

---

# AWS Storage Gateway

## User Guide

**API Version 2013-06-30**



## AWS Storage Gateway: User Guide

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

## Table of Contents

What is AWS Storage Gateway?	1
Amazon S3 File Gateway	1
Amazon FSx File Gateway	1
Tape Gateway	1
Volume Gateway	2
Are you a first-time Storage Gateway user?	2
How Storage Gateway works	3
File gateways	3
Volume gateways	4
Tape gateways	7
Pricing	9
Plan your gateway deployment	9
Getting Started	11
Sign Up for AWS Storage Gateway	11
AWS Regions	11
Requirements	11
Hardware and storage requirements	12
Network and firewall requirements	13
Supported hypervisors and host requirements	22
Supported NFS clients for a file gateway	22
Supported SMB clients for a file gateway	23
Supported file system operations	23
Supported iSCSI initiators	23
Supported third-party backup applications	24
Accessing AWS Storage Gateway	25
Using the hardware appliance	26
Supported AWS regions	27
Setting up your hardware appliance	27
Rack-mounting and connecting the hardware appliance to power	28
Hardware appliance dimensions	28
Configuring network parameters	31
Activating your hardware appliance	33
Launching a gateway	36
Configuring an IP address for the gateway	37
Configuring your gateway	38
Removing a gateway	38
Deleting your hardware appliance	38
Creating Your Gateway	40
Creating a file gateway	40
Creating a gateway	40
Creating a file share	46
Using your file share	61
Creating a Volume Gateway	67
Creating a Gateway	67
Creating a volume	72
Using Your Volume	74
Backing Up Your Volumes	81
Creating a Tape Gateway	84
Creating a Gateway	85
Creating Custom Tape Pools	91
Creating Tapes	93
Using Your Tape Gateway	96
Using a Tape Gateway on an AWS Snowball Edge device	149

Creating a Tape Gateway on your Snowball Edge device .....	150
Creating tapes for a Tape Gateway on a Snowball Edge device .....	151
Troubleshooting and best practices for a Tape Gateway on a Snowball Edge device .....	151
Using the Storage Gateway API with Tape Gateway on Snowball Edge .....	152
Activating a gateway in a virtual private cloud .....	153
Creating a gateway using a VPC endpoint .....	153
Managing Your Gateway .....	162
Managing your file gateway .....	162
Adding a file share .....	162
Deleting a file share .....	165
Editing settings for your NFS file share .....	166
Editing metadata defaults for your NFS file share .....	167
Editing access settings for your NFS file share .....	168
Editing gateway level access settings for your SMB file share .....	169
Editing settings for your SMB file share .....	171
Refreshing objects in your Amazon S3 bucket .....	173
Using S3 object lock with a file gateway .....	175
Understanding file share status .....	176
File share best practices .....	176
Managing Your Volume Gateway .....	177
Adding a Volume .....	178
Expanding the Size of a Volume .....	178
Cloning a Volume .....	179
Viewing Volume Usage .....	181
Deleting a Volume .....	181
Moving Your Volumes to a Different Gateway .....	182
Reducing the Amount of Billed Storage on a Volume .....	184
Creating a One-Time Snapshot .....	184
Editing a Snapshot Schedule .....	184
Deleting Snapshots .....	185
Understanding Volume Status and Transitions .....	193
Managing Your Tape Gateway .....	200
Adding Tapes .....	201
Managing Automatic Tape Creation .....	201
Archiving Tapes .....	202
Moving a Tape from Glacier to Deep Archive .....	203
Retrieving Archived Tapes .....	203
Viewing Tape Usage .....	204
Deleting Tapes .....	204
Deleting Custom Tape Pools .....	205
Disabling Your Tape Gateway .....	205
Understanding Tape Status .....	206
Moving your data to a new gateway .....	207
Migrating your Amazon S3 File Gateway .....	208
Moving stored volumes to a new stored volume gateway .....	208
Moving cached volumes to a new cached volume gateway virtual machine .....	209
Moving virtual tapes to a new tape gateway .....	211
Monitoring Storage Gateway .....	215
Understanding gateway metrics .....	215
Dimensions for Storage Gateway metrics .....	219
Monitoring the upload buffer .....	220
Monitoring cache storage .....	222
Understanding CloudWatch alarms .....	223
Creating CloudWatch alarms for Storage Gateway .....	223
Monitoring your file gateway .....	225
Getting file gateway health logs .....	225
Using Amazon CloudWatch metrics .....	226

Getting notified about file operations .....	227
Understanding file share metrics .....	233
Understanding file gateway audit logs .....	234
Monitoring Your Volume Gateway .....	237
Getting Volume Gateway Health Logs .....	237
Using Amazon CloudWatch Metrics .....	238
Measuring Performance Between Your Application and Gateway .....	239
Measuring Performance Between Your Gateway and AWS .....	241
Understanding Volume Metrics .....	243
Monitoring Your Tape Gateway .....	247
Getting Tape Gateway Health Logs .....	247
Using Amazon CloudWatch Metrics .....	248
Understanding Virtual Tape Metrics .....	249
Measuring Performance Between Your Tape Gateway and AWS .....	250
Maintaining Your Gateway .....	253
Shutting Down Your Gateway VM .....	253
Starting and Stopping a Volume or Tape Gateway .....	253
Managing local disks .....	254
Deciding the amount of local disk storage .....	254
Sizing the upload buffer .....	255
Sizing cache storage .....	256
Configuring an upload buffer and cache storage .....	256
Using ephemeral storage with EC2 gateways .....	257
Managing Bandwidth .....	258
Changing Bandwidth Throttling Using the Storage Gateway Console .....	258
Scheduling Bandwidth Throttling .....	259
Using the AWS SDK for Java .....	260
Using the AWS SDK for .NET .....	261
Using the AWS Tools for Windows PowerShell .....	262
Managing Gateway Updates .....	263
Performing Maintenance Tasks on the Local Console .....	264
Performing tasks on the VM local console (file gateway) .....	265
Performing tasks on the EC2 local console (file gateway) .....	280
Performing Tasks on the VM Local Console (Volume and Tape Gateways) .....	287
Performing Tasks on the EC2 Local Console (Volume and Tape Gateways) .....	304
Accessing the Gateway Local Console .....	310
Configuring Network Adapters for Your Gateway .....	315
Deleting Your Gateway and Removing Resources .....	319
Deleting Your Gateway by Using the Storage Gateway Console .....	320
Removing Resources from a Gateway Deployed On-Premises .....	320
Removing Resources from a Gateway Deployed on an Amazon EC2 Instance .....	321
Performance .....	323
Performance guidance for file gateways .....	323
File gateway performance on Linux clients .....	323
File gateway performance on Windows clients .....	323
Performance guidance for tape gateways .....	325
Optimizing Gateway Performance .....	327
Add Resources to Your Gateway .....	327
Optimize iSCSI Settings .....	328
Use a Larger Block Size for Tape Drives .....	328
Optimize the Performance of Virtual Tape Drives .....	329
Add Resources to Your Application Environment .....	329
Using VMware High Availability with Storage Gateway .....	329
Configure Your vSphere VMware HA Cluster .....	330
Download the .ova Image for Your Gateway Type .....	331
Deploy the Gateway .....	331
(Optional) Add Override Options for Other VMs on Your Cluster .....	331

Activate Your Gateway .....	332
Test Your VMware High Availability Configuration .....	332
Security .....	333
Data protection .....	333
Data encryption .....	334
Configuring CHAP authentication .....	335
Authentication and Access Control .....	336
Authentication .....	336
Access Control .....	337
Overview of Managing Access .....	338
Using Identity-Based Policies (IAM Policies) .....	341
Using ACLs for SMB File Share Access .....	347
Storage Gateway API Permissions Reference .....	349
Logging and Monitoring .....	355
Storage Gateway Information in CloudTrail .....	355
Understanding Storage Gateway Log File Entries .....	356
Compliance validation .....	357
Resilience .....	358
Infrastructure Security .....	358
Security Best Practices .....	359
Troubleshooting gateway issues .....	360
Troubleshooting on-premises gateway issues .....	360
Enabling AWS Support to help troubleshoot your gateway .....	362
Troubleshooting Microsoft Hyper-V setup issues .....	364
Troubleshooting Amazon EC2 gateway issues .....	366
Gateway activation hasn't occurred after a few moments .....	367
Can't find the EC2 gateway instance in the instance list .....	367
Can't attach a an Amazon EBS volume to the EC2 gateway instance .....	367
Can't attach an initiator to a volume target of the EC2 gateway .....	367
No disks available when you try to add storage volumes message .....	368
How to remove a disk allocated as upload buffer space to reduce upload buffer space .....	368
Throughput to or from the EC2 gateway drops to zero .....	368
Enabling AWS Support to help troubleshoot the gateway .....	368
Troubleshooting hardware appliance issues .....	369
How to determine service IP address .....	369
How to perform a factory reset .....	369
How to obtain Dell iDRAC support .....	370
How to find the hardware appliance serial number .....	370
How to get hardware appliance support .....	370
Troubleshooting file gateway issues .....	371
Error: InaccessibleStorageClass .....	371
Error: S3AccessDenied .....	371
Error: InvalidObjectState .....	372
Error: ObjectMissing .....	372
Notification: Reboot .....	372
Notification: HardReboot .....	373
Notification: HealthCheckFailure .....	373
Notification: AvailabilityMonitorTest .....	373
Error: RoleTrustRelationshipInvalid .....	373
Troubleshooting with CloudWatch metrics .....	373
Troubleshooting file share issues .....	375
File share is stuck in CREATING status .....	375
Can't create a file share .....	376
SMB file shares don't allow multiple different access methods .....	376
Multiple file shares can't write to the mapped S3 bucket .....	376
Can't upload files into S3 bucket .....	376
Can't change default encryption to SSE-KMS .....	376

Changes made directly in an S3 bucket with object versioning enabled may affect what you see in your file share .....	377
When writing to an S3 bucket with object versioning enabled, the file gateway may create multiple versions of an S3 object .....	377
Changes to an S3 bucket are not reflected in Storage Gateway .....	378
ACL permissions aren't working as expected .....	379
Gateway performance declined after a recursive operation .....	379
Troubleshooting volume issues .....	379
The Console Says That Your Volume Is Not Configured .....	379
The Console Says That Your Volume Is Irrecoverable .....	380
Your Cached Gateway is Unreachable And You Want to Recover Your Data .....	380
The Console Says That Your Volume Has PASS THROUGH Status .....	380
You Want to Verify Volume Integrity and Fix Possible Errors .....	381
Your Volume's iSCSI Target Doesn't Appear in Windows Disk Management Console .....	381
You Want to Change Your Volume's iSCSI Target Name .....	381
Your Scheduled Volume Snapshot Did Not Occur .....	381
You Need to Remove or Replace a Disk That Has Failed .....	381
Throughput from Your Application to a Volume Has Dropped to Zero .....	382
A Cache Disk in Your Gateway Encounters a Failure .....	382
A Volume Snapshot Has PENDING Status Longer Than Expected .....	382
High Availability Health Notifications .....	383
Troubleshooting virtual tape issues .....	383
Recovering a Virtual Tape From An Unrecoverable Gateway .....	383
Troubleshooting Irrecoverable Tapes .....	385
High Availability Health Notifications .....	383
Troubleshooting high availability issues .....	386
Health notifications .....	386
Metrics .....	387
Recovering your data: best practices .....	388
Recovering from an unexpected VM shutdown .....	388
Recovering data from malfunctioning gateway or VM .....	388
Recovering data from an irrecoverable volume .....	389
Recovering data from an irrecoverable tape .....	389
Recovering data from a malfunctioning cache disk .....	390
Recovering data from a corrupted file system .....	390
Recovering data from an inaccessible data center .....	391
Additional Resources .....	392
Host Setup .....	392
Configuring VMware for Storage Gateway .....	392
Synchronizing Your Gateway VM Time .....	397
Volume or Tape Gateway on Amazon EC2 Host .....	399
File gateway on EC2 host .....	401
Volume Gateway .....	404
Removing Disks from Your Gateway .....	404
EBS Volumes for EC2 Gateways .....	406
Tape Gateway .....	407
Working with VTL Devices .....	407
Working with Tapes .....	411
Getting Activation Key .....	413
Linux command line interface (CLI) .....	413
Microsoft Windows PowerShell .....	413
Connecting iSCSI Initiators .....	414
Connecting to Your Volumes to a Windows Client .....	415
Connecting to VTL Devices .....	418
Connecting Your Volumes or VTL Devices to a Linux Client .....	422
Customizing iSCSI Settings .....	424
Configuring CHAP Authentication .....	430

Using AWS Direct Connect with Storage Gateway .....	437
Port Requirements .....	437
Connecting to Your Gateway .....	440
Getting an IP Address from an Amazon EC2 Host .....	440
Understanding Resources and Resource IDs .....	441
Working with Resource IDs .....	441
Tagging Your Resources .....	442
Working with Tags .....	442
Open-Source Components .....	443
Storage Gateway quotas .....	444
Quotas for volumes .....	444
Quotas for tapes .....	444
Recommended local disk sizes for your gateway .....	445
API Reference .....	446
Required Request Headers .....	446
Signing Requests .....	447
Example Signature Calculation .....	448
Error Responses .....	449
Exceptions .....	450
Operation Error Codes .....	451
Error Responses .....	463
Operations .....	465
Document history .....	466
Earlier updates .....	475

Amazon S3 File Gateway documentation has been moved to [What is Amazon S3 File Gateway](#)

# What is AWS Storage Gateway?

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless integration with data security features between your on-premises IT environment and the AWS storage infrastructure. You can use the service to store data in the Amazon Web Services Cloud for scalable and cost-effective storage that helps maintain data security.

AWS Storage Gateway offers file-based file gateways (Amazon S3 File and Amazon FSx File), volume-based (Cached and Stored), and tape-based storage solutions:

## Topics

- [Amazon S3 File Gateway \(p. 1\)](#)
- [Amazon FSx File Gateway \(p. 1\)](#)
- [Tape Gateway \(p. 1\)](#)
- [Volume Gateway \(p. 2\)](#)
- [Are you a first-time Storage Gateway user? \(p. 2\)](#)
- [How Storage Gateway works \(architecture\) \(p. 3\)](#)
- [Storage Gateway pricing \(p. 9\)](#)
- [Plan your Storage Gateway deployment \(p. 9\)](#)

## Amazon S3 File Gateway

Amazon S3 File Gateway supports a file interface into Amazon Simple Storage Service (Amazon S3) and combines a service and a virtual software appliance. By using this combination, you can store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS) and Server Message Block (SMB). The software appliance, or gateway, is deployed into your on-premises environment as a virtual machine (VM) running on VMware ESXi, Microsoft Hyper-V, or Linux Kernel-based Virtual Machine (KVM) hypervisor. The gateway provides access to objects in S3 as files or file share mount points.

**Documentation:** For Amazon S3 File Gateway documentation, see [What is Amazon S3 File Gateway?](#).

## Amazon FSx File Gateway

Amazon FSx File Gateway (FSx File) is a new file gateway type that provides low latency, and efficient access to in-cloud Amazon FSx for Windows File Server file shares from your on-premises facility. If you maintain on-premises file storage because of latency or bandwidth requirements, you can instead use FSx File for seamless access to fully managed, highly reliable, and virtually unlimited Windows file shares provided in the Amazon Web Services Cloud by Amazon FSx for Windows File Server.

**Documentation:** For Amazon S3 File Gateway documentation, see [What is Amazon FSx File Gateway?](#).

## Tape Gateway

**Tape Gateway** – A tape gateway provides cloud-backed virtual tape storage. The tape gateway is deployed into your on-premises environment as a VM running on VMware ESXi, KVM, or Microsoft Hyper-V hypervisor.

With a tape gateway, you can cost-effectively and durably archive backup data in GLACIER or DEEP\_ARCHIVE. A tape gateway provides a virtual tape infrastructure that scales seamlessly with your

business needs and eliminates the operational burden of provisioning, scaling, and maintaining a physical tape infrastructure.

You can run Storage Gateway either on-premises as a VM appliance, as a hardware appliance, or in AWS as an Amazon EC2 instance. You deploy your gateway on an EC2 instance to provision iSCSI storage volumes in AWS. You can use gateways hosted on EC2 instances for disaster recovery, data mirroring, and providing storage for applications hosted on Amazon EC2.

For an architectural overview, see [How Storage Gateway works \(architecture\) \(p. 3\)](#). To see the wide range of use cases that AWS Storage Gateway helps make possible, see [AWS Storage Gateway](#).

**Documentation:** For Tape Gateway documentation, see [Creating a Tape Gateway \(p. 84\)](#).

## Volume Gateway

**Volume Gateway** – A volume gateway provides cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers.

The volume gateway is deployed into your on-premises environment as a VM running on VMware ESXi, KVM, or Microsoft Hyper-V hypervisor.

The gateway supports the following volume configurations:

- **Cached volumes** – You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data.
- **Stored volumes** – If you need low-latency access to your entire dataset, first configure your on-premises gateway to store all your data locally. Then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive offsite backups that you can recover to your local data center or Amazon Elastic Compute Cloud (Amazon EC2). For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2.

