esempio seguente illustra i dettagli della creazione di 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 «Lun, 10 settembre 2012 00:00:00". GMT
- L'endpoint è la regione Stati Uniti orientali (Ohio).

La sintassi generale della richiesta (incluso il corpo) è: JSON

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{ }
```

Il formato canonico della richiesta calcolata per [Fase 1. Creazione di una richiesta canonica](#) è:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

L'ultima riga della richiesta canonica è l'hash del corpo della richiesta. Nota inoltre la terza riga vuota nella richiesta canonica. Questo perché non esistono parametri di interrogazione per questo API (o per alcuni Storage Gateway APIs).

La stringa di firma per [Fase 2: creazione di una stringa di firma](#) è:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La prima riga della stringa di firma è l'algoritmo, la seconda è il timestamp, la terza è l'ambito credenziali e l'ultima è un hash del formato della richiesta canonica in Fase 1.

Per [Fase 3. Creazione di una firma](#), la chiave derivata può essere rappresentata come segue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-
east-2"), "storagegateway"), "aws4_request")
```

Se viene utilizzata la chiave di accesso segreta wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY, la firma calcolata è:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

La fase finale consiste nel creare l'intestazione Authorization. Per la chiave di accesso dimostrativa AKIAIOSFODNN7EXAMPLE, l'intestazione (con interruzioni di riga aggiunte per motivi di leggibilità) è:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

## Risposte agli errori

### Argomenti

- [Eccezioni](#)
- [Codici di errore delle operazioni](#)
- [Risposte agli errori](#)

Questa sezione fornisce informazioni di riferimento sugli errori. AWS Storage Gateway Questi errori sono rappresentati da un'eccezione di errore e da un codice di errore dell'operazione. Ad

esempio, l'eccezione di errore `InvalidSignatureException` viene restituita da qualsiasi API risposta in caso di problemi con la firma della richiesta. Tuttavia, il codice di errore dell'operazione `ActivationKeyInvalid` viene restituito solo per [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

Nella tabella seguente sono elencate le AWS Storage Gateway API eccezioni. 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	HTTPCodice di stato
<code>IncompleteSignatureException</code>	La firma specificata non è completa.	400 Richiesta non valida
<code>InternalFailure</code>	L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto sconosciuto.	500 - Errore interno del server
<code>InternalServerError</code>	Uno dei messaggi dei codici di errore delle operazioni in <a href="#">Codici di errore delle operazioni</a> .	500 - Errore interno del server
<code>InvalidAction</code>	L'azione o l'operazione richiesta non è valida.	400 Richiesta non valida
<code>InvalidClientTokenId</code>	Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.	403 Non consentito

Eccezione	Messaggio	HTTPCodice di stato
InvalidGatewayRequestException	Uno dei messaggi dei codici di errore delle operazioni in <a href="#">Codici di errore delle operazioni</a> .	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. Verifica che il tuo JSON payload sia ben formato.	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
ThrottlingException	Velocità superata.	400 Richiesta non valida



Eccezione	Messaggio	HTTPCodice di stato
TooManyRequests	Troppe richieste.	429 Troppe richieste
UnknownOperationException	È stata specificata un'operazione sconosciuta. Le operazioni valide sono elencate in <a href="#">Operazioni in Storage Gateway</a> .	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 APIs che può restituire i codici. Tutti i codici di errore delle operazioni vengono restituiti con una delle due eccezioni generali `InternalServerError` e `InvalidGatewayRequestException` descritte in [Eccezioni](#).

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
ActivationKeyExpired	La chiave di attivazione specificata è scaduta.	<a href="#">ActivateGateway</a>
ActivationKeyInvalid	La chiave di attivazione specificata non è valida.	<a href="#">ActivateGateway</a>
ActivationKeyNotFound	La chiave di attivazione specificata non è stata trovata.	<a href="#">ActivateGateway</a>

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.	<a href="#">DeleteBandwidthRateLimit</a>
CannotExportSnapshot	Lo snapshot specificato non può essere esportato.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
InitiatorNotFound	L'iniziatore specificato non è stato trovato.	<a href="#">DeleteChapCredentials</a>
DiskAlreadyAllocated	Il disco specificato è già allocato.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskDoesNotExist	Il disco specificato non esiste.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskSizeNotGigAligned	Il disco specificato non è allineato ai gigabyte.	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeGreaterThanVolumeMaxSize	La dimensione del disco specificata è superiore alla dimensione massima del volume.	<a href="#">CreateStorediSCSIVolume</a>

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.	<a href="#">CreateStorediSCSIVolume</a>
DuplicateCertificateInfo	Le informazioni sul certificato specificate sono duplicate.	<a href="#">ActivateGateway</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
GatewayInternalError	Si è verificato un errore interno del gateway.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
GatewayNotConnected	Il gateway specificato non è connesso.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
GatewayNotFound	Il gateway specificato non è stato trovato.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a>



Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">ListLocalDisks</a>
		<a href="#">ListVolumes</a>
		<a href="#">ListVolumeRecoveryPoints</a>
		<a href="#">ShutdownGateway</a>
		<a href="#">StartGateway</a>
		<a href="#">UpdateBandwidthRateLimit</a>
		<a href="#">UpdateChapCredentials</a>
		<a href="#">UpdateMaintenanceStartTime</a>
		<a href="#">UpdateGatewaySoftwareNow</a>
		<a href="#">UpdateSnapshotSchedule</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
GatewayProxyNetworkConnectionBusy	La connessione di rete proxy gateway specificata è occupata.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
InternalError	Si è verificato un errore interno.	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
<b>InvalidParameters</b>	La richiesta specificata contiene parametri non corretti.	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
LocalStorageLimitExceeded	Il limite di storage locale è stato superato.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a>
LunInvalid	Il valore specificato non LUN è corretto.	<a href="#">CreateStorediSCSIVolume</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
MaximumVolumeCount Exceeded	Il numero massimo di volumi è stato superato.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a>
NetworkConfigurationChanged	La configurazione di rete del gateway è stata modificata.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>



Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
NotSupported	L'operazione specifica non è supportata.	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
OutdatedGateway	Il gateway specificato non è aggiornato.	<a href="#">ActivateGateway</a>
SnapshotInProgressException	Lo snapshot specificato è in corso.	<a href="#">DeleteVolume</a>
SnapshotIdInvalid	Lo snapshot specificato non è valido.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
StagingAreaFull	L'area di gestione temporanea è piena.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
TargetAlreadyExists	La destinazione specificata esiste già.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetInvalid	La destinazione specificata non è valida.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">UpdateChapCredentials</a>
TargetNotFound	La destinazione specificata non è stata trovata.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">UpdateChapCredentials</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
<code>UnsupportedOperationForGatewayType</code>	L'operazione specifica non è valida per il tipo di gateway.	<a href="#">AddCache</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteSnapshotSchedule</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeUploadBuffer</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListVolumeRecoveryPoints</a>
<code>VolumeAlreadyExists</code>	Il volume specificato esiste già.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
<code>VolumeIdInvalid</code>	Il volume specificato non è valido.	<a href="#">DeleteVolume</a>
<code>VolumeInUse</code>	Il volume specificato è già in uso.	<a href="#">DeleteVolume</a>

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
VolumeNotFound	Il volume specificato non è stato trovato.	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">UpdateSnapshotSchedule</a>
VolumeNotReady	Il volume specificato non è pronto.	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a>

## 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 appropriato o di stato 4xx 5xx HTTP

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 JSON di risposta agli errori mostrati nella sintassi precedente.

#### \_\_type

Una delle eccezioni elencate in [Eccezioni](#).

Tipo: Stringa

#### error

Contiene dettagli API sull'errore specifici. In caso di errori generali (ossia non specifici API), queste informazioni sull'errore non vengono visualizzate.

Tipo: raccolta

#### errorCode

Uno dei codici di errore delle operazioni .

Tipo: Stringa

#### errorDetails

Questo campo non è utilizzato nella versione corrente di API.

Tipo: Stringa

#### message

Uno dei messaggi dei codici di errore delle operazioni.