**Documentation:** For Volume Gateway documentation, see [Creating a Volume Gateway \(p. 67\)](#).

## Are you a first-time Storage Gateway user?

In the following documentation, you can find a Getting Started section that covers setup information common to all gateways and also gateway-specific setup sections. The Getting Started section shows you how to deploy, activate, and configure storage for a gateway. The management section shows you how to manage your gateway and resources:

- [Creating a file gateway \(p. 40\)](#) provides instructions on how to create and use a file gateway. It shows you how to create a file share, map your drive to an Amazon S3 bucket, and upload files and folders to Amazon S3.
- [Creating a Volume Gateway \(p. 67\)](#) describes how to create and use a volume gateway. It shows you how to create storage volumes and back up data to the volumes.
- [Creating a Tape Gateway \(p. 84\)](#) provides instructions on how to create and use a tape gateway. It shows you how to back up data to virtual tapes and archive the tapes.

- [Managing Your Gateway \(p. 162\)](#) describes how to perform management tasks for all gateway types and resources.

In this guide, you can primarily find how to work with gateway operations by using the AWS Management Console. If you want to perform these operations programmatically, see the [AWS Storage Gateway API Reference](#).

## How Storage Gateway works (architecture)

Following, you can find an architectural overview of the available Storage Gateway solutions.

### Topics

- [File gateways \(p. 3\)](#)
- [Volume gateways \(p. 4\)](#)
- [Tape gateways \(p. 7\)](#)

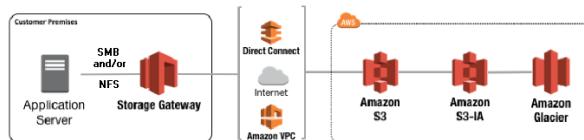
## File gateways

To use a file gateway, you start by downloading a VM image for the file gateway. You then activate the file gateway from the AWS Management Console or through the Storage Gateway API. You can also create a file gateway using an Amazon EC2 image.

After the file gateway is activated, you create and configure your file share and associate that share with your Amazon Simple Storage Service (Amazon S3) bucket. Doing this makes the share accessible by clients using either the Network File System (NFS) or Server Message Block (SMB) protocol. Files written to a file share become objects in Amazon S3, with the path as the key. There is a one-to-one mapping between files and objects, and the gateway asynchronously updates the objects in Amazon S3 as you change the files. Existing objects in the Amazon S3 bucket appear as files in the file system, and the key becomes the path. Objects are encrypted with Amazon S3-server-side encryption keys (SSE-S3). All data transfer is done through HTTPS.

The service optimizes data transfer between the gateway and AWS using multipart parallel uploads or byte-range downloads, to better use the available bandwidth. Local cache is maintained to provide low latency access to the recently accessed data and reduce data egress charges. CloudWatch metrics provide insight into resource use on the VM and data transfer to and from AWS. CloudTrail tracks all API calls.

With file gateway storage, you can do such tasks as ingesting cloud workloads to Amazon S3, performing backups and archiving, tiering, and migrating storage data to the Amazon Web Services Cloud. The following diagram provides an overview of file storage deployment for Storage Gateway.



File gateway converts files to S3 objects when uploading files to Amazon S3. The interaction between file operations performed against files shares on File gateway and S3 objects requires certain operations to be carefully considered when converting between files and objects.

Common file operations change file metadata, which results in the deletion of the current S3 object and the creation of a new S3 object. The following table shows example file operations and the impact on S3 objects.

File operation	S3 object impact	Storage class implication
Rename file	Replaces existing S3 object and creates a new S3 object for each file	Early deletion fees and retrieval fees may apply
Rename folder	Replaces all existing S3 objects and creates new S3 objects for each folder and files in the folder structure	Early deletion fees and retrieval fees may apply
Change file/folder permissions	Replaces existing S3 object and creates a new S3 object for each file or folder	Early deletion fees and retrieval fees may apply
Change file/folder ownership	Replaces existing S3 object and creates a new S3 object for each file or folder	Early deletion fees and retrieval fees may apply
Append to a file	Replaces existing S3 object and creates a new S3 object for each file	Early deletion fees and retrieval fees may apply

When a file is written to the file gateway by an NFS or SMB client, the file gateway uploads the file's data to Amazon S3 followed by its metadata, (ownerships, timestamps, etc.). Uploading the file data creates an S3 object, and uploading the metadata for the file updates the metadata for the S3 object. This process creates another version of the object, resulting in two versions of an object. If S3 Versioning is enabled, both versions will be stored.

When a file is modified in the file gateway by an NFS or SMB client after it has been uploaded to Amazon S3, the file gateway uploads the new or modified data instead of uploading the whole file. The file modification results in a new version of the S3 object being created.

When the file gateway uploads larger files, it might need to upload smaller chunks of the file before the client is done writing to the file gateway. Some reasons for this include freeing up cache space or a high rate of writes to a file share. This can result in multiple versions of an object in the S3 bucket.

You should monitor your S3 bucket to determine how many versions of an object exist before setting up lifecycle policies to move objects to different storage classes. You should configure lifecycle expiration for previous versions to minimize the number of versions you have for an object in your S3 bucket. The use of Same-Region replication (SRR) or Cross-Region replication (CRR) between S3 buckets will increase the storage used.

## Volume gateways

For volume gateways, you can use either cached volumes or stored volumes.

### Topics

- [Cached volumes architecture \(p. 4\)](#)
- [Stored volumes architecture \(p. 6\)](#)

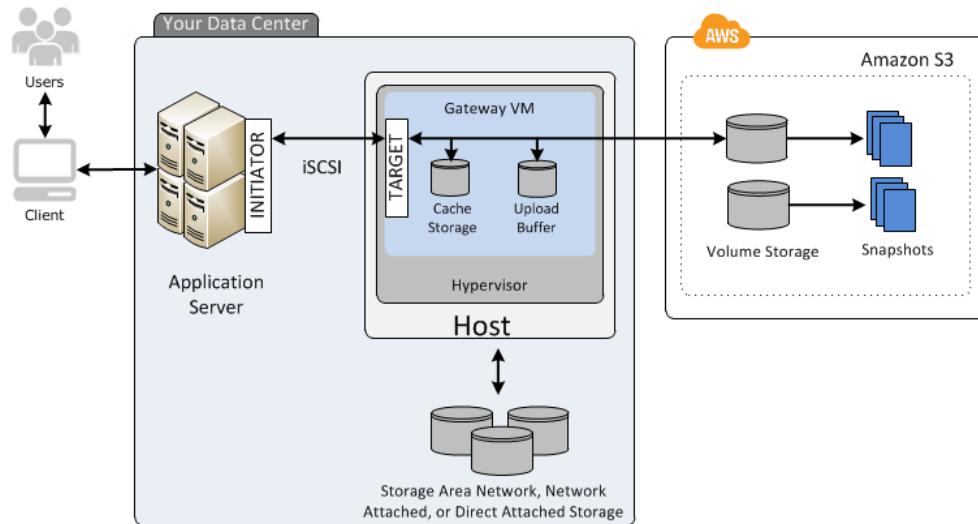
## Cached volumes architecture

By using cached volumes, you can use Amazon S3 as your primary data storage, while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale

your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. You can create storage volumes up to 32 TiB in size and attach to them as iSCSI devices from your on-premises application servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage.

Cached volumes can range from 1 GiB to 32 TiB in size and must be rounded to the nearest GiB. Each gateway configured for cached volumes can support up to 32 volumes for a total maximum storage volume of 1,024 TiB (1 PiB).

In the cached volumes solution, Storage Gateway stores all your on-premises application data in a storage volume in Amazon S3. The following diagram provides an overview of the cached volumes deployment.



After you install the Storage Gateway software appliance—the VM—on a host in your data center and activate it, you use the AWS Management Console to provision storage volumes backed by Amazon S3. You can also provision storage volumes programmatically using the Storage Gateway API or the AWS SDK libraries. You then mount these storage volumes to your on-premises application servers as iSCSI devices.

You also allocate disks on-premises for the VM. These on-premises disks serve the following purposes:

- **Disks for use by the gateway as cache storage** – As your applications write data to the storage volumes in AWS, the gateway first stores the data on the on-premises disks used for cache storage. Then the gateway uploads the data to Amazon S3. The cache storage acts as the on-premises durable store for data that is waiting to upload to Amazon S3 from the upload buffer.

The cache storage also lets the gateway store your application's recently accessed data on-premises for low-latency access. If your application requests data, the gateway first checks the cache storage for the data before checking Amazon S3.

You can use the following guidelines to determine the amount of disk space to allocate for cache storage. Generally, you should allocate at least 20 percent of your existing file store size as cache storage. Cache storage should also be larger than the upload buffer. This guideline helps make sure that cache storage is large enough to persistently hold all data in the upload buffer that has not yet been uploaded to Amazon S3.

- **Disks for use by the gateway as the upload buffer** – To prepare for upload to Amazon S3, your gateway also stores incoming data in a staging area, referred to as an *upload buffer*. Your gateway uploads this buffer data over an encrypted Secure Sockets Layer (SSL) connection to AWS, where it is stored encrypted in Amazon S3.

You can take incremental backups, called *snapshots*, of your storage volumes in Amazon S3. These point-in-time snapshots are also stored in Amazon S3 as Amazon EBS snapshots. When you take a new snapshot, only the data that has changed since your last snapshot is stored. You can initiate snapshots on a scheduled or one-time basis. When you delete a snapshot, only the data not needed for any other snapshots is removed. For information about Amazon EBS snapshots, see [Amazon EBS snapshots](#).

You can restore an Amazon EBS snapshot to a gateway storage volume if you need to recover a backup of your data. Alternatively, for snapshots up to 16 TiB in size, you can use the snapshot as a starting point for a new Amazon EBS volume. You can then attach this new Amazon EBS volume to an Amazon EC2 instance.

All gateway data and snapshot data for cached volumes is stored in Amazon S3 and encrypted at rest using server-side encryption (SSE). However, you can't access this data with the Amazon S3 API or other tools such as the Amazon S3 Management Console.

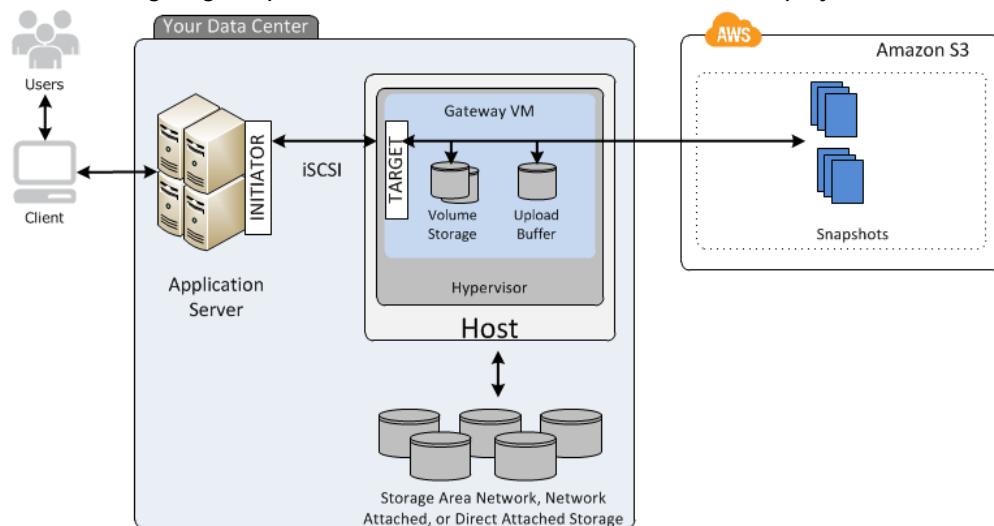
## Stored volumes architecture

By using stored volumes, you can store your primary data locally, while asynchronously backing up that data to AWS. Stored volumes provide your on-premises applications with low-latency access to their entire datasets. At the same time, they provide durable, offsite backups. You can create storage volumes and mount them as iSCSI devices from your on-premises application servers. Data written to your stored volumes is stored on your on-premises storage hardware. This data is asynchronously backed up to Amazon S3 as Amazon Elastic Block Store (Amazon EBS) snapshots.

Stored volumes can range from 1 GiB to 16 TiB in size and must be rounded to the nearest GiB. Each gateway configured for stored volumes can support up to 32 volumes and a total volume storage of 512 TiB (0.5 PiB).

With stored volumes, you maintain your volume storage on-premises in your data center. That is, you store all your application data on your on-premises storage hardware. Then, using features that help maintain data security, the gateway uploads data to the Amazon Web Services Cloud for cost-effective backup and rapid disaster recovery. This solution is ideal if you want to keep data locally on-premises, because you need to have low-latency access to all your data, and also to maintain backups in AWS.

The following diagram provides an overview of the stored volumes deployment.



After you install the Storage Gateway software appliance—the VM—on a host in your data center and activated it, you can create gateway *storage volumes*. You then map them to on-premises direct-attached storage (DAS) or storage area network (SAN) disks. You can start with either new disks or disks already

holding data. You can then mount these storage volumes to your on-premises application servers as iSCSI devices. As your on-premises applications write data to and read data from a gateway's storage volume, this data is stored and retrieved from the volume's assigned disk.

To prepare data for upload to Amazon S3, your gateway also stores incoming data in a staging area, referred to as an *upload buffer*. You can use on-premises DAS or SAN disks for working storage. Your gateway uploads data from the upload buffer over an encrypted Secure Sockets Layer (SSL) connection to the Storage Gateway service running in the Amazon Web Services Cloud. The service then stores the data encrypted in Amazon S3.

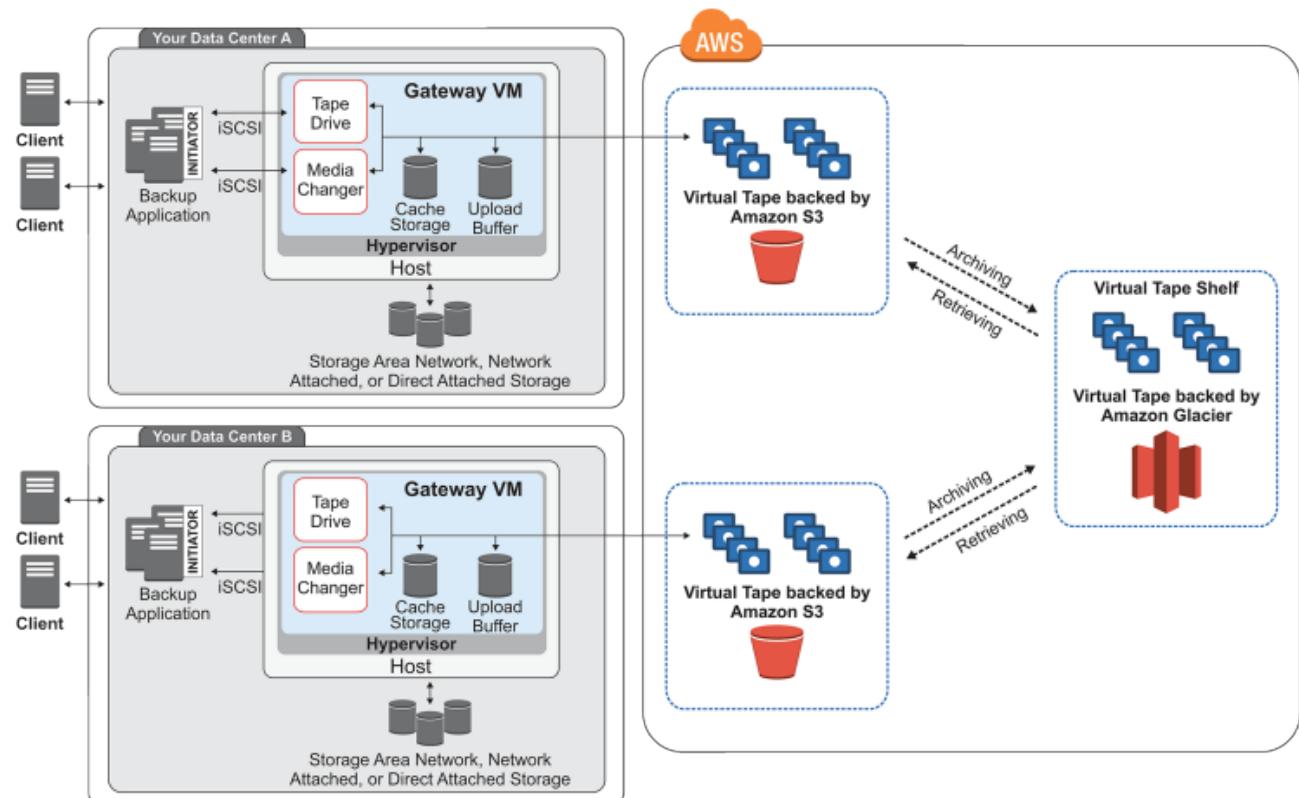
You can take incremental backups, called *snapshots*, of your storage volumes. The gateway stores these snapshots in Amazon S3 as Amazon EBS snapshots. When you take a new snapshot, only the data that has changed since your last snapshot is stored. You can initiate snapshots on a scheduled or one-time basis. When you delete a snapshot, only the data not needed for any other snapshot is removed.

You can restore an Amazon EBS snapshot to an on-premises gateway storage volume if you need to recover a backup of your data. You can also use the snapshot as a starting point for a new Amazon EBS volume, which you can then attach to an Amazon EC2 instance.

## Tape gateways

Tape Gateway offers a durable, cost-effective solution to archive your data in the Amazon Web Services Cloud. With its virtual tape library (VTL) interface, you use your existing tape-based backup infrastructure to store data on virtual tape cartridges that you create on your tape gateway. Each tape gateway is preconfigured with a media changer and tape drives. These are available to your existing client backup applications as iSCSI devices. You add tape cartridges as you need to archive your data.