Tipo: Stringa

## Esempi di risposta di errore

Il seguente JSON corpo viene restituito se si utilizza DescribeStoredi SCSIVolumes API e si specifica un input di ARN richiesta gateway che non esiste.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
"message": "The specified volume was not found.",
"error": {
  "errorCode": "VolumeNotFound"
}
}
```

Il seguente JSON corpo 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 dello Storage Gateway, vedere [Azioni](#) nel AWS Storage Gateway API riferimento.

# Cronologia dei documenti della Guida per l'utente per Gateway di volumi

- API versione: 2013-06-30
- 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 iscriverti a un feed. RSS

Modifica	Descrizione	Data
<a href="#">È stata aggiunta l'opzione per attivare o disattivare gli aggiornamenti di manutenzione</a>	Storage Gateway riceve aggiornamenti di manutenzione regolari che possono includere aggiornamenti del sistema operativo e del software, correzioni per la stabilità, le prestazioni e la sicurezza e l'accesso a nuove funzionalità. È ora possibile configurare un'impostazione per attivare o disattivare questi aggiornamenti per ogni singolo gateway della distribuzione. Per ulteriori informazioni, vedere <a href="#">Gestione degli aggiornamenti del gateway tramite la AWS Storage Gateway console</a> .	6 giugno 2024
<a href="#">Supporto obsoleto per Tape Gateway su Snowball Edge</a>	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 .

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 aggiornate e anche per HealthNotifications e AvailabilityNotifications . Per ulteriori informazioni, vedere [gli CloudWatch allarmi](#).

2 ottobre 2023

[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, consulta la Guida per [l'utente del gateway di nastri virtuali](#) e la Guida per [l'utente del 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 dei nastri](#)

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 i gateway di nastri virtuali e 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 rispettivi tipi di gateway, sono stati rimossi alcuni argomenti non necessari.

21 luglio 2021

---

<a href="#">Supporto per IBM Spectrum Protect 8.1.10 su Windows e Linux per Tape Gateway</a>	I Tape Gateway ora supportano la versione 8.1.10 di IBM Spectrum Protect in esecuzione su Microsoft Windows Server e Linux. Per ulteriori informazioni, consulta <a href="#">Testare la configurazione utilizzando IBM Spectrum Protect</a> .	24 novembre 2020
<a href="#">RAMPConformità Fed</a>	Storage Gateway è ora RAMP conforme alla Fed. Per ulteriori informazioni, consulta <a href="#">Convalida della conformità per Storage Gateway</a> .	24 novembre 2020
<a href="#">Limitazione della larghezza di banda basata sulla pianificazione</a>	Storage Gateway ora supporta la limitazione della larghezza di banda basata sulla pianificazione per i gateway di nastri virtuali e di volumi. Per ulteriori informazioni, vedere <a href="#">Pianificazione della limitazione della larghezza di banda utilizzando la console Storage Gateway</a> .	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 informazioni, 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 ritenzione del nastro e write-once-read-many \(WORM\) la protezione del nastro](#)

Storage Gateway supporta il blocco della conservazione dei nastri su nastri virtuali e la funzionalità Write Once Read Many (WORM). Il blocco di conservazione dei nastri 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 [Utilizzo del blocco di conservazione dei nastri](#). WORM-i nastri virtuali attivati 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 \(\) Tape Protection](#). WORM

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

---

<a href="#">Support per gli endpoint Federal Information Processing Standard (FIPS) in nuove regioni AWS</a>	Ora puoi attivare un gateway con FIPS endpoint nelle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon) e Canada (centrali). Per ulteriori informazioni, consulta <a href="#">Endpoint e quote AWS Storage Gateway</a> nella Riferimenti generali di AWS.	31 luglio 2020
<a href="#">Migrazione del gateway</a>	Storage Gateway ora supporta la migrazione dei gateway di nastri virtuali e di volumi archiviati verso nuove macchine virtuali. Per ulteriori informazioni, consulta <a href="#">Spostamento dei dati su un nuovo gateway</a> .	31 luglio 2020
<a href="#">Visualizza gli CloudWatch allarmi Amazon nella console Storage Gateway</a>	È ora possibile visualizzare gli CloudWatch allarmi nella console Storage Gateway. <a href="#">Per ulteriori informazioni, vedere . CloudWatch</a>	29 maggio 2020

[Supporto per gli endpoint  
Federal Information Processin  
g Standard \(FIPS\)](#)

Ora puoi attivare un gateway con FIPS endpoint nelle Regioni. AWS GovCloud (US) Per scegliere un FIPS endpoint per un Volume Gateway, vedi [Scelta di un endpoint di servizio](#). Per scegliere un FIPS endpoint per un Tape Gateway, vedi [Connect your Tape Gateway 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 l'hypervisor Virtual Machine \(\) KVM basato su kernel Linux](#)

Storage Gateway ora offre la possibilità di implementare un gateway locale sulla piattaforma di KVM virtualizzazione. I gateway distribuiti su KVM hanno tutte le stesse funzionalità e caratteristiche dei gateway locali esistenti. Per ulteriori informazioni, consulta l'argomento relativo agli [Hypervisor supportati e requisiti host](#) nella Guida per l'utente di Storage Gateway.

4 febbraio 2020

[Support per l'VMware vSphere alta disponibilità](#)

Storage Gateway ora fornisce supporto per l'alta disponibilità per aiutare VMware a proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, vedere [Using VMware vSphere High Availability with Storage Gateway](#) nella Storage Gateway User Guide. Questa versione include inoltre i miglioramenti delle prestazioni. Per ulteriori informazioni, consulta [Prestazioni](#) nella Guida per l'utente di Storage Gateway.

20 novembre 2019

### [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

### [Support per IBM Spectrum Protect versione 7.1.9 su Linux e per Tape Gateway una dimensione massima del nastro aumentata a 5 TiB](#)

I Tape Gateway ora supportano IBM Spectrum Protect (Tivoli Storage Manager) versione 7.1.9 in esecuzione su Linux, oltre a funzionare su Microsoft Windows. Per ulteriori informazioni, vedere [Testing Your Setup by Using IBM Spectrum Protect](#) nella Storage Gateway User Guide. 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 [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

[Support per l'attivazione di un gateway in un cloud privato virtuale \(\) VPC](#)

Ora puoi attivare un gateway in unVPC. 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

[SMBsupporto per la condivisione di file per Microsoft Windows ACLs](#)

Per i File Gateway, ora puoi utilizzare le liste di controllo degli accessi di Microsoft Windows (ACLs) per controllare l'accesso alle condivisioni di file Server Message Block (SMB). Per ulteriori informazioni, vedere [Utilizzo di Microsoft Windows ACLs per controllare l'accesso a una condivisione di SMB file](#).

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 spazio di archiviazione utilizzabile sull'appliance hardware 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

### [Support per Bacula Enterprise e IBM Spectrum Protect](#)

I Tape Gateway 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 Tape Gateway sono ora compatibili con Microsoft System Center 2016 Data Protection Manager (DPM). Ora puoi usare Microsoft DPM per eseguire il backup dei dati su Amazon S3 e archivarli direttamente nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta [Test della configurazione utilizzando Microsoft System Center Data Protection Manager](#).

18 luglio 2018

[Support per il protocollo Server Message Block \(SMB\)](#)

File Gateways ha aggiunto il supporto per il protocollo Server Message Block (SMB) alle condivisioni di 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. Attualmente, è possibile eseguire questa operazione utilizzando il AWS Storage Gateway API. 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 e NovaStor DataCenter / Network versione 6.4 o 7.1 per eseguire il backup dei dati su Amazon S3 e archivarli 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 <a href="#">Creazione di una condivisione file</a> .	4 aprile 2018
Nuova regione	Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Singapore). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	3 Aprile 2018
Supporta le notifiche di aggiornamento della cache, i pagamenti dei richiedenti e i bucket predefiniti per Amazon ACLs S3.	<p>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 <a href="#">RefreshCache.html</a> nello Storage Gateway API Reference.</p> <p>I gateway di file permettono ora al richiedente o al lettore di pagare le tariffe di accesso al posto del proprietario del bucket.</p> <p>I File Gateway ora consentono di dare il pieno controllo al proprietario del bucket S3 associato alla condivisione di file. NFS</p> <p>Per ulteriori informazioni, consulta <a href="#">Creazione di una condivisione file</a>.</p>	1 marzo 2018
Support per Dell EMC NetWorker V9.x	I Tape Gateway ora supportano Dell V9.x. EMC NetWorker Ora puoi utilizzare Dell EMC NetWorker V9.x per eseguire il backup dei dati su Amazon S3 e archivarli direttamente su storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). <a href="#">Per</a>	27 febbraio 2018

Modifica	Descrizione	Data della modifica
	<a href="#">ulteriori informazioni, consulta Testare la configurazione utilizzando Dell. EMC NetWorker</a>	
Nuova regione	Storage Gateway è ora disponibile nella regione Europa (Parigi). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	18 dicembre 2017
Support per la notifica di caricamento dei file e l'individuazione del tipo MIME	<p>I File Gateway ora possono avvisarti quando tutti i file scritti nella tua condivisione di NFS file sono stati caricati su Amazon S3. Per ulteriori informazioni, vedere <a href="#">NotifyWhenUploaded</a> Storage Gateway API Reference.</p> <p>I File Gateway ora consentono di indovinare il MIME tipo di oggetti caricati in base alle estensioni dei file. Per ulteriori informazioni, consulta <a href="#">Creazione di una condivisione file</a>.</p>	21 Novembre 2017