The following diagram provides an overview of tape gateway deployment.



The diagram identifies the following tape gateway components:

- **Virtual tape** – A virtual tape is like a physical tape cartridge. However, virtual tape data is stored in the Amazon Web Services Cloud. Like physical tapes, virtual tapes can be blank or can have data written on them. You can create virtual tapes either by using the Storage Gateway console or programmatically by using the Storage Gateway API. Each gateway can contain up to 1,500 tapes or up to 1 PiB of total tape data at a time. The size of each virtual tape, which you can configure when you create the tape, is between 100 GiB and 5 TiB.
- **Virtual tape library (VTL)** – A VTL is like a physical tape library available on-premises with robotic arms and tape drives. Your VTL includes the collection of stored virtual tapes. Each tape gateway comes with one VTL.

The virtual tapes that you create appear in your gateway's VTL. Tapes in the VTL are backed up by Amazon S3. As your backup software writes data to the gateway, the gateway stores data locally and then asynchronously uploads it to virtual tapes in your VTL—that is, Amazon S3.

- **Tape drive** – A VTL tape drive is analogous to a physical tape drive that can perform I/O and seek operations on a tape. Each VTL comes with a set of 10 tape drives, which are available to your backup application as iSCSI devices.
- **Media changer** – A VTL media changer is analogous to a robot that moves tapes around in a physical tape library's storage slots and tape drives. Each VTL comes with one media changer, which is available to your backup application as an iSCSI device.
- **Archive** – Archive is analogous to an offsite tape holding facility. You can archive tapes from your gateway's VTL to the archive. If needed, you can retrieve tapes from the archive back to your gateway's VTL.
- **Archiving tapes** – When your backup software ejects a tape, your gateway moves the tape to the archive for long-term storage. The archive is located in the AWS Region in which you activated the gateway. Tapes in the archive are stored in the virtual tape shelf (VTS). The VTS is backed by [S3 Glacier](#) or [S3 Glacier Deep Archive](#), low-cost storage service for data archiving, backup, and long-term data retention.
- **Retrieving tapes** – You can't read archived tapes directly. To read an archived tape, you must first retrieve it to your tape gateway by using either the Storage Gateway console or the Storage Gateway API.

#### Important

If you archive a tape in GLACIER, you can retrieve the tape typically within 3-5 hours. If you archive the tape in DEEP\_ARCHIVE, you can retrieve it typically within 12 hours.

After you deploy and activate a tape gateway, you mount the virtual tape drives and media changer on your on-premises application servers as iSCSI devices. You create virtual tapes as needed. Then you use your existing backup software application to write data to the virtual tapes. The media changer loads and unloads the virtual tapes into the virtual tape drives for read and write operations.

## Allocating local disks for the gateway VM

Your gateway VM needs local disks, which you allocate for the following purposes:

- **Cache storage** – The cache storage acts as the durable store for data that is waiting to upload to Amazon S3 from the upload buffer.

If your application reads data from a virtual tape, the gateway saves the data to the cache storage. The gateway stores recently accessed data in the cache storage for low-latency access. If your application requests tape data, the gateway first checks the cache storage for the data before downloading the data from AWS.

- **Upload buffer** – The upload buffer provides a staging area for the gateway before it uploads the data to a virtual tape. The upload buffer is also critical for creating recovery points that you can use to recover tapes from unexpected failures. For more information, see [You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway \(p. 383\)](#).

As your backup application writes data to your gateway, the gateway copies data to both the cache storage and the upload buffer. It then acknowledges completion of the write operation to your backup application.

For guidelines on the amount of disk space to allocate for the cache storage and upload buffer, see [Deciding the amount of local disk storage \(p. 254\)](#).

## Storage Gateway pricing

For current information about pricing, see [Pricing](#) on the AWS Storage Gateway details page.

## Plan your Storage Gateway deployment

By using the Storage Gateway software appliance, you can connect your existing on-premises application infrastructure with scalable, cost-effective AWS cloud storage that provides data security features.

To deploy Storage Gateway, you first need to decide on the following two things:

**1. Your storage solution** – Choose from one of the following storage solutions:

- **File Gateway** – You can use a file gateway to ingest files to Amazon S3 for use by object-based workloads and for cost-effective storage for traditional backup applications. You can also use it to tier on-premises file storage to S3. You can cost-effectively and durably store and retrieve your on-premises objects in Amazon S3 using industry-standard file protocols.
- **Volume Gateway** – Using volume gateways, you can create storage volumes in the Amazon Web Services Cloud. Your on-premises applications can access these as Internet Small Computer System Interface (iSCSI) targets. There are two options—cached and stored volumes.

With cached volumes, you store volume data in AWS, with a small portion of recently accessed data in the cache on-premises. This approach enables low-latency access to your frequently accessed dataset. It also provides seamless access to your entire dataset stored in AWS. By using cached volumes, you can scale your storage resource without having to provision additional hardware.

With stored volumes, you store the entire set of volume data on-premises and store periodic point-in-time backups (snapshots) in AWS. In this model, your on-premises storage is primary, delivering low-latency access to your entire dataset. AWS storage is the backup that you can restore in the event of a disaster in your data center.

For an architectural overview of volume gateways, see [Cached volumes architecture \(p. 4\)](#) and [Stored volumes architecture \(p. 6\)](#).

- **Tape Gateway** – If you are looking for a cost-effective, durable, long-term, offsite alternative for data archiving, deploy a tape gateway. With its virtual tape library (VTL) interface, you can use your existing tape-based backup software infrastructure to store data on virtual tape cartridges that you create. For more information, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#). When you archive tapes, you don't worry about managing tapes on your premises and arranging shipments of tapes offsite. For an architectural overview, see [Tape gateways \(p. 7\)](#).

- 2. Hosting option** – You can run Storage Gateway either on-premises as a VM appliance, or as hardware appliance or in AWS as an Amazon EC2 instance. For more information, see [Requirements \(p. 11\)](#). If your data center goes offline and you don't have an available host, you can deploy a gateway on an EC2 instance. Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image.

Additionally, as you configure a host to deploy a gateway software appliance, you need to allocate sufficient storage for the gateway VM.

Before you continue to the next step, make sure that you have done the following:

1. For a gateway deployed on-premises, you choose the type of VM host and set it up. Your options are VMware ESXi Hypervisor, Microsoft Hyper-V, and Linux Kernel-based Virtual Machine (KVM). If you deploy the gateway behind a firewall, make sure that ports are accessible to the gateway VM. For more information, see [Requirements \(p. 11\)](#).
2. For a tape gateway, you have installed client backup software. For more information, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

# Getting Started

In this section, you can find instructions about how to get started with Storage Gateway. To get started, you first sign up for AWS. If you are a first-time user, we recommend that you read the regions and requirements section.

## Topics

- [Sign Up for AWS Storage Gateway \(p. 11\)](#)
- [AWS Regions \(p. 11\)](#)
- [Requirements \(p. 11\)](#)
- [Accessing AWS Storage Gateway \(p. 25\)](#)

## Sign Up for AWS Storage Gateway

To use Storage Gateway, you need an Amazon Web Services account that gives you access to all AWS resources, forums, support, and usage reports. You aren't charged for any of the services unless you use them. If you already have an Amazon Web Services account, you can skip this step.

### To sign up for Amazon Web Services account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

For information about pricing, see [Pricing](#) on the Storage Gateway details page.

## AWS Regions

Storage Gateway stores volume, snapshot, tape, and file data in the AWS Region in which your gateway is activated. File data is stored in the AWS Region where your Amazon S3 bucket is located. You select an AWS Region at the upper right of the Storage Gateway Management Console before you start deploying your gateway.

- Storage Gateway—For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the *AWS General Reference*.
- Storage Gateway Hardware Appliance—For supported AWS Regions you can use with the hardware appliance, see [AWS Storage Gateway Hardware Appliance Regions](#) in the *AWS General Reference*.

## Requirements

Unless otherwise noted, the following requirements are common to all gateway configurations.

## Topics

- [Hardware and storage requirements \(p. 12\)](#)
- [Network and firewall requirements \(p. 13\)](#)
- [Supported hypervisors and host requirements \(p. 22\)](#)

- [Supported NFS clients for a file gateway \(p. 22\)](#)
- [Supported SMB clients for a file gateway \(p. 23\)](#)
- [Supported file system operations for a file gateway \(p. 23\)](#)
- [Supported iSCSI initiators \(p. 23\)](#)
- [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#)

## Hardware and storage requirements

In this section, you can find information about the minimum hardware and settings for your gateway and the minimum amount of disk space to allocate for the required storage. For information about best practices for file gateway performance, see [Performance guidance for file gateways \(p. 323\)](#).

### Hardware requirements for on-premises VMs

When deploying your gateway on-premises, you must make sure that the underlying hardware on which you deploy the gateway VM can dedicate the following minimum resources:

- Four virtual processors assigned to the VM.
- 16 GiB of reserved RAM for file gateways

For volume and tape gateways, your hardware should dedicate the following amounts of RAM:

- 16 GiB of reserved RAM for gateways with cache size up to 16 TiB
- 32 GiB of reserved RAM for gateways with cache size 16 TiB to 32 TiB
- 48 GiB of reserved RAM for gateways with cache size 32 TiB to 64 TiB
- 80 GiB of disk space for installation of VM image and system data.

For more information, see [Optimizing Gateway Performance \(p. 327\)](#). For information about how your hardware affects the performance of the gateway VM, see [AWS Storage Gateway quotas \(p. 444\)](#).

### Requirements for Amazon EC2 instance types

When deploying your gateway on Amazon Elastic Compute Cloud (Amazon EC2), the instance size must be at least **xlarge** for your gateway to function. However, for the compute-optimized instance family the size must be at least **2xlarge**. Use one of the following instance types recommended for your gateway type.

#### Recommended for file gateway types

- General-purpose instance family – m4 or m5 instance type.
- Compute-optimized instance family – c4 or c5 instance types. Choose the **2xlarge** instance size or higher to meet the required RAM requirements.
- Memory-optimized instance family – r3 instance types.
- Storage-optimized instance family – i3 instance types.

#### Note

When you launch your gateway in Amazon EC2, and the instance type you select supports ephemeral storage, the disks are listed automatically. For more information about Amazon EC2 instance storage, see [Instance storage](#) in the *Amazon EC2 User Guide*.

Application writes are stored in the cache synchronously, and then asynchronously uploaded to durable storage in Amazon S3. If the ephemeral storage is lost because an instance stops before the upload is complete, then the data that still resides in cache and has not yet written to S3 can be lost. Before you stop the instance that hosts the gateway make sure the CachePercentDirty CloudWatch metric is 0. For information about ephemeral storage,

see [Using ephemeral storage with EC2 gateways \(p. 257\)](#). For more information about monitoring metrics for your storage gateway, see [Monitoring Storage Gateway \(p. 215\)](#). If you have more than 5 million objects in your S3 bucket and you are using a General Purposes SSD volume, a minimum root EBS volume of 350 GiB is needed for acceptable performance of your gateway during start up. For information about how to increase your volume size, see [Modifying an EBS volume using elastic volumes \(console\)](#).

### Recommended for cached volumes and tape gateway types

- General-purpose instance family – m4 or m5 instance types. We don't recommend using the **m4.16xlarge** instance type.
- Compute-optimized instance family – c4 or c5 instance types. Choose the **2xlarge** instance size or higher to meet the required RAM requirements.
- Storage-optimized instance family – d2, i2, or i3 instance types.

## Storage requirements

In addition to 80 GiB disk space for the VM, you also need additional disks for your gateway.

The following table recommends sizes for local disk storage for your deployed gateway.

Gateway Type	Cache (Minimum)	Cache (Maximum)	Upload Buffer (Minimum)	Upload Buffer (Maximum)	Other Required Local Disks
File gateway	150 GiB	64 TiB	—	—	—
Cached volume gateway	150 GiB	64 TiB	150 GiB	2 TiB	—
Stored volume gateway	—	—	150 GiB	2 TiB	1 or more for stored volume or volumes
Tape gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

#### Note

You can configure one or more local drives for your cache and upload buffer, up to the maximum capacity.

When adding cache or upload buffer to an existing gateway, it's important to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

For information about gateway quotas, see [AWS Storage Gateway quotas \(p. 444\)](#).

## Network and firewall requirements

Your gateway requires access to the internet, local networks, Domain Name Service (DNS) servers, firewalls, routers, and so on. Following, you can find information about required ports and how to allow access through firewalls and routers.

#### Note

In some cases, you might deploy Storage Gateway on Amazon EC2 or use other types of deployment (including on-premises) with network security policies that restrict AWS IP address ranges. In these cases, your gateway might experience service connectivity issues when the

AWS IP range values changes. The AWS IP address range values that you need to use are in the Amazon service subset for the AWS Region that you activate your gateway in. For the current IP range values, see [AWS IP address ranges](#) in the *AWS General Reference*.

**Note**

Network bandwidth requirements vary based on the quantity of data that is uploaded and downloaded by the gateway. A minimum of 100Mbps is required to successfully download, activate, and update the gateway. Your data transfer patterns will determine the bandwidth necessary to support your workload. In some cases, you might deploy Storage Gateway on Amazon EC2 or use other types of deployment

**Topics**

- [Port requirements \(p. 14\)](#)
- [Networking and firewall requirements for the Storage Gateway Hardware Appliance \(p. 18\)](#)
- [Allowing AWS Storage Gateway access through firewalls and routers \(p. 20\)](#)
- [Configuring security groups for your Amazon EC2 gateway instance \(p. 21\)](#)

## Port requirements

Storage Gateway requires certain ports to be allowed for its operation. The following illustrations show the required ports that you must allow for each type of gateway. Some ports are required by all gateway types, and others are required by specific gateway types. For more information about port requirements, see [Port Requirements \(p. 437\)](#).

### Common ports for all gateway types

The following ports are common to all gateway types and are required by all gateway types.

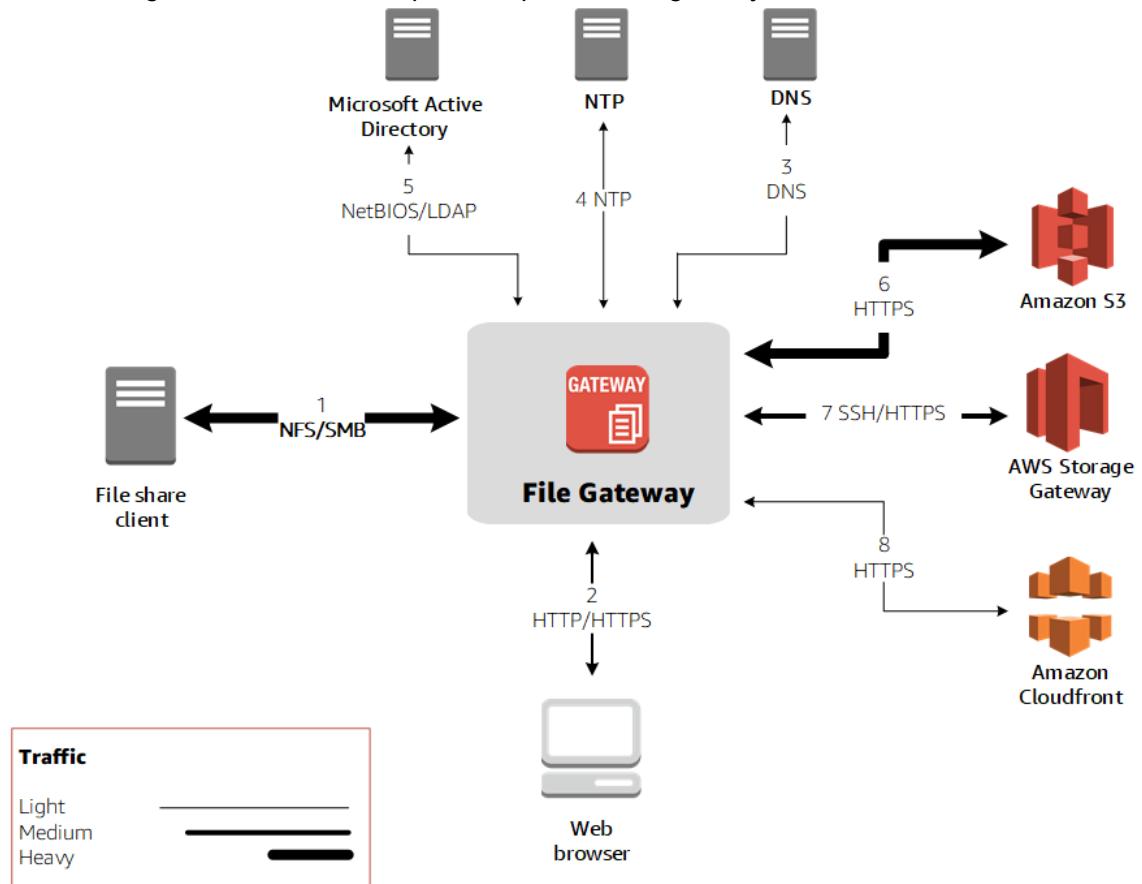
Protocol	Port	Direction	Source	Destination	How Used
TCP	443 (HTTPS)	Outbound	Storage Gateway	AWS	For communication from Storage Gateway to the AWS service endpoint. For information about service endpoints, see <a href="#">Allowing AWS Storage Gateway access through firewalls and routers (p. 20)</a> .
TCP	80 (HTTP)	Inbound	The host from which you connect to the AWS Management Console.	Storage Gateway	By local systems to obtain the storage gateway activation key. Port 80 is only used during activation of

Protocol	Port	Direction	Source	Destination	How Used
					<p>the Storage Gateway appliance.</p> <p>Storage Gateway does not require port 80 to be publicly accessible. The required level of access to port 80 depends on your network configuration. If you activate your gateway from the Storage Gateway Management Console, the host from which you connect to the console must have access to your gateway's port 80.</p>
UDP/UDP	53 (DNS)	Outbound	Storage Gateway	Domain Name Service (DNS) server	For communication between Storage Gateway and the DNS server.
TCP	22 (Support channel)	Outbound	Storage Gateway	AWS Support	Allows AWS Support to access your gateway to help you with troubleshooting gateway issues. You don't need this port open for the normal operation of your gateway, but it is required for troubleshooting.