Support per la versione VMware ESXi 6.5 di Hypervisor	AWS Storage Gateway ora supporta la versione 6.5 di VMware ESXi Hypervisor. Questa si aggiunge alle versioni 4.1, 5.0, 5.1, 5.5 e 6.0. Per ulteriori informazioni, consulta <a href="#">Hypervisor supportati e requisiti di hosting</a> .	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 <a href="#">Testare la configurazione utilizzando Commvault</a> .	12 settembre 2017

Modifica	Descrizione	Data della modifica
Supporto del gateway di file per l'hypervisor Microsoft Hyper-V	Puoi ora distribuire un gateway di file in un hypervisor Microsoft Hyper-V. Per informazioni, consultare <a href="#">Hypervisor supportati e requisiti di hosting</a> .	22 giugno 2017
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. È inoltre possibile determinare la quantità di dati scritti sul nastro dall'applicazione di backup o dalla libreria a nastro virtuale (VTL). Per ulteriori informazioni, consulta <a href="#">Visualizzazione dell'utilizzo dei nastri</a> .	23 maggio 2017
Nuova regione	Storage Gateway è ora disponibile nella regione Asia Pacifico (Mumbai). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	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 <a href="#">Creazione di una condivisione file</a> .  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, vedere <a href="#">RefreshCache</a> nella Guida di API riferimento.	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 <a href="#">Clonazione di un volume</a> .	16 marzo 2017

Modifica	Descrizione	Data della modifica
Support per File Gateway su Amazon EC2	AWS Storage Gateway ora offre la possibilità di implementare un File Gateway in AmazonEC2. Puoi avviare un File Gateway in Amazon EC2 utilizzando lo Storage Gateway Amazon Machine Image (AMI) ora disponibile come communityAMI. Per informazioni su come creare un File Gateway e distribuirlo su un'EC2istanza, consulta <a href="#">Creare e attivare un Amazon S3 File Gateway o Creare e attivare un FSx Amazon File Gateway</a> . Per informazioni su come avviare un File GatewayAMI, consulta <a href="#">Implementazione di un S3 File Gateway su un EC2 host Amazon</a> o <a href="#">Distribuzione di FSx File Gateway su un host Amazon</a> . 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 archivarli direttamente in S3 Glacier Flexible Retrieval. Per ulteriori informazioni, vedere <a href="#">Test della configurazione utilizzando Arcserve Backup r17.0</a> .	17 gennaio 2017
Nuova regione	Storage Gateway è ora disponibile nella regione Europa (Londra). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	13 dicembre 2016
Nuova regione	Storage Gateway è ora disponibile nella regione Canada (Centrale). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	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. File Gateway combina un servizio e un'appliance software virtuale, che consente di archiviare e recuperare oggetti in Amazon S3 utilizzando protocolli di file standard del settore come Network File System (NFS). Il gateway fornisce l'accesso agli oggetti in Amazon S3 come file su un punto di NFS montaggio.	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 <a href="#">Testare la configurazione utilizzando Veritas Backup Exec</a> .	7 Novembre 2016
Compatibilità con Micro Focus (HPE) Data Protector 9.x	Tape Gateway è ora compatibile con Micro Focus (HPE) Data Protector 9.x. Ora puoi utilizzare HPE Data Protector per eseguire il backup dei dati su Amazon S3 e archivarli direttamente su S3 Glacier Flexible Retrieval. Per ulteriori informazioni, consulta <a href="#">Testare la configurazione utilizzando Micro Focus (HPE) Data Protector</a> .	2 Novembre 2016
Nuova regione	Storage Gateway ora è disponibile nella regione Stati Uniti orientali (Ohio). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	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 collegamenti diretti a AWS servizi integrati come CloudWatch AmazonEBS. Per ulteriori informazioni, consulta <a href="#">Registrati per AWS Storage Gateway</a> .	30 agosto 2016
Compatibilità con Veeam Backup & Replication V9 Update 2 o versioni successive	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 successive. È ora possibile utilizzare Veeam Backup Replication V9 Update 2 o versione successiva 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 <a href="#">Test della configurazione utilizzando Veeam Backup &amp; Replication</a> .	15 agosto 2016
Volume e istantanee più lunghi IDs	Storage Gateway sta introducendo una IDs versione più lunga per volumi e istantanee. È possibile attivare il formato ID più lungo per i volumi, le istantanee e altre risorse supportate AWS . Per ulteriori informazioni, consulta <a href="#">Informazioni sulle risorse e sulle risorse dello Storage Gateway IDs</a> .	25 Aprile 2016



Modifica	Descrizione	Data della modifica