Protocol	Port	Direction	Source	Destination	How Used
UDP	123 (NTP)	Outbound	NTP client	NTP server	Used by local systems to synchronize VM time to the host time.

### Ports for file gateways

The following illustration shows the ports to open for a file gateway.



#### Note

For specific port requirements (including NFS and SMB port requirements), see [Port Requirements \(p. 437\)](#).

You only need to use Microsoft Active Directory when you want to allow domain users to access an Server Message Block (SMB) file share. You can join your file gateway to any valid Microsoft Windows domain (resolvable by DNS).

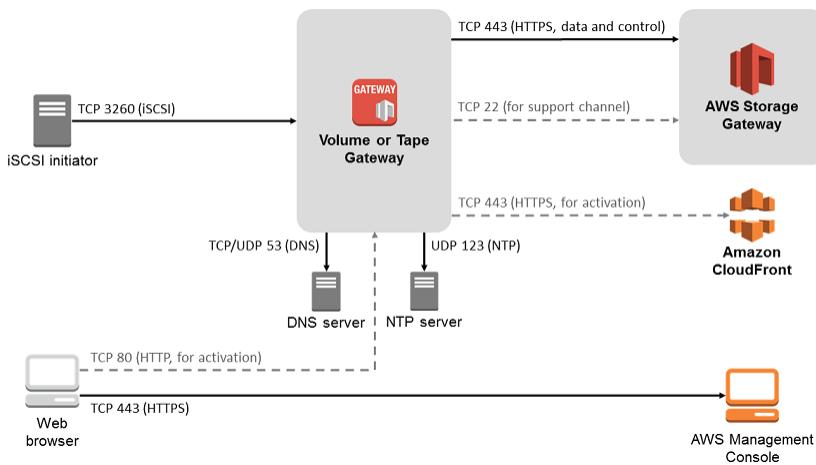
You can also use the AWS Directory Service to create an [AWS managed Microsoft Active Directory](#) in the Amazon Web Services Cloud. For most AWS-managed Active Directory deployments, you need to configure the Dynamic Host Configuration Protocol (DHCP) service for your VPC. For more information about how to create a DHCP options set, see [Create a DHCP options set](#).

In addition to the common ports, file gateways require the following ports.

Protocol	Port	Direction	Source	Destination	How Used
TCP/UDP	2049 (NFS)	Inbound	NFS Clients	Storage Gateway	For local systems to connect to NFS shares that your gateway exposes.
TCP/UDP	111 (NFSv3)	Inbound	NFSv3 client	Storage Gateway	For local systems to connect to the port mapper that your gateway exposes.  <b>Note</b> This port is needed only for NFSv3.
TCP/UDP	20048 (NFSv3)	Inbound	NFSv3 client	Storage Gateway	For local systems to connect to mounts that your gateway exposes.  <b>Note</b> This port is needed only for NFSv3.

#### Ports for volume and tape gateways

The following illustration shows the ports to open for volume and tape gateways.



In addition to the common ports, volume and tape gateways require the following port.

Protocol	Port	Direction	Source	Destination	How Used
TCP	3260 (iSCSI)	Inbound	iSCSI Initiators	Storage Gateway	By local systems to connect to iSCSI targets exposed by the gateway.

For detailed information about port requirements, see [Port Requirements \(p. 437\)](#) in the *Additional Storage Gateway resources* section.

## Networking and firewall requirements for the Storage Gateway Hardware Appliance

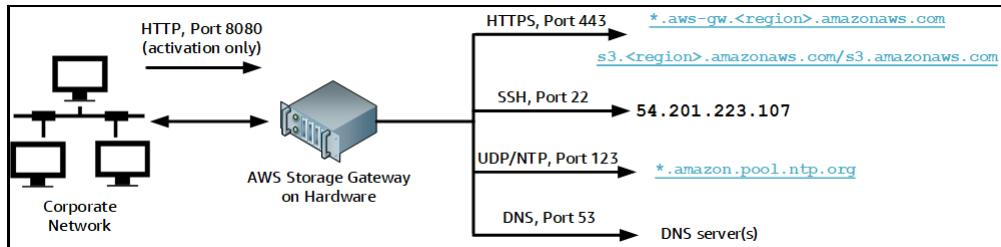
Each Storage Gateway Hardware Appliance requires the following network services:

- **Internet access** – an always-on network connection to the internet through any network interface on the server.
- **DNS services** – DNS services for communication between the hardware appliance and DNS server.
- **Time synchronization** – an automatically configured Amazon NTP time service must be reachable.
- **IP address** – A DHCP or static IPv4 address assigned. You cannot assign an IPv6 address.

There are five physical network ports at the rear of the Dell PowerEdge R640 server. From left to right (facing the back of the server) these ports are as follows:

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

You can use the iDRAC port for remote server management.



A hardware appliance requires the following ports to operate.

Protocol	Port	Direction	Source	Destination	How Used
SSH	22	Outbound	Hardware appliance	54.201.223.107	Support channel
DNS	53	Outbound	Hardware appliance	DNS servers	Name resolution
UDP/NTP	123	Outbound	Hardware appliance	*.amazon.pool.ntp.org	Time synchronization
HTTPS	443	Outbound	Hardware appliance	*.amazonaws.com	Data transfer
HTTP	8080	Inbound	AWS	Hardware appliance	Activation (only briefly)

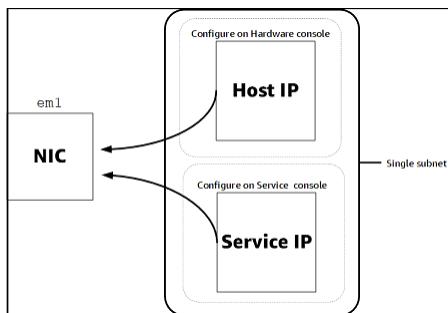
To perform as designed, a hardware appliance requires network and firewall settings as follows:

- Configure all connected network interfaces in the hardware console.
- Make sure that each network interface is on a unique subnet.
- Provide all connected network interfaces with outbound access to the endpoints listed in the diagram preceding.
- Configure at least one network interface to support the hardware appliance. For more information, see [Configuring network parameters \(p. 31\)](#).

#### Note

For an illustration showing the back of the server with its ports, see [Rack-mounting your hardware appliance and connecting it to power \(p. 28\)](#)

All IP addresses on the same network interface (NIC), whether for a gateway or a host, must be on the same subnet. The following illustration shows the addressing scheme.



For more information on activating and configuring a hardware appliance, see [Using the Storage Gateway Hardware Appliance \(p. 26\)](#).

## Allowing AWS Storage Gateway access through firewalls and routers

Your gateway requires access to the following service endpoints to communicate with AWS. If you use a firewall or router to filter or limit network traffic, you must configure your firewall and router to allow these service endpoints for outbound communication to AWS.

**Important**

Depending on your gateway's AWS Region, replace `region` in the service endpoint with the correct region string.

The following service endpoint is required by all gateways for head-bucket operations.

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

The following service endpoints are required by all gateways for control path (anon-cp, client-cp, proxy-app) and data path (dp-1) operations.

```
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
```

The following gateway service endpoint is required to make API calls.

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

The following example is a gateway service endpoint in the US West (Oregon) Region (us-west-2).

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

The Amazon S3 service endpoint, shown following, is used by file gateways only. A file gateway requires this endpoint to access the S3 bucket that a file share maps to.

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

The following example is an S3 service endpoint in the US East (Ohio) Region (us-east-2).

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

**Note**

If your gateway can't determine the AWS Region where your S3 bucket is located, this service endpoint defaults to `s3.us-east-1.amazonaws.com`. We recommend that you allow access to the US East (N. Virginia) Region (`us-east-1`) in addition to AWS Regions where your gateway is activated, and where your S3 bucket is located.

The following are S3 service endpoints for AWS GovCloud (US) Regions.

```
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))
```

The following example is a FIPS service endpoint for an S3 bucket in the AWS GovCloud (US-West) Region.

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

The Amazon CloudFront endpoint following is required for Storage Gateway to get the list of available AWS Regions.

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

A Storage Gateway VM is configured to use the following NTP servers.

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

- Storage Gateway—For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.
- Storage Gateway Hardware Appliance—For supported AWS Regions you can use with the hardware appliance see [Storage Gateway hardware appliance regions](#) in the *AWS General Reference*.

## Configuring security groups for your Amazon EC2 gateway instance

A security group controls traffic to your Amazon EC2 gateway instance. When you configure a security group, we recommend the following:

- The security group should not allow incoming connections from the outside internet. It should allow only instances within the gateway security group to communicate with the gateway. If you need to allow instances to connect to the gateway from outside its security group, we recommend that you allow connections only on ports 3260 (for iSCSI connections) and 80 (for activation).
- If you want to activate your gateway from an Amazon EC2 host outside the gateway security group, allow incoming connections on port 80 from the IP address of that host. If you cannot determine the activating host's IP address, you can open port 80, activate your gateway, and then close access on port 80 after completing activation.
- Allow port 22 access only if you are using AWS Support for troubleshooting purposes. For more information, see [You want AWS Support to help troubleshoot your EC2 gateway \(p. 368\)](#).

In some cases, you might use an Amazon EC2 instance as an initiator (that is, to connect to iSCSI targets on a gateway that you deployed on Amazon EC2. In such a case, we recommend a two-step approach:

1. You should launch the initiator instance in the same security group as your gateway.
2. You should configure access so the initiator can communicate with your gateway.

For information about the ports to open for your gateway, see [Port Requirements \(p. 437\)](#).

## Supported hypervisors and host requirements

You can run Storage Gateway on-premises as either a virtual machine (VM) appliance, or a physical hardware appliance, or in AWS as an Amazon EC2 instance.

Storage Gateway supports the following hypervisor versions and hosts:

- VMware ESXi Hypervisor (version 6.0, 6.5 or 6.7) – A free version of VMware is available on the [VMware website](#). For this setup, you also need a VMware vSphere client to connect to the host.
- Microsoft Hyper-V Hypervisor (version 2012 R2 or 2016) – A free, standalone version of Hyper-V is available at the [Microsoft Download Center](#). For this setup, you need a Microsoft Hyper-V Manager on a Microsoft Windows client computer to connect to the host.
- Linux Kernel-based Virtual Machine (KVM) – A free, open-source virtualization technology. KVM is included in all versions of Linux version 2.6.20 and newer. Storage Gateway is tested and supported for the CentOS/RHEL 7.7, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS distributions. Any other modern Linux distribution may work, but function or performance is not guaranteed. We recommend this option if you already have a KVM environment up and running and you are already familiar with how KVM works.
- Amazon EC2 instance – Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image. Only file, cached volume, and tape gateway types can be deployed on Amazon EC2. For information about how to deploy a gateway on Amazon EC2, see [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#).
- Storage Gateway Hardware Appliance – Storage Gateway provides a physical hardware appliance as a on-premises deployment option for locations with limited virtual machine infrastructure.

### Note

Storage Gateway doesn't support recovering a gateway from a VM that was created from a snapshot or clone of another gateway VM or from your Amazon EC2 AMI. If your gateway VM malfunctions, activate a new gateway and recover your data to that gateway. For more information, see [Recovering from an unexpected virtual machine shutdown \(p. 388\)](#).

Storage Gateway doesn't support dynamic memory and virtual memory ballooning.

## Supported NFS clients for a file gateway

File gateways support the following Network File System (NFS) clients:

- Amazon Linux
- Mac OS X
- RHEL 7
- SUSE Linux Enterprise Server 11 and SUSE Linux Enterprise Server 12
- Ubuntu 14.04
- Microsoft Windows 10 Enterprise, Windows Server 2012, and Windows Server 2016. Native clients only support NFS version 3.

- Windows 7 Enterprise and Windows Server 2008.

Native clients only support NFS v3. The maximum supported NFS I/O size is 32 KB, so you might experience degraded performance on these versions of Windows.

**Note**

You can now use SMB file shares when access is required through Windows (SMB) clients instead of using Windows NFS clients.

## Supported SMB clients for a file gateway

File gateways support the following Service Message Block (SMB) clients:

- Microsoft Windows Server 2008 and later
- Windows desktop versions: 10, 8, and 7.
- Windows Terminal Server running on Windows Server 2008 and later

**Note**

Server Message Block encryption requires clients that support SMB v2.1.

## Supported file system operations for a file gateway

Your NFS or SMB client can write, read, delete, and truncate files. When clients send writes to AWS Storage Gateway, it writes to local Cache synchronously. Then it writes to S3 asynchronously through optimized transfers. Reads are first served through the local cache. If data is not available, it's fetched through S3 as a read-through cache.

Writes and reads are optimized in that only the parts that are changed or requested are transferred through your gateway. Deletes remove objects from S3. Directories are managed as folder objects in S3, using the same syntax as in the Amazon S3 Management Console.

HTTP operations such as `GET`, `PUT`, `UPDATE`, and `DELETE` can modify files in a file share. These operations conform to the atomic create, read, update, and delete (CRUD) functions.

## Supported iSCSI initiators

When you deploy a cached volume or stored volume gateway, you can create iSCSI storage volumes on your gateway. When you deploy a tape gateway, the gateway is preconfigured with one media changer and 10 tape drives. These tape drives and the media changer are available to your existing client backup applications as iSCSI devices.

To connect to these iSCSI devices, Storage Gateway supports the following iSCSI initiators:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

- VMware ESX Initiator, which provides an alternative to using initiators in the guest operating systems of your VMs

**Important**

Storage Gateway doesn't support Microsoft Multipath I/O (MPIO) from Windows clients.

Storage Gateway supports connecting multiple hosts to the same volume if the hosts coordinate access by using Windows Server Failover Clustering (WSFC). However, you can't connect multiple hosts to that same volume (for example, sharing a nonclustered NTFS/ext4 file system) without using WSFC.

## Supported third-party backup applications for a Tape Gateway

You use a backup application to read, write, and manage tapes with a tape gateway. The following third-party backup applications are supported to work with tape gateways.

The type of medium changer you choose depends on the backup application you plan to use. The following table lists third-party backup applications that have been tested and found to be compatible with tape gateways. This table includes the medium changer type recommended for each backup application.

Backup Application	Medium Changer Type
Arcserve Backup	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL or STK-L700
Commvault V11	STK-L700
Dell EMC NetWorker 19.5	AWS-Gateway-VTL
IBM Spectrum Protect v8.1.10	IBM-03584L32-0402
Micro Focus (HPE) Data Protector 9.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 or 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/Network 6.4 or 7.1	STK-L700
Quest NetVault Backup 12.4 or 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014 or 15 or 16 or 20.x	AWS-Gateway-VTL
Veritas Backup Exec 2012	STK-L700
<b>Note</b> Veritas has ended support for Backup Exec 2012.	
Veritas NetBackup Version 7.x or 8.x	AWS-Gateway-VTL

**Important**

We highly recommend that you choose the medium changer that's listed for your backup application. Other medium changers might not function properly. You can choose a different

medium changer after the gateway is activated. For more information, see [Selecting a Medium Changer After Gateway Activation \(p. 408\)](#).

## Accessing AWS Storage Gateway

You can use the [Storage Gateway Management Console](#) to perform various gateway configuration and management tasks. The Getting Started section and various other sections of this guide use the console to illustrate gateway functionality.

To enable browser access to the Storage Gateway console, ensure that your browser has access to the Storage Gateway API endpoint. For more information, see [Storage Gateway endpoints and quotas](#) in the [AWS General Reference](#).

Additionally, you can use the AWS Storage Gateway API to programmatically configure and manage your gateways. For more information about the API, see [API Reference for Storage Gateway \(p. 446\)](#).

You can also use the AWS SDKs to develop applications that interact with Storage Gateway. The AWS SDKs for Java, .NET, and PHP wrap the underlying Storage Gateway API to simplify your programming tasks. For information about downloading the SDK libraries, see [Sample Code Libraries](#).

# Using the Storage Gateway Hardware Appliance

The Storage Gateway Hardware Appliance is a physical hardware appliance with the Storage Gateway software preinstalled on a validated server configuration. You can manage your hardware appliance from the **Hardware** page on the AWS Storage Gateway console.

The hardware appliance is a high-performance 1U server that you can deploy in your data center, or on-premises inside your corporate firewall. When you buy and activate your hardware appliance, the activation process associates your hardware appliance with your Amazon Web Services account. After activation, your hardware appliance appears in the console as a gateway on the **Hardware** page. You can configure your hardware appliance as a file gateway, tape gateway, or volume gateway type. The procedure that you use to deploy and activate these gateway types on a hardware appliance is same as on a virtual platform.