<p>Nuova regione</p> <p>Supporto per storage di dimensioni fino a 512 TiB per i volumi archiviati</p> <p>Altri aggiornamenti e miglioramenti del gateway per la console locale Storage Gateway</p>	<p>Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Seoul). Per ulteriori informazioni, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a>.</p> <p>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 <a href="#">Architettura dei volumi archiviati</a> e <a href="#">AWS Storage Gateway quote</a>.</p> <p>Le dimensioni totali di tutti i nastri in una libreria di nastri virtuali (VTL) sono state aumentate a 1 PiB. Per ulteriori informazioni, consulta <a href="#">AWS Storage Gateway quote</a>.</p> <p>Puoi ora impostare la password per la console locale della macchina virtuale nella console Storage Gateway. Per informazioni, consultare <a href="#">Impostazione della password della console locale dalla console Storage Gateway</a>.</p>	<p>21 marzo 2016</p>
<p>Compatibilità con Dell 8.x EMC NetWorker</p>	<p>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 archivarli direttamente sullo storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). <a href="#">Per ulteriori informazioni, consulta Testare la configurazione utilizzando Dell. EMC NetWorker</a></p>	<p>29 febbraio 2016</p>

Modifica	Descrizione	Data della modifica
<p>Support per VMware ESXi Hypervisor versione 6.0 e iniziatore Red Hat Enterprise Linux 7 i SCSI</p> <p>Nuova struttura dei contenuti</p>	<p>AWS Storage Gateway ora supporta la versione VMware ESXi Hypervisor 6.0 e l'iniziatore Red Hat Enterprise Linux 7 i. SCSI Per ulteriori informazioni, consulta <a href="#">Hypervisor supportati e requisiti di hosting</a> e <a href="#">SCSISupportato negli iniziatori</a>.</p> <p>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 <a href="#">Gestione del gateway</a>.</p>	<p>20 Ottobre 2015</p>

Modifica	Descrizione	Data della modifica
<p>Supporto per storage di dimensioni fino a 1.024 TiB per i volumi nella cache</p> <p>Supporto per il tipo di adattatore di rete VMXNET3 (10 GbE) nell'hypervisor VMware ESXi</p> <p>Miglioramenti per le prestazioni</p> <p>Miglioramenti e aggiornamenti vari per la console locale Storage Gateway</p>	<p>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 <a href="#">Architettura dei volumi memorizzati nella cache</a> e <a href="#">AWS Storage Gateway quote</a>.</p> <p>Se il gateway è ospitato su un VMware ESXi hypervisor, è possibile riconfigurare il gateway per utilizzare il tipo di adattatore. VMXNET3 Per ulteriori informazioni, consulta <a href="#">Configurazione delle schede di rete per il gateway</a>.</p> <p>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.</p> <p>La console locale Storage Gateway è stata aggiornata e migliorata con caratteristiche aggiuntive per semplificare le attività di manutenzione. Per ulteriori informazioni, consulta <a href="#">Configurazione di rete del gateway</a>.</p>	<p>16 settembre 2015</p>
<p>Supporto per il tagging</p>	<p>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 <a href="#">Tagging per risorse Storage Gateway</a>.</p>	<p>2 settembre 2015</p>

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 archivarli direttamente nello storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta <a href="#">Test della configurazione utilizzando Quest NetVault Backup</a> .	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 <a href="#">Architettura dei volumi archiviati</a> .	3 giugno 2015
Supporto per controlli delle risorse di sistema nella console locale Storage Gateway	È ora possibile determinare se le risorse di sistema (CPUcore virtuali, dimensione del volume root eRAM) sono sufficienti per il corretto funzionamento del gateway. Per ulteriori informazioni, consulta <a href="#">Visualizzazione dello stato relativo alle risorse di sistema del gateway</a> o <a href="#">Visualizzazione dello stato relativo alle risorse di sistema del gateway</a> .	
Supporto per l'SCSIinziatore Red Hat Enterprise Linux 6 i	Storage Gateway ora supporta l'SCSIinziatore Red Hat Enterprise Linux 6 i. Per ulteriori informazioni, consulta <a href="#">Requisiti per la configurazione di Volume Gateway</a> .	
	<p>Questa versione include i miglioramenti e gli aggiornamenti per Storage Gateway seguenti:</p> <ul style="list-style-type: none"><li>• Dalla console Storage Gateway puoi ora visualizzare la data e l'ora dell'applicazione dell'ultimo aggiornamento software al gateway. Per ulteriori informazioni, consulta <a href="#">Gestione degli aggiornamenti del gateway</a>.</li><li>• Storage Gateway ora fornisce uno strumento API che consente di elencare SCSI gli iniziatori collegati</li></ul>	

Modifica	Descrizione	Data della modifica
	ai volumi di storage. Per ulteriori informazioni, vedere <a href="#">ListVolumeInitiators</a> nel API riferimento.	
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 <a href="#">Hypervisor supportati e requisiti di hosting</a> .	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 e 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 <a href="#">Testare la configurazione utilizzando Veritas Backup Exec</a> .	6 Aprile 2015
CHAP supporto all'autenticazione per volumi di archiviazione	Storage Gateway ora supporta la configurazione CHAP dell'autenticazione per i volumi di storage. Per ulteriori informazioni, vedere <a href="#">Configurare CHAP l'autenticazione per i volumi</a> .	2 Aprile 2015
Support per VMware ESXi Hypervisor versione 5.1 e 5.5	Storage Gateway ora supporta le versioni 5.1 e 5.5 di VMware ESXi Hypervisor. Ciò si aggiunge al supporto per le versioni 4.1 e 5.0 di VMware ESXi Hypervisor. Per ulteriori informazioni, consulta <a href="#">Hypervisor supportati e requisiti di hosting</a> .	30 marzo 2015

Modifica	Descrizione	Data della modifica
Supporto per l'CHKDSKutilità Windows	Storage Gateway ora supporta l'CHKDSKutilità Windows. Puoi usare questa utilità per verificare l'integrità dei volumi e correggere gli errori nei volumi. Per ulteriori informazioni, consulta <a href="#">Risoluzione dei problemi dei volumi</a> .	04 marzo 2015
Integrazione con AWS CloudTrail per acquisire API chiamate	<p>Storage Gateway è ora integrato con AWS CloudTrail. AWS CloudTrail acquisisce le API chiamate effettuate da o per conto di Storage Gateway nel tuo account Amazon Web Services e invia i file di registro a un bucket Amazon S3 da te specificato. Per ulteriori informazioni, consulta <a href="#">Registrazione e monitoraggio AWS Storage Gateway</a>.</p> <p>Questa versione include i miglioramenti e gli aggiornamenti per Storage Gateway seguenti:</p> <ul style="list-style-type: none"><li>• 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 <a href="#">Recupero di un nastro virtuale da un gateway compromesso</a>.</li></ul>	16 dicembre 2014

Modifica	Descrizione	Data della modifica
Compatibilità con unità di sostituzione dei supporti e software di backup aggiuntivi	<p>Il gateway di nastri virtuali è ora compatibile con i software di backup seguenti:</p> <ul style="list-style-type: none"><li>• Symantec Backup Exec 2014</li><li>• Microsoft System Center 2012 R2 Data Protection Manager</li><li>• Veeam Backup &amp; Replication V7</li><li>• Veeam Backup &amp; Replication V8</li></ul> <p>Ora puoi utilizzare questi quattro prodotti software di backup con la libreria a nastro virtuale Storage Gateway (VTL) per eseguire il backup su Amazon S3 e archiviare direttamente sullo storage offline (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive). Per ulteriori informazioni, consulta <a href="#">Utilizzo del software di backup per testare la configurazione del gateway</a>.</p> <p>Storage Gateway fornisce ora un'unità di sostituzione dei supporti aggiuntiva compatibile con il nuovo software di backup.</p> <p>AWS Storage Gateway Questa versione include vari miglioramenti e aggiornamenti.</p>	3 Novembre 2014
Regione Europa (Francoforte)	Storage Gateway è ora disponibile nella regione Europa (Francoforte). Per informazioni dettagliate, consulta <a href="#">Regioni AWS che supportano Storage Gateway</a> .	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 <a href="#">Creazione di un gateway di nastri virtuali</a> .	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 <a href="#">Testare la configurazione utilizzando Veritas Backup Exec</a> .	28 aprile 2014

Modifica	Descrizione	Data della modifica
<p>Supporto per Windows Server Failover Clustering</p> <p>Support per l'VMwareESXiniziatore</p> <p>Supporto per l'esecuzione di attività di configurazione nella console locale Storage Gateway</p>	<ul style="list-style-type: none"> <li>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 è possibile connettere più host allo stesso volume senza utilizzare WSFC.</li> <li>Storage Gateway ora consente di gestire la connettività di storage direttamente tramite l'ESXhost. Ciò fornisce un'alternativa all'utilizzo di iniziatori residenti nel sistema operativo guest del tuo VMs.</li> <li>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 <a href="#">Esecuzione delle operazioni sulla console locale della VM di</a> o <a href="#">Esecuzione delle operazioni sulla console locale della VM di</a>. Per informazioni sull'esecuzione delle attività di configurazione sui gateway distribuiti su un'istanza EC2, consulta o <a href="#">Esecuzione di attività sulla console EC2 locale di Amazon</a> <a href="#">Esecuzione di attività sulla console EC2 locale di Amazon</a>.</li> </ul>	<p>31 gennaio 2014</p>

Modifica	Descrizione	Data della modifica
Support per Virtual Tape Library (VTL) e introduzione della API versione 2013-06-30	<p>Storage Gateway collega un'appliance software locale con lo storage basato sul cloud per integrare l'ambiente IT locale con l'infrastruttura di storage. AWS Oltre ai Volume Gateway (volumi memorizzati nella cache e volumi archiviati), Storage Gateway ora supporta gateway—virtual tape library (). VTL 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 SCSI comandi, quindi le applicazioni di backup locali esistenti funzioneranno senza modifiche. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS Storage Gateway .</p> <ul style="list-style-type: none"><li>• Per una panoramica dell'architettura, vedi <a href="#">Come funziona un gateway di nastri virtuali (architettura)</a>.</li><li>• Per iniziare a usare il gateway di nastri virtuali, consulta <a href="#">Creazione di un gateway di nastri virtuali</a>.</li></ul>	5 Novembre 2013