The Storage Gateway Hardware Appliance can be ordered directly from the AWS Storage Gateway console.

## To order a hardware appliance

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home> and choose the AWS Region that you want your appliance in.
2. Choose **Hardware** from the navigation pane.
3. Choose **Order appliance**, and then choose **Proceed**. You are redirected to the AWS Elemental Appliances and Software Management Console to request a sales quote.
4. Fill out the necessary information and choose **Submit**.

Once the information has been reviewed, a sale quote is generated and you are able to proceed with the ordering process and submit a Purchase Order, or arrange for pre-payment.

## To view a sales quote or order history for the hardware appliance

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **Hardware** from the navigation pane.
3. Choose **Quotes and orders**, and then choose **Proceed**. You are redirected to the AWS Elemental Appliances and Software Management Console to review sales quotes and order history.

In the sections that follow, you can find instructions about how to set up, configure, activate, launch, and use an Storage Gateway Hardware Appliance.

## Topics

- [Supported AWS regions \(p. 27\)](#)
- [Setting up your hardware appliance \(p. 27\)](#)
- [Rack-mounting your hardware appliance and connecting it to power \(p. 28\)](#)
- [Configuring network parameters \(p. 31\)](#)

- [Activating your hardware appliance \(p. 33\)](#)
- [Launching a gateway \(p. 36\)](#)
- [Configuring an IP address for the gateway \(p. 37\)](#)
- [Configuring your gateway \(p. 38\)](#)
- [Removing a gateway from the hardware appliance \(p. 38\)](#)
- [Deleting your hardware appliance \(p. 38\)](#)

## Supported AWS regions

Storage Gateway Hardware Appliance is available for shipping worldwide where it is legally allowed and permitted for exporting by the US government. For information about supported AWS Regions, see [Storage Gateway Hardware Appliance Regions](#) in the *AWS General Reference*.

## Setting up your hardware appliance

After you receive your Storage Gateway Hardware Appliance, you use the hardware appliance console to configure networking to provide an always-on connection to AWS and activate your appliance. Activation associates your appliance with the Amazon Web Services account that is used during the activation process. After the appliance is activated, you can launch a file, volume, or tape gateway from the Storage Gateway console.

**Note**

It is your responsibility to ensure the hardware appliance firmware is up-to-date.

### To install and configure your hardware appliance

1. Rack-mount the appliance, and plug in power and network connections. For more information, see [Rack-mounting your hardware appliance and connecting it to power \(p. 28\)](#).
2. Set the Internet Protocol version 4 (IPv4) addresses for both the hardware appliance (the host) and Storage Gateway (the service). For more information, see [Configuring network parameters \(p. 31\)](#).
3. Activate the hardware appliance on the console **Hardware** page in the AWS Region of your choice. For more information, see [Activating your hardware appliance \(p. 33\)](#).
4. Install the Storage Gateway on your hardware appliance. For more information, see [Configuring your gateway \(p. 38\)](#).

You set up gateways on your hardware appliance the same way that you set up gateways on VMware ESXi, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), or Amazon EC2.

### Increasing the usable cache storage

You can increase the usable storage on the hardware appliance from 5 TB to 12 TB. Doing this provides a larger cache for low latency access to data in AWS. If you ordered the 5 TB model, you can increase the usable storage to 12 TB by buying five 1.92 TB SSDs (solid state drives), which are available for ordering on the console **Hardware** page. You can order the additional SSDs by following the same ordering process as ordering a hardware appliance and requesting a sales quote from the Storage Gateway console.

You can then add them to the hardware appliance before you activate it. If you have already activated the hardware appliance and want to increase the usable storage on the appliance to 12 TB, do the following:

1. Reset the hardware appliance to its factory settings. Contact Amazon Web Services Support for instructions on how to do this.
2. Add five 1.92 TB SSDs to the appliance.

#### **Network interface card options**

Depending on the model of appliance you ordered, it may come with a 10G-Base-T copper network card or a 10G DA/SFP+ network card.

- 10G-Base-T NIC configuration:
  - Use CAT6 cables for 10G or CAT5(e) for 1G
- 10G DA/SFP+ NIC configuration:
  - Use Twinax copper Direct Attach Cables up to 5 meters
  - Dell/Intel compatible SFP+ optical modules (SR or LR)
  - SFP/SFP+ copper transceiver for 1G-Base-T or 10G-Base-T

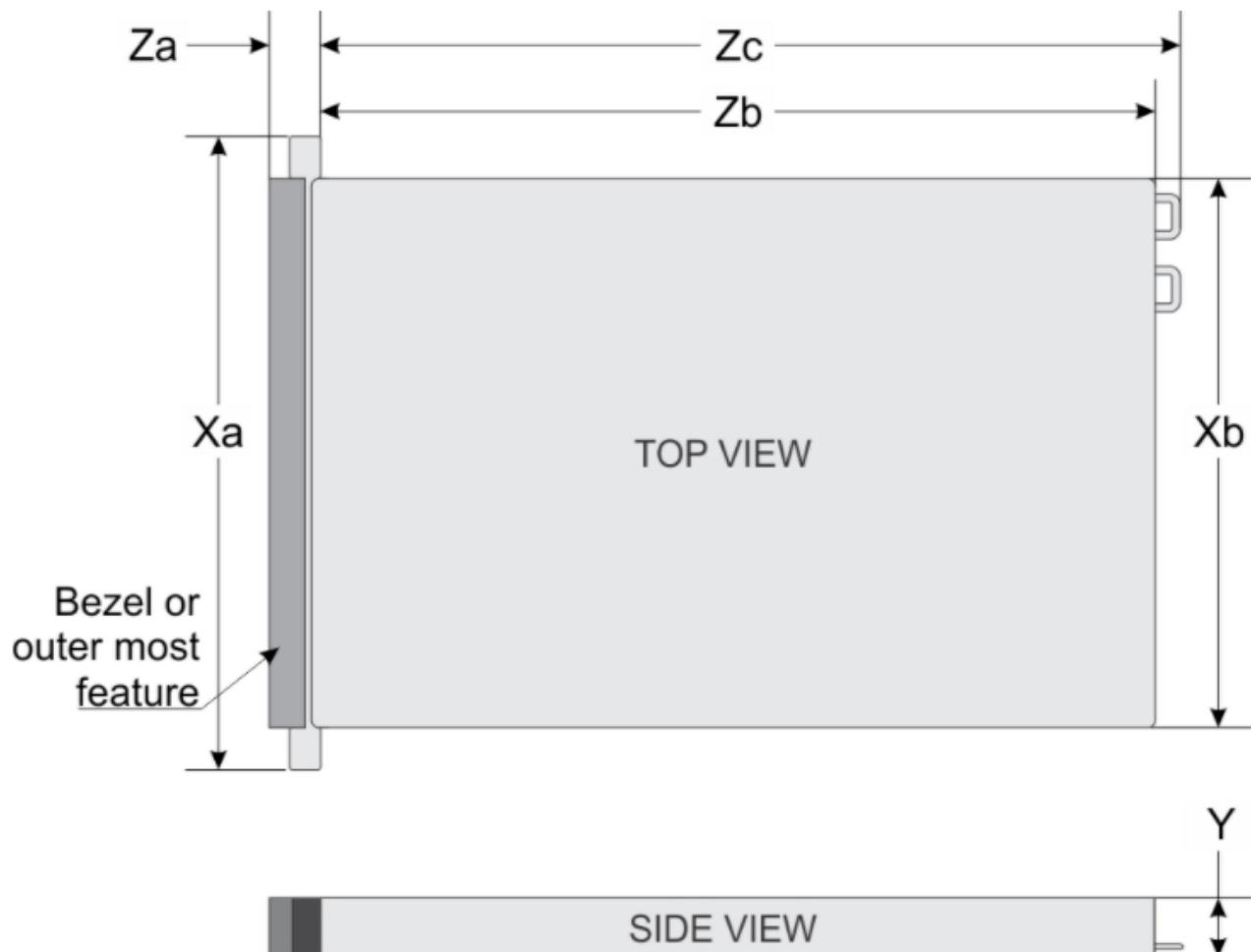
## Rack-mounting your hardware appliance and connecting it to power

After you unbox your Storage Gateway Hardware Appliance, follow the instructions contained in the box to rack-mount the server. Your appliance has a 1U form factor and fits in a standard International Electrotechnical Commission (IEC) compliant 19-inch rack.

To install your hardware appliance, you need the following components:

- Power cables: one required, two recommended.
- Supported network cabling (depending on which Network Interface Card (NIC) is included in the hardware appliance). Twinax Copper DAC, SFP+ optical module (Intel compatible) or SFP to Base-T copper transceiver.
- Keyboard and monitor, or a keyboard, video, and mouse (KVM) switch solution.

## Hardware appliance dimensions



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)

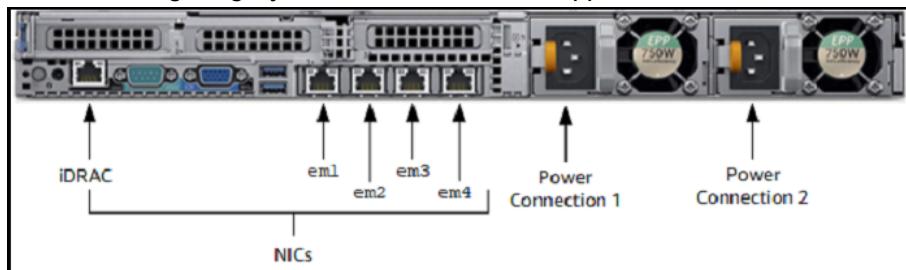
### To connect the hardware appliance to power

#### Note

Before you perform the following procedure, make sure that you meet all of the requirements for the Storage Gateway Hardware Appliance as described in [Networking and firewall requirements for the Storage Gateway Hardware Appliance \(p. 18\)](#).

1. Plug in a power connection to each of the two power supplies. It's possible to plug in to only one power connection, but we recommend power connections to both power supplies.

In the following image, you can see the hardware appliance with the different connections.



2. Plug an Ethernet cable into the em1 port to provide an always-on internet connection. The em1 port is the first of the four physical network ports on the rear, from left to right.

**Note**

The hardware appliance doesn't support VLAN trunking. Set up the switch port to which you are connecting the hardware appliance as a non-trunked VLAN port.

3. Plug in the keyboard and monitor.
4. Power on the server by pressing the **Power** button on the front panel, as shown in the following image.

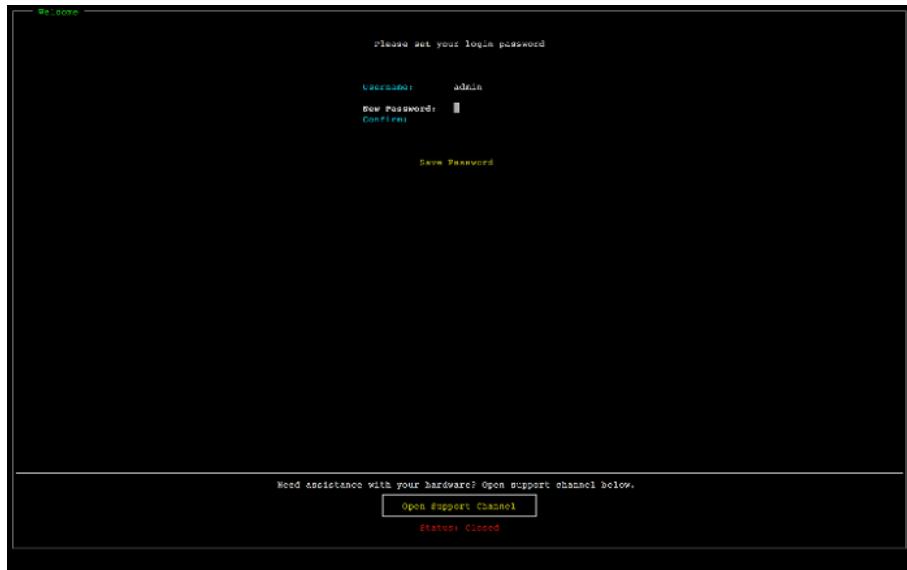


After the server boots up, the hardware console appears on the monitor. The hardware console presents a user interface specific to AWS that you can use to configure initial network parameters. You configure these parameters to connect the appliance to AWS and open up a support channel for troubleshooting by Amazon Web Services Support.

To work with the hardware console, enter text from the keyboard and use the Up, Down, Right, and Left Arrow keys to move about the screen in the indicated direction. Use the Tab key to move forward in order through items on-screen. On some setups, you can use the Shift+Tab keystroke to move sequentially backward. Use the Enter key to save selections, or to choose a button on the screen.

**To set a password for the first time**

1. For **Set Password**, enter a password, and then press Down arrow.
2. For **Confirm**, re-enter your password, and then choose **Save Password**.



At this point, you are in the hardware console, shown following.



### Next step

[Configuring network parameters \(p. 31\)](#)

## Configuring network parameters

After the server boots up, you can enter your first password in the hardware console as described in [Rack-mounting your hardware appliance and connecting it to power \(p. 28\)](#).

Next, on the hardware console take the following steps to configure network parameters so your hardware appliance can connect to AWS.

## To set a network address

1. Choose **Configure Network** and press the **Enter** key. The **Configure Network** screen shown following appears.



2. For **IP Address**, enter a valid IPv4 address from one of the following sources:

- Use the IPv4 address assigned by your Dynamic Host Configuration Protocol (DHCP) server to your physical network port.

If you do so, note this IPv4 address for later use in the activation step.

- Assign a static IPv4 address. To do so, choose **Static** in the **em1** section and press **Enter** to view the **Configure Static IP** screen shown following.

The **em1** section is at upper left section in the group of port settings.

After you have entered a valid IPv4 address, press the **Down arrow** or **Tab**.

### Note

If you configure any other interface, it must provide the same always-on connection to the AWS endpoints listed in the requirements.



3. For **Subnet**, enter a valid subnet mask, and then press Down arrow.
4. For **Gateway**, enter your network gateway's IPv4 address, and then press Down arrow.
5. For **DNS1**, enter the IPv4 address for your Domain Name Service (DNS) server, and then press Down arrow.
6. (Optional) For **DNS2**, enter a second IPv4 address, and then press Down arrow. A second DNS server assignment would provide additional redundancy should the first DNS server become unavailable.
7. Choose **Save** and then press **Enter** to save your static IPv4 address setting for the appliance.

#### To log out of the hardware console

1. Choose **Back** to return to the Main screen.
2. Choose **Logout** to return to the Login screen.

#### Next step

[Activating your hardware appliance \(p. 33\)](#)

## Activating your hardware appliance

After configuring your IP address, you enter this IP address in the console on the **Hardware** page, as described following. The activation process validates that your hardware appliance has the appropriate security credentials and registers the appliance to your Amazon Web Services account.

You can choose to activate your hardware appliance in any of the supported AWS Regions. For a list of supported AWS Regions, see [Storage Gateway Hardware Appliance Regions](#) in the [AWS General Reference](#).

#### To activate your appliance for the first time or in an AWS Region where you have no gateways deployed

1. Sign in to the AWS Management Console and open the Storage Gateway console at [AWS Storage Gateway Management Console](#) with the account credentials to use to activate your hardware.

If this is your first gateway in an AWS Region, you see the splash screen shown following. After you create a gateway in this AWS Region, this screen no longer displays.

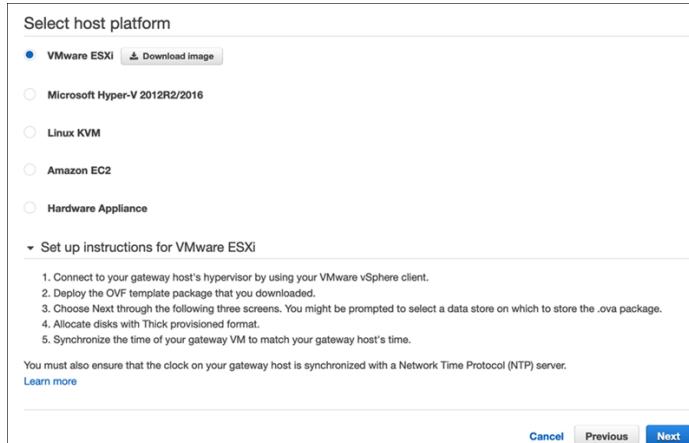


### Note

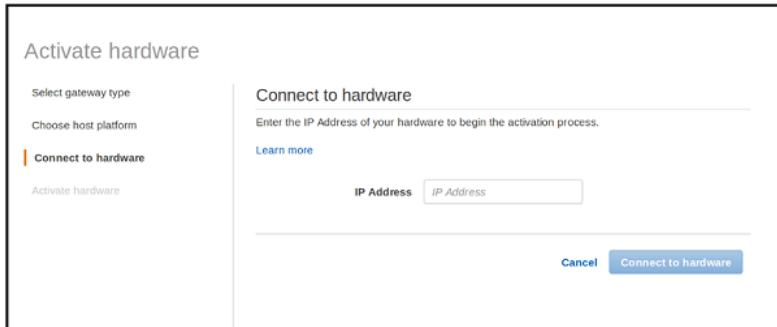
For activation only, the following must be true:

- Your browser must be on the same network as your hardware appliance.
- Your firewall must allow HTTP access on port 8080 to the appliance for inbound traffic.