Supporto per Microsoft Hyper-V	<p>Storage Gateway offre ora la possibilità di distribuire un gateway on-premise nella piattaforma di virtualizzazione Microsoft Hyper-V. I gateway distribuiti in Microsoft Hyper-V hanno tutti le stesse funzionalità e caratteristiche di Storage Gateway on-premise esistente. Per informazioni su come iniziare a distribuire un gateway con Microsoft Hyper-V, consulta <a href="#">Hypervisor supportati e requisiti di hosting</a>.</p>	10 Aprile 2013

Modifica	Descrizione	Data della modifica
Support per l'implementazione di un gateway su Amazon EC2	Storage Gateway ora offre la possibilità di implementare un gateway in Amazon Elastic Compute Cloud (AmazonEC2). Puoi avviare un'istanza gateway in Amazon EC2 utilizzando lo Storage Gateway AMI disponibile in <a href="#">Marketplace AWS</a> . Per iniziare a implementare un gateway utilizzando Storage GatewayAMI, vedere <a href="#">Implementazione di un'EC2istanza Amazon per ospitare Volume Gateway</a> .	15 gennaio 2013

Modifica	Descrizione	Data della modifica
Support per i volumi memorizzati nella cache e introduzione della API versione 2012-06-30	<p>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. È possibile creare volumi di storage di dimensioni fino a 32 TiB e montarli come SCSI dispositivi i dai server delle 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.</p> <p>In questa versione, Storage Gateway introduce anche una nuova API versione che, oltre a supportare le operazioni correnti, fornisce nuove operazioni per supportare i volumi memorizzati nella cache.</p> <p>Per ulteriori informazioni sulle due soluzioni Storage Gateway, consulta <a href="#">Come funziona il gateway di volumi (architettura)</a>.</p> <p>Puoi anche provare una configurazione di test. Per istruzioni, consulta <a href="#">Creazione di un gateway di nastri virtuali</a>.</p>	29 Ottobre 2012

Modifica	Descrizione	Data della modifica
APIe supporto IAM	<p>In questa versione, Storage Gateway introduce API il supporto e il supporto per AWS Identity and Access Management(IAM).</p> <ul style="list-style-type: none"> <li>• API supporto: ora è possibile configurare e gestire in modo programmatico le risorse dello Storage Gateway. Per ulteriori informazioni suAPI, vedere <a href="#">API Riferimento per Storage Gateway</a> la Guida per l'AWS Storage Gateway utente.</li> <li>• IAM support — AWS Identity and Access Management (IAM) consente di creare utenti e gestire l'accesso degli utenti alle risorse dello Storage Gateway tramite IAM policy. Per esempi di policy IAM, consulta <a href="#">Identity and Access Management per AWS Storage Gateway</a>. Per ulteriori informazioni su ( )IAM, vedere la pagina di dettaglio <a href="#">AWS Identity and Access Management (IAM)</a>.</li> </ul>	9 maggio 2012
Supporto per indirizzi IP statici	Puoi ora specificare un indirizzo IP statico per il gateway locale. Per ulteriori informazioni, consulta <a href="#">Configurazione di rete del gateway</a> .	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 dell'appliance Volume Gateway

Queste note di rilascio descrivono le funzionalità, i miglioramenti e le correzioni nuovi e aggiornati inclusi in ogni versione dell'appliance . 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'[DescribeGatewayInformation](#) APIazione 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 API risposta.

## 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 Volume Gateway, incluso come modificare la pianificazione automatica predefinita di manutenzione e aggiornamento per un gateway, vedere [Managing Gateway Using the AWS Storage Gateway Console](#).

Data di rilascio	Versione del software	Note di rilascio
2024-07-29	2.10.0	<ul style="list-style-type: none"><li>• Aggiornamenti del sistema operativo per gateway nuovi ed esistenti</li></ul>

Data di rilascio	Versione del software	Note di rilascio
		<ul style="list-style-type: none"><li>• Correzioni di bug e miglioramenti vari</li></ul>
2024-06-17	2,9,2	<ul style="list-style-type: none"><li>• Aggiornamenti del sistema operativo per gateway nuovi ed esistenti</li></ul>
2024-05-28	2.9.0	<ul style="list-style-type: none"><li>• Tempo di riavvio del gateway ridotto durante gli aggiornamenti del software</li><li>• Riduzione della quantità di dati trasferiti per la stima della larghezza di banda della rete</li></ul>
2024-05-08	2,83	<ul style="list-style-type: none"><li>• Risolto il problema di connettività cloud durante l'utilizzo del proxy SOCKS5</li></ul>
2024-04-10	28,1	<ul style="list-style-type: none"><li>• Risolto un problema di utilizzo della memoria introdotto nella versione 2.8.0</li><li>• Aggiornamenti delle patch di sicurezza</li><li>• Processo di aggiornamento del software migliorato</li><li>• Risolto il problema del componente Network Time Protocol (NTP) mancante per i nuovi gateway</li></ul>



Data di rilascio	Versione del software	Note di rilascio
2024-03-06	2.8.0	<ul style="list-style-type: none"><li>• Aggiornamenti del sistema operativo per nuovi gateway</li><li>• Aggiornamenti delle patch di sicurezza</li></ul>
2019-12-19	2.7.0	<ul style="list-style-type: none"><li>• Aggiornamenti del sistema operativo per nuovi gateway</li></ul>
2023-12-14	2,6,6	<ul style="list-style-type: none"><li>• Versione di manutenzione</li></ul>