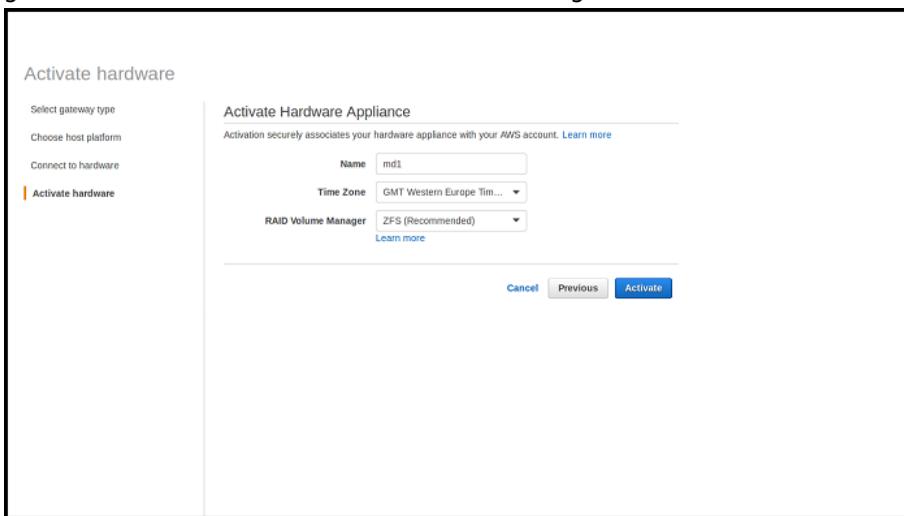
2. Choose **Get started** to view the Create gateway wizard, and then choose **Hardware Appliance** on the **Select host platform** page, as shown following.



3. Choose **Next** to view the **Connect to hardware** screen shown following.



4. For **IP Address**, enter the IPv4 address of your appliance, and then choose **Connect to Hardware** to go to the Activate Hardware screen shown following.



5. For **Hardware name**, enter a name for your appliance. Names can be up to 255 characters long and can't include a slash character.
6. (Optional) For **Hardware time zone**, enter your local settings.

The time zone controls when hardware updates take place, with 2 a.m. local time used as the time for updates.

**Note**

We recommend setting the time zone for your appliance as this determines a standard update time that is out of the usual working day window.

7. (Optional) Keep the **RAID Volume Manager** set to **ZFS**.

ZFS RAID is a software-based, open-source file system and logical volume manager. We recommend using ZFS for most hardware appliance use cases because it offers superior performance and integration compared with MD RAID. The hardware appliance is specifically tuned for ZFS RAID. For more information on ZFS RAID, see the [ZFS Wikipedia page](#).

If you don't want to accept CDDL license terms, as documented in [CDDL 1.0](#) on the Opensource.org site, we also offer MD RAID. For more information on MD RAID, see the [mdadm Wikipedia page](#). To change the volume manager on your hardware appliance, contact [Amazon Web Services Support](#). Amazon Web Services Support can provide an International Organization for Standardization (ISO) standard image, instructions on performing a factory reset of a hardware appliance, and instructions on installing the new ISO image.

8. Choose **Next** to finish activation.

A console banner appears on the Hardware page indicating that the hardware appliance has been successfully activated, as shown following.

At this point, the appliance is associated with your account. The next step is to launch a file, tape, or cached volume gateway on your appliance.

Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
praksuji-bh	vl5ioueix9yotyn5	Dell PowerEdge R640	-
praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Name	praksuji-bh	Vendor	Dell
ID	vl5ioueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

### Next step

[Launching a gateway \(p. 36\)](#)

## Launching a gateway

You can launch any of the three storage gateways on the appliance—file gateway, volume gateway (cached), or tape gateway.

### To launch a gateway on your hardware appliance

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **Hardware**.
3. For **Actions**, choose **Launch Gateway**.
4. For **Gateway Type**, choose the type of gateway you want to create.

#### Note

Storage Gateway offers the following gateway types:

- [FSx File Gateway](#)
- [S3 File Gateway](#)
- [Tape Gateway](#)
- [Volume Gateway](#)

5. For **Gateway name**, enter a name for your gateway. Names can be 255 characters long and can't include a slash character.
6. Choose **Launch gateway**.

The Storage Gateway software for your chosen gateway type installs on the appliance. It can take up to 5–10 minutes for a gateway to show up as **online** in the console.

To assign a static IP address to your installed gateway, you next configure the gateway's network interfaces so your applications can use it.

**Next step**

[Configuring an IP address for the gateway \(p. 37\)](#)

## Configuring an IP address for the gateway

To assign a static IP address to a gateway installed on your hardware appliance, configure the IP address from the local console of that gateway. Your applications (such as your NFS or SMB client, your iSCSI initiator, and so on) connect to this IP address. You can access the gateway local console from the hardware appliance console.

### To configure an IP address on your appliance to work with applications

1. On the hardware console, choose **Open Service Console** to open a login screen for the gateway local console.
2. Enter the localhost **login** password, and then press **Enter**.

The default account is **admin** and the default password is **password**.

3. Change the default password. Choose **Actions** then **Set Local Password** and enter your new credentials in the **Set Local Password** dialog box.
4. (Optional) Configure your proxy settings. See [the section called "Setting the Local Console Password from the Storage Gateway Console" \(p. 289\)](#) for instructions.

5. Navigate to the Network Settings page of the gateway local console as shown following.

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: \_

6. Type 2 to go to the **Network Configuration** page shown following.

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: \_

7. Configure a static or DHCP IP address for the network port on your hardware appliance to present a file, volume, and tape gateway for applications. This IP address must be on the same subnet as the IP address used during hardware appliance activation.

### To exit the gateway local console

- Press the **Crtl+]** (close bracket) keystroke. The hardware console appears.

**Note**

The keystroke preceding is the only way to exit the gateway local console.

**Next step**

[Configuring your gateway \(p. 38\)](#)

## Configuring your gateway

After your hardware appliance has been activated and configured, your appliance appears in the console. Now you can create the type of gateway that you want. Continue the installation for your gateway type at the one of the configure local disks sections:

- For file gateway, see: [Configuring local disks \(p. 45\)](#).
- For tape gateway, see: [Configuring Local Disks \(p. 90\)](#).
- For volume gateway, see: [Configuring Local Disks \(p. 71\)](#).

## Removing a gateway from the hardware appliance

To remove gateway software from your hardware appliance, use the following procedure. After you do so, the gateway software is uninstalled from your hardware appliance.

### To remove a gateway from a hardware appliance

1. From the **Hardware** page of the Storage Gateway console, choose the check box for the hardware appliance.
2. From the **Actions** menu, choose **Remove Gateway**.
3. In the **Remove gateway from hardware appliance** dialog box, type *remove* in the input field, then choose **Remove**.

#### Note

When you delete a gateway, you can't undo the action. For certain gateway types, you can lose data on deletion, particularly cached data. For more information on deleting a gateway, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).

Deleting a gateway doesn't delete the hardware appliance from the console. The hardware appliance remains for future gateway deployments.

## Deleting your hardware appliance

After you activate your hardware appliance in your Amazon Web Services account, you might have a need to move and activate it in a different Amazon Web Services account. In this case, you first delete the appliance from the Amazon Web Services account and activate it in another Amazon Web Services account. You might also want to delete the appliance completely from your Amazon Web Services account because you no longer need it. Follow these instructions to delete your hardware appliance.

### To delete your hardware appliance

1. If you have installed a gateway on the hardware appliance, you must first remove the gateway before you can delete the appliance. For instructions on how to remove a gateway from your hardware appliance, see [Removing a gateway from the hardware appliance \(p. 38\)](#).
2. On the Hardware page, choose the hardware appliance you want to delete.

3. For **Actions**, choose **Delete Appliance**.
4. In the **Confirm deletion of resource(s)** dialog box, choose the confirmation check box and choose **Delete**. A message indicating successful deletion is displayed.

When you delete the hardware appliance, all the resources associated with the gateway that is installed on the appliance are deleted also, but the data on the hardware appliance itself is not deleted.

# Creating Your Gateway

To create your gateway, open the [Storage Gateway Management Console](#) and choose the AWS Region that you want to create your gateway in. If you haven't created a gateway in this AWS Region, the Storage Gateway service homepage is displayed.



Choose **Get started** to open the **Create gateway** page. On this page, you choose a gateway type. If you have a gateway in the current AWS Region, the console shows your gateway in the console.

## Topics

- [Creating a file gateway \(p. 40\)](#)
- [Creating a Volume Gateway \(p. 67\)](#)
- [Creating a Tape Gateway \(p. 84\)](#)
- [Using a Tape Gateway on an AWS Snowball Edge device \(p. 149\)](#)
- [Activating a gateway in a virtual private cloud \(p. 153\)](#)

## Creating a file gateway

### Note

The documentation for the file gateway that supports a file interface into Amazon Simple Storage Service has moved to [What is Amazon S3 File Gateway?](#).

In this section, you can find instructions about how to create and use a file gateway.

## Topics

- [Creating a gateway \(p. 40\)](#)
- [Creating a file share \(p. 46\)](#)
- [Using your file share \(p. 61\)](#)

## Creating a gateway

### Note

The documentation for the file gateway that supports a file interface into Amazon Simple Storage Service has moved to [What is Amazon S3 File Gateway?](#).

In this section, you can find instructions about how to create, deploy, and activate a file gateway.

## Topics

- [Choosing a gateway type \(p. 41\)](#)
- [Choosing a host platform and downloading the VM \(p. 41\)](#)
- [Choosing a service endpoint \(p. 42\)](#)
- [Connecting to the gateway \(p. 43\)](#)
- [Activating the gateway \(p. 44\)](#)
- [Configuring local disks \(p. 45\)](#)
- [Configuring Amazon CloudWatch logging \(p. 45\)](#)
- [Verifying VMware High Availability \(VMware HA clusters only\) \(p. 45\)](#)

## Choosing a gateway type

With a file gateway, you store and retrieve objects in Amazon S3 with a local cache for low latency access to your most recently used data.

### To choose a gateway type

1. Open the AWS Management Console at <https://console.aws.amazon.com/storagegateway/home/>, and choose the AWS Region that you want to create your gateway in.  
  
If you have previously created a gateway in this AWS Region, the console shows your gateway. Otherwise, the service homepage appears.
2. If you haven't created a gateway in the AWS Region that you chose, choose **Get started**. If you already have a gateway in the AWS Region that you chose, choose **Gateways** from the navigation pane, and then choose **Create gateway**.
3. For **Select gateway type**, choose **File gateway**, and then choose **Next**.

## Choosing a host platform and downloading the VM

If you create your gateway on-premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see [Supported hypervisors and host requirements \(p. 22\)](#).

#### Note

You can run only file, cached volume, and tape gateways on an Amazon EC2 instance.

### To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:
  - If you choose the hardware appliance, activate it by following the instructions in [Activating your hardware appliance \(p. 33\)](#).
  - If you choose one of the other options, choose **Download image** next to your virtualization platform to download a .zip file that contains the .ova file for your virtualization platform.

#### Note

The .zip file is over 500 MB in size and might take some time to download, depending on your network connection.

For Amazon EC2, you create an instance from the provided AMI.

3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache and one local disk for your upload buffer during the deployment. A file

gateway requires only one local disk for a cache. For information about local disk requirements, see [Hardware and storage requirements \(p. 12\)](#).

Depending your hypervisor, set certain options:

- If you choose VMware, do the following:
  - Store your disk using the **Thick provisioned format** option. When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in thick-provisioned format.
  - Configure your gateway VM to use paravirtualized disk controllers. For more information, see [Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers \(p. 395\)](#).
- If you choose Microsoft Hyper-V, do the following:
  - Configure the disk type using the **Fixed size** option. When you use fixed-size provisioning, the disk storage is allocated immediately, resulting in better performance. If you don't use fixed-size provisioning, the storage is allocated on demand. On-demand allocation can affect the functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in fixed-size provisioned format.
  - When allocating disks, choose **virtual hard disk (.vhdx) file**. Storage Gateway supports the .vhdx file type. By using this file type, you can create larger virtual disks than with other file types. If you create a .vhdx type virtual disk, make sure that the size of the virtual disks that you create doesn't exceed the recommended disk size for your gateway.
- If you choose Linux Kernel-bases Virtual Machine (KVM), do the following:
  - Don't configure your disk to use **sparse** formatting. When you use fixed-size (nonsparse) provisioning, the disk storage is allocated immediately, resulting in better performance.
  - Use the parameter **sparse=false** to store your disk in nonsparse format when creating new virtual disks in the VM with the **virt-install** command for provisioning new virtual machines.
  - Use **virtio** drivers for disk and network devices.
  - We recommend that you don't set the **current\_memory** option. If necessary, set it equal to the RAM provisioned to the gateway in the **--ram** parameter.

Following is an example **virt-install** command for installing KVM.

```
virt-install --name "SGW_KVM" --description "SGW KVM" --os-type=generic --  
ram=32768 --vcpus=16 --disk path=fgw-kvm.qcow2,bus=virtio,size=80,sparse=false  
--disk path=fgw-kvm-cache.qcow2,bus=virtio,size=1024,sparse=false --network  
default,model=virtio --graphics none --import
```

#### Note

For VMware, Microsoft Hyper-V, and KVM, synchronizing the VM time with the host time is required for successful gateway activation. Make sure that your host clock is set to the correct time and synchronize it with a Network Time Protocol (NTP) server.

For information about deploying your gateway to an Amazon EC2 host, see [Deploying a file gateway on an Amazon EC2 host \(p. 401\)](#).

## Choosing a service endpoint

You can activate your gateway using:

- A public service endpoint and have your gateway communicate with AWS storage services over the public internet.

- A Federal Information Processing Standards (FIPS) compliant public service endpoint and have your gateway communicate with AWS storage services over the public internet.
- A public service endpoint and have your gateway communicate with AWS storage services using a virtual private cloud (VPC) endpoint, which is private.

**Note**

If you use a VPC endpoint, all VPC endpoint communication from your gateway to AWS services occurs through the public service endpoint using your VPC in AWS.

**To choose a service endpoint**

1. For **Select service endpoint**, choose one of the following:
  - To have your gateway access AWS services over the public internet using a public service endpoint, choose **Public**.
  - To have your gateway access AWS services over the public internet using a public service endpoint that complies with FIPS, choose **FIPS**.

If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

  - To have your gateway access AWS services over a private VPC endpoint connection using a public service endpoint, choose **VPC**.

**Note**

The FIPS service endpoint is only available in some AWS Regions. For more information, see [Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.

This procedure assumes that you are activating your gateway with a public endpoint. For information about how to activate a gateway using a VPC endpoint, see [Activating a gateway in a virtual private cloud \(p. 153\)](#).

2. Choose **Next** to connect and activate your gateway.

## Connecting to the gateway

To connect to your gateway, first get the IP address or activation key of your gateway VM. You use the IP address or activation key to activate your gateway. For gateways deployed and activated on an on-premises host, you can get the IP address or activation key from your gateway VM local console or your hypervisor client. For gateways deployed and activated on an Amazon EC2 instance, you can get the IP address or activation key from the Amazon EC2 console.

The activation process associates your gateway with your AWS account. Your gateway VM must be running for activation to succeed.

**Note**

Make sure that you select the correct gateway type. The .ova files and Amazon Machine Images (AMIs) for the gateway types are different and are not interchangeable.

**To get the IP address or activation key for your gateway VM from the local console**

1. Log on to your gateway VM local console. For detailed instructions, see the following:
  - VMware ESXi – [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).

2. Get the IP address from the top of the menu page, and note it for later use.

### To get the IP address or activation key from an EC2 instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then choose the EC2 instance.
3. Choose the **Details** tab at the bottom, and then note the IP address or activation key. You use one of these to activate the gateway.

#### Note

For activation with an IP address, you can use the public or private IP address assigned to a gateway. You must be able to reach the IP address that you use from the browser from which you perform the activation.

### To associate your gateway with your AWS account

1. For **Connect to gateway**, choose one of the following:
  - **IP address**
  - **Activation key**
2. Enter the IP address or activation key of your gateway, and then choose **Next**.

For detailed information about how to get a gateway IP address, see [Connecting to Your Gateway \(p. 440\)](#).

## Activating the gateway

The following, shown on the activation page, are the gateway settings that you selected. The activation page appears after you associate your gateway with your Amazon Web Services account, as described preceding.

- **Gateway type** specifies the type of gateway that you are activating.
- **Endpoint type** specifies the type of endpoint that you selected for your gateway.
- **AWS Region** specifies the AWS Region where your gateway will be activated and where your data will be stored. If **Endpoint type** is **VPC**, the AWS Region should be same as the Region where your VPC endpoint is located.

### To activate your gateway

1. In **Activate gateway**, do the following:
  - For **Gateway time zone**, select a time zone to use for your gateway.
  - For **Gateway name**, enter a name to identify your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.

#### Note

The gateway name must be between 2 and 255 characters in length.

2. (Optional) For **Add tags**, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

If activation isn't successful, see [Troubleshooting your gateway \(p. 360\)](#) for possible solutions.

## Configuring local disks

When you deployed the VM, you allocated local disks for your gateway. Now you configure your gateway to use these disks. For information about using ephemeral storage, see [Using ephemeral storage with EC2 gateways \(p. 257\)](#).

### To configure local disks

1. For **Configure local disks**, identify the disks that you added and decide which ones to allocate for cached storage. For information about disk size limits, see [Recommended local disk sizes for your gateway \(p. 445\)](#).
2. For **Allocated to**, choose **Cache** for the disk that you want to configure as cache storage.  
If you don't see your disks, choose **Refresh**.
3. Choose **Save and continue** to save your configuration settings.

## Configuring Amazon CloudWatch logging

To notify you about the health of your file gateway and its resources, you can configure an Amazon CloudWatch log group. For more information, see [Getting file gateway health logs with CloudWatch Log Groups \(p. 225\)](#).

### To configure a CloudWatch log group for your file gateway

1. For **Configure logging - optional**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.
  - **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.  
Choose a log group from the **Existing log group list**.
2. Choose **Save and continue** to save your configuration settings.

## Verifying VMware High Availability (VMware HA clusters only)

If your gateway is not deployed on a VMware host that is enabled for VMware High Availability (HA), you can skip this section.

If your gateway is deployed on a VMware host that is enabled for VMware High Availability (HA) cluster, you can either test the configuration when activating the gateway or after your gateway is activated. The following instructions show you how to test the configuration during activation.

### To test for VMware HA

1. For **Verify VMware High Availability configuration**, choose **Next**. Verification can take up to two minutes to complete.  
If the test is successful, a message that indicates a successful test is displayed in the banner. If the test fails, a failed message is displayed. You can make changes in your vSphere configuration and repeat the test.
2. To repeat the test, on the **Gateways** dashboard, choose your gateway, and then for **Actions**, choose **Verify VMware High Availability**.

For information about how to configure your gateway for VMware HA, see [Using VMware vSphere High Availability with Storage Gateway \(p. 329\)](#).

## Next Step

[Creating a file share \(p. 46\)](#)

# Creating a file share

### Note

The documentation for the file gateway that supports a file interface into Amazon Simple Storage Service has moved to [What is Amazon S3 File Gateway?](#).

When a file is written to the file gateway by an NFS or SMB client, the file gateway uploads the file's data to Amazon S3 followed by its metadata, (ownerships, timestamps, etc.). Uploading the file data creates an S3 object, and uploading the metadata for the file updates the metadata for the S3 object. This process creates another version of the object, resulting in two versions of an object. If S3 Versioning is enabled, both versions will be stored.

In this section, you can find instructions about how to create a file share. You can create a file share that can be accessed using either the Network File System (NFS) or Server Message Block (SMB) protocol.

### Note

When a file is written to the file gateway by an NFS or SMB client, the file gateway uploads the file's data to Amazon S3 followed by its metadata, (ownerships, timestamps, etc.). Uploading the file data creates an S3 object, and uploading the metadata for the file updates the metadata for the S3 object. This process creates another version of the object, resulting in two versions of an object. If S3 Versioning is enabled, both versions will be stored.

If you change the metadata of a file stored in file gateway, a new S3 object will be created and will replace the existing S3 object. This behavior is different from editing a file in a file system where editing a file will not result in a new file being created. You should test all file operations you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

The use of S3 Versioning and Cross-Region replication (CRR) in Amazon S3 should be carefully considered when data is being uploaded from file gateway. Uploading files from file gateway to Amazon S3 when S3 Versioning is enabled results in at least two versions of an S3 object.

Certain workflows involving large files and file writing patterns such as file uploads that are performed in several steps can increase the number of stored S3 object versions. If the file gateway cache needs to free up space due to high file write rates that may result in multiple S3 object versions being created. These scenarios increase S3 storage if S3 Versioning is enabled and increases transfer costs associated with CRR. You should test all file operations you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

Using the Rsync utility with file gateway results in the creation of temporary files in the cache and creation of temporary S3 objects in Amazon S3. This will result in early deletion charges in the S3 Standard-Infrequent Access (S3 Standard-IA), and S3 Intelligent-Tiering storage classes.

When you create an NFS share, by default anyone who has access to the NFS server can access the NFS file share. You can limit access to clients by IP address.

For SMB, you can have one of three different modes of authentication:

- A file share with Microsoft Active Directory (AD) access. Any authenticated Microsoft AD user gets access to this file share type.
- An SMB file share with limited access. Only certain domain users and groups that you specify are allowed access (allow list). Users and groups can also be denied access (deny list).
- An SMB file share with guest access. Any users who can provide the guest password get access to this file share.

### Note

File shares exported through the gateway for NFS file shares support POSIX permissions. For SMB file shares, you can use access control lists (ACLs) to manage permissions on files and

folders in your file share. For more information, see [Using Microsoft Windows ACLs to Control Access to an SMB File Share \(p. 347\)](#).

A file gateway can host one or more file shares of different types. You can have multiple NFS and SMB file shares on a file gateway.

**Important**

To create a file share, a file gateway requires you to activate AWS Security Token Service (AWS STS). Make sure that AWS STS is activated in the AWS Region that you are creating your file gateway in. If AWS STS is not activated in that AWS Region, activate it. For information about how to activate AWS STS, see [Activating and deactivating AWS STS in an AWS Region](#) in the *AWS Identity and Access Management User Guide*.

**Note**

You can use AWS Key Management Service (AWS KMS) to encrypt objects that your file gateway stores in Amazon S3. To do this using the Storage Gateway console, see [Create an NFS file share \(p. 47\)](#) or [Creating an SMB file share \(p. 58\)](#). You can also do this by using the Storage Gateway API. For instructions, see the [CreateNFSFileShare](#) or [CreateSMBFileShare](#) in the Storage Gateway API Reference.

By default, a file gateway uses server-side encryption managed with Amazon S3 (SSE-S3) when it writes data to an S3 bucket. If you make SSE-KMS (server-side encryption with AWS KMS-managed keys) the default encryption for your S3 bucket, objects that a file gateway stores there are encrypted using SSE-KMS.

To encrypt using SSE-KMS with your own AWS KMS key, you must enable SSE-KMS encryption. When you do so, provide the Amazon Resource Name (ARN) of the KMS key when you create your file share. You can also update KMS settings for your file share by using the [UpdateNFSFileShare](#) or [UpdateSMBFileShare](#) API operation. This update applies to objects stored in the Amazon S3 buckets after the update.

**Topics**

- [Create an NFS file share \(p. 47\)](#)
- [Create an SMB file share \(p. 51\)](#)

## Create an NFS file share

Use the following procedure to create an NFS file share.

**Note**

When a file is written to the file gateway by an NFS client, the file gateway uploads the file's data to Amazon S3 followed by its metadata (ownerships, timestamps, etc.). Uploading the file data creates an S3 object, and uploading the metadata for the file updates the metadata for the S3 object. This process creates another version of the object, resulting in two versions of an object. If S3 Versioning is enabled, both versions will be stored.

If you change the metadata of a file stored in your file gateway, a new S3 object is created and replaces the existing S3 object. This behavior is different from editing a file in a file system, where editing a file does not result in a new file being created. You should test all file operations that you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

The use of S3 Versioning and Cross-Region replication (CRR) in Amazon S3 should be carefully considered when data is being uploaded from your file gateway. Uploading files from your file gateway to Amazon S3 when S3 Versioning is enabled results in at least two versions of an S3 object.

Certain workflows involving large files and file-writing patterns such as file uploads that are performed in several steps can increase the number of stored S3 object versions. If the file gateway cache needs to free up space due to high file-write rates, multiple S3 object versions might be created. These scenarios increase S3 storage if S3 Versioning is enabled and increase

transfer costs associated with CRR. You should test all file operations that you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

Using the Rsync utility with your file gateway results in the creation of temporary files in the cache and the creation of temporary S3 objects in Amazon S3. This situation results in early deletion charges in the S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Intelligent-Tiering storage classes.

### To create an NFS file share

1. Open the AWS Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home/>.
2. Choose **Create file share** to open the **File share settings** page.
3. For **Gateway**, choose your Amazon S3 File Gateway from the list.
4. For **Amazon S3 location**, do one of the following:
  - To connect the file share directly to an S3 bucket, choose **S3 bucket name**, then enter the S3 bucket name and, optionally, a prefix name for objects created by the file share. Your gateway uses this bucket to store and retrieve files. For information about creating a new bucket, see [How do I create an S3 bucket?](#) in the *Amazon Simple Storage Service Console User Guide*. For information about using prefix names, see [Organizing objects using prefixes](#) in the *Amazon Simple Storage Service Console User Guide*.
  - To connect the file share to an S3 bucket through an access point, choose **S3 access point**, then enter the S3 access point name and, optionally, a prefix name for objects created by the file share. Your bucket policy must be configured to delegate access control to the access point. For information about access points, see [Managing data access with Amazon S3 access points](#) and [Delegating access control to access points](#) in the *Amazon Simple Storage Service User Guide*. For information about using prefix names, see [Organizing objects using prefixes](#) in the *Amazon Simple Storage Service Console User Guide*.

#### Note

- If you enter a prefix name or choose to connect through an access point, you must enter a file share name.
  - The prefix name must end with a forward slash (/).
  - After the file share is created, the prefix name can't be modified or deleted.
5. For **AWS Region**, choose the AWS Region of the S3 bucket.
  6. For **File share name**, enter a name for the file share. The default name is the S3 bucket name or access point name.

#### Note

- If you entered a prefix name, you must enter a file share name.
  - After the file share is created, the file share name can't be deleted.
7. (Optional) For **AWS PrivateLink for S3**, do the following:
    1. To configure the file share to connect to S3 through an interface endpoint in your VPC powered by AWS PrivateLink, select **Use VPC endpoint**.
    2. Choose either **VPC endpoint ID** or **VPC endpoint DNS name** to identify the VPC interface endpoint that you want the file share to connect through, and then provide the required information in the corresponding field.

**Note**

- This step is required if the file share connects to S3 through a VPC access point.
  - File share connections using AWS PrivateLink are not supported on FIPS gateways.
  - For information about AWS PrivateLink, see [AWS PrivateLink for Amazon S3](#) in the *Amazon Simple Storage Service User Guide*.
8. For **Access objects using**, choose **Network File System (NFS)**.
  9. For **Audit logs**, choose one of the following:
    - Choose **Disable logging** to turn off logging.
    - Choose **Create a new log group** to create a new audit log.
    - Choose **Use an existing log group**, and then choose an existing audit log from the list.

For more information about audit logs, see [Understanding file gateway audit logs \(p. 234\)](#).

10. For **Automated cache refresh from S3**, choose **Set refresh interval**, and set the time in days, hours, and minutes to refresh the file share's cache using Time To Live (TTL). TTL is the length of time since the last refresh. After the TTL interval has elapsed, accessing the directory causes the file gateway to first refresh that directory's contents from the Amazon S3 bucket.
11. For **File upload notification**, choose **Settling time (seconds)** to be notified when a file has been fully uploaded to S3 by the file gateway. Set the **Settling Time** in seconds to control the number of seconds to wait after the last point in time that a client wrote to a file before generating an **ObjectUploaded** notification. Because clients can make many small writes to files, it's best to set this parameter for as long as possible to avoid generating multiple notifications for the same file in a small time period. For more information, see [Getting file upload notification \(p. 228\)](#).

**Note**

This setting has no effect on the timing of the object uploading to S3, only on the timing of the notification.

12. (Optional) In the **Add tags** section, enter a key and value to add tags to your file share. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your file share.
13. Choose **Next**. The **Configure how files are stored in Amazon S3** page appears.
14. For **Storage class for new objects**, choose a storage class to use for new objects created in your Amazon S3 bucket:
  - Choose **S3 Standard** to store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard storage class, see [Storage classes for frequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Intelligent-Tiering** to optimize storage costs by automatically moving data to the most cost-effective storage access tier. For more information about the S3 Intelligent-Tiering storage class, see [Storage class for automatically optimizing frequently and infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Standard-IA** to store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 One Zone-IA** to store your infrequently accessed object data in a single Availability Zone. For more information about the S3 One Zone-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.

To help monitor your S3 billing, use AWS Trusted Advisor. For more information, see [Monitoring tools](#) in the *Amazon Simple Storage Service User Guide*.

15. For **Object metadata**, choose the metadata that you want to use:
  - Choose **Guess MIME type** to enable guessing of the MIME type for uploaded objects based on file extensions.
  - Choose **Give bucket owner full control** to give full control to the owner of the S3 bucket that maps to the NFS file share. For more information about using your file share to access objects in a bucket owned by another account, see [Using a file share for cross-account access \(p. 164\)](#).
  - Choose **Enable requester pays** if you are using this file share on a bucket that requires the requester or reader instead of the bucket owner to pay for access charges. For more information, see [Requester pays buckets](#).
16. For **Access to your S3 bucket**, choose the AWS Identity and Access Management (IAM) role that you want your file gateway to use to access your Amazon S3 bucket:
  - Choose **Create a new IAM role** to enable the file gateway to create a new IAM role and access the policy on your behalf.
  - Choose **Use an existing IAM role** to choose an existing IAM role and to set up the access policy manually. In the **IAM role** box, enter the Amazon Resource Name (ARN) for the role used to access your bucket. For information about IAM roles, see [IAM roles](#) in the *AWS Identity and Access Management User Guide*.

For more information about access to your S3 bucket, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).

17. For **Encryption**, choose the type of encryption keys to use to encrypt objects that your file gateway stores in Amazon S3:
  - Choose **S3-Managed Keys (SSE-S3)** to use server-side encryption managed with Amazon S3 (SSE-S3).
  - Choose **KMS-Managed Keys (SSE-KMS)** to use server-side encryption managed with AWS Key Management Service (SSE-KMS). In the **Master key** box, choose an existing master KMS key or choose **Create a new KMS key** to create a new KMS key in the AWS Key Management Service (AWS KMS) console. For more information about AWS KMS, see [What is AWS Key Management Service?](#) in the *AWS Key Management Service Developer Guide*.

**Note**

To specify an AWS KMS key with an alias that is not listed or to use an AWS KMS key from a different AWS account, you must use the AWS Command Line Interface (AWS CLI). For more information, see [CreateNFSFileShare](#) in the *AWS Storage Gateway API Reference*. Asymmetric customer master keys (CMKs) are not supported.

18. Choose **Next** to configure file access settings.

### To configure file access settings

1. For **Allowed clients**, specify whether to allow or restrict each client's access to your file share. Provide the IP address or CIDR notation for the clients that you want to allow. For information about supported NFS clients, see [Supported NFS clients for a file gateway \(p. 22\)](#).
2. For **Mount options**, specify the options that you want for **Squash level** and **Export as**.

For **Squash level**, choose one of the following:

- **All squash:** All user access is mapped to User ID (UID) (65534) and Group ID (GID) (65534).
- **No root squash:** The remote superuser (root) receives access as root.

- **Root squash (default):** Access for the remote superuser (root) is mapped to UID (65534) and GID (65534).

For **Export as**, choose one of the following:

- **Read-write**
- **Read-only**

**Note**

For file shares that are mounted on a Microsoft Windows client, if you choose **Read-only**, you might see a message about an unexpected error keeping you from creating the folder. You can ignore this message.

3. For **File metadata defaults**, you can edit the **Directory permissions**, **File permissions**, **User ID**, and **Group ID**. For more information, see [Editing metadata defaults for your NFS file share \(p. 167\)](#).
4. Choose **Next**.
5. Review your file share configuration settings, and then choose **Finish**.

After your NFS file share is created, you can see your file share settings in the file share's **Details** tab.

### Next Step

[Mounting your NFS file share on your client \(p. 62\)](#)

## Create an SMB file share

Before you create an SMB file share, make sure that you configure SMB security settings for your file gateway. You also must configure either Microsoft Active Directory (AD) or guest access for authentication. A file share provides one type of SMB access only.

**Note**

An SMB file share doesn't operate correctly unless the required ports are open in your security group. For more information, see [Port Requirements \(p. 437\)](#).

**Note**

When a file is written to the file gateway by an SMB client, the file gateway uploads the file's data to Amazon S3 followed by its metadata (ownerships, timestamps, etc.). Uploading the file data creates an S3 object, and uploading the metadata for the file updates the metadata for the S3 object. This process creates another version of the object, resulting in two versions of an object. If S3 Versioning is enabled, both versions will be stored.

If you change the metadata of a file stored in your file gateway, a new S3 object is created and replaces the existing S3 object. This behavior is different from editing a file in a file system, where editing a file does not result in a new file being created. You should test all file operations that you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

The use of S3 Versioning and Cross-Region replication (CRR) in Amazon S3 should be carefully considered when data is being uploaded from your file gateway. Uploading files from your file gateway to Amazon S3 when S3 Versioning is enabled results in at least two versions of a S3 object.

Certain workflows involving large files and file-writing patterns such as file uploads that are performed in several steps can increase the number of stored S3 object versions. If the file gateway cache needs to free up space due to high file-write rates, multiple S3 object versions might be created. These scenarios increase S3 storage if S3 Versioning is enabled and increase transfer costs associated with CRR. You should test all file operations that you plan to use with Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.

Using the Rsync utility with your file gateway results in the creation of temporary files in the cache and the creation of temporary S3 objects in Amazon S3. This situation results in early deletion charges in the S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Intelligent-Tiering storage classes.

## Create SMB settings

### To create an SMB file share

1. Open the AWS Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home/>.
2. Choose **Create file share** to open the **File share settings** page.
3. For **Gateway**, choose your Amazon S3 File Gateway from the list.
4. For **Amazon S3 location**, do one of the following:
  - To connect the file share directly to an S3 bucket, choose **S3 bucket name**, then enter the bucket name and, optionally, a prefix name for objects created by the file share. Your gateway uses this bucket to store and retrieve files. For information about creating a new bucket, see [How do I create an S3 bucket?](#) in the *Amazon Simple Storage Service Console User Guide*. For information about using prefix names, see [Organizing objects using prefixes](#) in the *Amazon Simple Storage Service Console User Guide*.
  - To connect the file share to an S3 bucket through an access point, choose **S3 access point**, then enter the S3 access point name and, optionally, a prefix name for objects created by the file share. Your bucket policy must be configured to delegate access control to the access point. For information about access points, see [Managing data access with Amazon S3 access points](#) and [Delegating access control to access points](#) in the *Amazon Simple Storage Service User Guide*. For information about using prefix names, see [Organizing objects using prefixes](#) in the *Amazon Simple Storage Service Console User Guide*.

#### Note

- If you enter a prefix name or choose to connect through an access point, you must enter a file share name.
- The prefix name must end with a forward slash (/).
- After the file share is created, the prefix name can't be modified or deleted.

5. For **AWS Region**, choose the AWS Region of the S3 bucket.
6. For **File share name**, enter a name for the file share. The default name is the S3 bucket name or access point name.

#### Note

- If you entered a prefix name, you must enter a file share name.
- After the file share is created, the file share name can't be deleted.

7. (Optional) For **AWS PrivateLink for S3**, do the following:
  1. To configure the file share to connect to S3 through an interface endpoint in your VPC powered by AWS PrivateLink, select **Use VPC endpoint**.
  2. Choose either **VPC endpoint ID** or **VPC endpoint DNS name** to identify the VPC interface endpoint that you want the file share to connect through, and then provide the required information in the corresponding field.

#### Note

- This step is required if the file share connects to S3 through a VPC access point.

- File share connections using AWS PrivateLink are not supported on FIPS gateways.
  - For information about AWS PrivateLink, see [AWS PrivateLink for Amazon S3](#) in the *Amazon Simple Storage Service User Guide*.
8. For **Access objects using**, choose **Server Message Block (SMB)**.
  9. For **Audit logs**, choose one of the following:
    - Choose **Disable logging** to turn off logging.
    - Choose **Create a new log group** to create a new audit log.
    - Choose **Use an existing log group**, and then choose an existing audit log from the list.
- For more information about audit logs, see [Understanding file gateway audit logs \(p. 234\)](#).
10. For **Automated cache refresh from S3**, choose **Set refresh interval**, and then set the time in days, hours, and minutes to refresh the file share's cache using Time To Live (TTL). TTL is the length of time since the last refresh. After the TTL interval has elapsed, accessing the directory causes the file gateway to first refresh that directory's contents from the Amazon S3 bucket.
  11. For **File upload notification**, choose **Settling time (seconds)** to be notified when a file has been fully uploaded to S3 by the file gateway. Set the **Settling Time** in seconds to control the number of seconds to wait after the last point in time that a client wrote to a file before generating an **ObjectUploaded** notification. Because clients can make many small writes to files, it's best to set this parameter for as long as possible to avoid generating multiple notifications for the same file in a small time period. For more information, see [Getting file upload notification \(p. 228\)](#).
- Note**  
This setting has no effect on the timing of the object uploading to S3, only on the timing of the notification.
12. (Optional) In the **Tags** section, choose **Add new tag**, and then enter a key and value to add tags to your file share. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your file share.
  13. Choose **Next**. The **Amazon S3 storage settings** page appears.
  14. For **Storage class for new objects**, choose a storage class to use for new objects created in your Amazon S3 bucket:
    - Choose **S3 Standard** to store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard storage class, see [Storage classes for frequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 Intelligent-Tiering** to optimize storage costs by automatically moving data to the most cost-effective storage access tier. For more information about the S3 Intelligent-Tiering storage class, see [Storage class for automatically optimizing frequently and infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 Standard-IA** to store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 One Zone-IA** to store your infrequently accessed object data in a single Availability Zone. For more information about the S3 One Zone-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.

To help monitor your S3 billing, use AWS Trusted Advisor. For more information, see [Monitoring tools](#) in the *Amazon Simple Storage Service User Guide*.

15. For **Object metadata**, choose the metadata that you want to use:

- Choose **Guess MIME type** to enable guessing of the MIME type for uploaded objects based on file extensions.
  - Choose **Give bucket owner full control** to give full control to the owner of the S3 bucket that maps to the NFS file share. For more information about using your file share to access objects in a bucket owned by another account, see [Using a file share for cross-account access \(p. 164\)](#).
  - Choose **Enable requester pays** if you are using this file share on a bucket that requires the requester or reader instead of the bucket owner to pay for access charges. For more information, see [Requester pays buckets](#).
16. For **Access to your S3 bucket**, choose the AWS Identity and Access Management (IAM) role that you want your file gateway to use to access your Amazon S3 bucket:
- Choose **Create a new IAM role** to enable the file gateway to create a new IAM role and access the policy on your behalf.
  - Choose **Use an existing IAM role** to choose an existing IAM role and to set up the access policy manually. In the **IAM role** box, enter the Amazon Resource Name (ARN) for the role used to access your bucket. For information about IAM roles, see [IAM roles in the AWS Identity and Access Management User Guide](#).

For more information about access to your S3 bucket, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).

17. For **Encryption**, choose the type of encryption keys to use to encrypt objects that your file gateway stores in Amazon S3:
- Choose **S3-Managed Keys (SSE-S3)** to use server-side encryption managed with Amazon S3 (SSE-S3).
  - Choose **KMS-Managed Keys (SSE-KMS)** to use server-side encryption managed with AWS Key Management Service (SSE-KMS). In the **Master key** box, choose an existing master KMS key or choose **Create a new KMS key** to create a new KMS key in the AWS Key Management Service (AWS KMS) console. For more information about AWS KMS, see [What is AWS Key Management Service?](#) in the [AWS Key Management Service Developer Guide](#).

**Note**

To specify an AWS KMS key with an alias that is not listed or to use an AWS KMS key from a different AWS account, you must use the AWS Command Line Interface (AWS CLI). For more information, see [CreateNFSFileShare](#) in the [AWS Storage Gateway API Reference](#). Asymmetric customer master keys (CMKs) are not supported.

18. Choose **Next**. The **File access settings** page appears.
19. For **Authentication method**, choose the authentication method that you want to use.
- Choose **Active Directory** to use your corporate Microsoft AD for user authenticated access to your SMB file share. Your file gateway must be joined to a domain.
  - Choose **Guest access** to provide only guest access; your file gateway doesn't have to be part of a Microsoft AD domain. You can also use a file gateway that is a member of an AD domain to create file shares with guest access. You must set a guest password for your SMB server in the corresponding field.

**Note**

Both access types are available at the same time.

20. In the **SMB share settings** section, choose your settings.

For **Export as**, choose one of the following:

- **Read-write** (the default value)

- **Read-only**

**Note**

For file shares that are mounted on a Microsoft Windows client, if you choose **Read-only**, you might see a message about an unexpected error preventing you from creating the folder. You can ignore this message.

For **File/directory access controlled by**, choose one of the following:

- Choose **Windows Access Control List** to set fine-grained permissions on files and folders in your SMB file share. For more information, see [Using Microsoft Windows ACLs to Control Access to an SMB File Share \(p. 347\)](#).
- Choose **POSIX permissions** to use POSIX permissions to control access to files and directories that are stored through an NFS or SMB file share.

If your authentication method is **Active Directory**, for **Admin users/groups**, enter a comma-separated list of AD users and groups. Do this if you want the admin user to have privileges to update access control lists (ACLs) on all files and folders in the file share. These users and groups then have administrator rights to the file share. A group must be prefixed with the @ character, for example, @group1.

For **Case sensitivity**, choose **Client specified** to allow the gateway to control the case sensitivity, or choose **Force case sensitivity** to allow the client to control the case sensitivity.

**Note**

- If selected, this setting applies will configure the gateway to always process client requests in a case-sensitive manner. You should select this option if Windows clients will be used to access the share and you plan to have files of mixed case in the same directory. Note: The version of Windows and the application accessing the files may impact how a Windows client handles case sensitivity.

For **Access based enumeration**, choose **Disabled** for files and directories to make the files and folders on the share visible only to users who have read access, or choose **Enabled for files and directories** to make the files and folders on the share visible to all users during directory enumeration.

**Note**

Access-based enumeration is a system that filters the enumeration of files and folders on an SMB file share based on the share's access control lists (ACLs).

For **Opportunistic lock (oplock)**, choose one of the following:

- Choose **Enabled** to allow the file share to use opportunistic locking to optimize the file buffering strategy, which improves performance in most cases, particularly with regard to Windows context menus.
- Choose **Disabled** to prevent the use of opportunistic locking. If multiple Windows clients in your environment frequently edit the same files simultaneously, disabling opportunistic locking can sometimes improve performance.

**Note**

Enabling opportunistic locking on case-sensitive shares is not recommended for workloads that involve access to files with the same name in different case.

21. (Optional) In the **User and group file share access** section, choose your settings.

For **Allowed users and groups**, choose **Add allowed user** or **Add allowed group** and enter an AD user or group that you want to allow file share access. Repeat this process to allow as many users and groups as necessary.

For **Denied users and groups**, choose **Add denied user** or **Add denied group** and enter an AD user or group that you want to deny file share access. Repeat this process to deny as many users and groups as necessary.

**Note**

The **User and group file share access** section appears only if **Active Directory** is selected. Enter only the AD user or group name. The domain name is implied by the membership of the gateway in the specific AD that the gateway is joined to.

If you don't specify valid or invalid users or groups, any authenticated AD user can export the file share.

22. Choose **Next**.

23. Review your file share configuration settings, and then choose **Finish**.

After your SMB file share is created, you can see your file share settings in the file share's **Details** tab.

- [Configuring SMB security settings \(p. 56\)](#)
- [Configuring Microsoft Active Directory access \(p. 57\)](#)
- [Configuring guest access \(p. 57\)](#)
- [Creating an SMB file share \(p. 58\)](#)

## Configuring SMB security settings

Use the following procedure to configure your file gateway SMB security settings.

### To configure SMB security settings

1. Choose the pencil icon in the upper right corner of the **SMB security settings** section.
2. For **Security level**, choose one of the following:

**Note**

This setting is called **SMBSecurityStrategy** in the API Reference.  
A higher security level can affect performance.

- **Enforce encryption** – if you choose this option, file gateway only allows connections from SMBv3 clients that have encryption enabled. This option is highly recommended for environments that handle sensitive data. This option works with SMB clients on Microsoft Windows 8, Windows Server 2012, or newer.
- **Enforce signing** – if you choose this option, file gateway only allows connections from SMBv2 or SMBv3 clients that have signing enabled. This option works with SMB clients on Microsoft Windows Vista, Windows Server 2008, or newer.
- **Client negotiated** – if you choose this option, requests are established based on what is negotiated by the client. This option is recommended when you want to maximize compatibility across different clients in your environment.

**Note**

For gateways activated before June 20, 2019, the default security level is **Client negotiated**.  
For gateways activated on June 20, 2019 and later, the default security level is **Enforce encryption**.

3. Choose **Close** if you are done.

## Configuring Microsoft Active Directory access

Use the following procedure to configure your file gateway Microsoft AD access settings.

### To configure your SMB file share Microsoft AD access settings

1. Choose the pencil icon in the upper right corner of the **Active Directory settings** section.
2. For **Domain name**, provide the domain that you want the gateway to join. You can join a domain by using its IP address or its organizational unit. An *organizational unit* is an Active Directory subdivision that can hold users, groups, computers, and other organizational units.

#### Note

You can use the [AWS Directory Service](#) to create a hosted Microsoft AD domain service in the Amazon Web Services Cloud.

If your gateway can't join a Microsoft AD directory, try joining with the directory's IP address by using the [JoinDomain](#) API operation.

**Active Directory status** shows **Detached** when a gateway has never joined a domain.

3. For **Domain user**, enter your account name. Your account must be able to join a server to a domain.
4. For **Domain password**, enter your account password.
5. (Optional) For **Organizational unit**, enter your organizational unit.
6. (Optional) For **Domain controller(s)**, enter a comma-separated list of Internet Protocol version 4 (IPv4) addresses, NetBIOS names, or hostnames of your domain server.
7. Choose **Save** to save your changes.
8. Choose **Close** if you are done.

## Configuring guest access

Use the following procedure to configure your file gateway guest access settings.

### To configure your SMB file share for guest access

1. Choose the pencil icon in the upper right corner of the **Guest access settings** section.
2. For **Guest password**, enter a password that meets your organization's security requirements.
3. Choose **Save** to complete the authentication.

#### Note

If you provide only guest access, your file gateway doesn't have to be part of an AD domain. You can also use a file gateway that is a member of your Microsoft AD domain to create file shares with guest access.

4. Choose **Close** if you are done.

A message at the top of the **Gateways** section of your console should appear, saying that your gateway Successfully joined domain.

If the banner displays the message **Invalid domain name/DNS name cannot be resolved**, the correct endpoint wasn't found. You might also see the error **Invalid users/Invalid password**, an authentication failure that means that your logon was not recognized by the domain service.

The error message **The gateway cannot connect to the specified domain** can indicate that the quota of users has been exhausted, in other words there are no more users in the quota. The default limit allows each user to join up to 10 systems to a domain. This error can also appear if the user that tried to connect didn't have administrator privileges.

The error message **The specified request timed out** might indicate that there is a problem with your firewall rules not allowing access to the domain.

## Creating an SMB file share

In this procedure, you create an SMB file share with either Microsoft AD or guest access. Make sure that you define the SMB file share settings for your file gateway before performing the following steps. To configure the SMB file share settings, see [Create SMB settings \(p. 52\)](#).

### To create an SMB file share

1. Open the AWS Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home/>.
2. Choose **Create file share**.
3. On the **Configure file share settings** page, for **Amazon S3 bucket name / Prefix name**, do one or more of the following:
  - In *Existing S3 bucket name*, enter the name for an existing Amazon S3 bucket. You use this bucket for your gateway to store files in and retrieve. For information on creating a new bucket, see [How do I create an S3 bucket?](#) in the *Amazon Simple Storage Service Console User Guide*.
  - (Optional) In *S3 prefix name*, enter a prefix name for the S3 bucket.

#### Note

- The prefix name must end with a "/".
- If you enter a prefix name, you must enter a file share name.
- Once the file share is created, the prefix name can't be modified or deleted.

4. (Optional) For **File share name**, enter a name for the file share. The default name is the S3 bucket name.

#### Note

- If you enter a prefix name, you must enter a file share name.
- Once the file share is created, the file share name can't be deleted.

5. For **Access objects using**, choose **Server Message Block (SMB)**.

6. For **Gateway**, make sure that your gateway is chosen.

7. For **Audit logs**, choose one of the following:

- **Disable logging**
- **Create a new log group** to create a new audit log.
- **Use an existing log group** and choose an existing audit log from the list.

For more information about audit logs, see [Understanding file gateway audit logs \(p. 234\)](#).

8. (Optional) For **Automated cache refresh from S3 after**, select the check box and set the time in days, hours, and minutes to refresh the file share's cache using Time To Live (TTL). TTL is the length of time since the last refresh after which access to the directory would cause the file gateway to first refresh that directory's contents from the Amazon S3 bucket.
9. (Optional) For **File upload notification**, choose the check box to be notified when a file has been fully uploaded to S3 by the file gateway. Set the **Settling Time** in seconds to control the number of seconds to wait after the last point in time a client wrote to a file before generating an **ObjectUploaded** notification. Because clients can make many small writes to files, it's best to set this parameter for as long as possible to avoid generating multiple notifications for the same file in a small time period. For more information, see [Getting file upload notification \(p. 228\)](#).

#### Note

This setting has no effect on the timing of the object uploading to S3, only the timing of the notification.

10. (Optional) In the **Add tags** section, enter a key and value to add tags to your file share. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your file share.

11. Choose **Next**. The **Configure how files are stored in Amazon S3** page appears.
12. For **Storage class for new objects**, choose a storage class to use for new objects created in your Amazon S3 bucket:
  - Choose **S3 Standard** to store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard storage class, see [Storage classes for frequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Intelligent-Tiering** to optimize storage costs by automatically moving data to the most cost-effective storage access tier. For more information about the S3 Intelligent-Tiering storage class, see [Storage class for automatically optimizing frequently and infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Standard-IA** to store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 One Zone-IA** to store your infrequently accessed object data in a single Availability Zone. For more information about the S3 One Zone-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
13. For **Object metadata**, choose the metadata you want to use:
  - Choose **Guess MIME type** to enable guessing of the MIME type for uploaded objects based on file extensions.
  - Choose **Give bucket owner full control** to give full control to the owner of the S3 bucket that maps to the file SMB file share. For more information on using your file share to access objects in a bucket owned by another account, see [Using a file share for cross-account access \(p. 164\)](#).
  - Choose **Enable requester pays** if you are using this file share on a bucket that requires the requester or reader instead of bucket owner to pay for access charges. For more information, see [Requester Pays Buckets](#).
14. For **Access to your S3 bucket**, choose the AWS Identity and Access Management (IAM) role that you want your file gateway to use to access your Amazon S3 bucket:
  - **Create a new IAM role** to enable the file gateway to create a new IAM role and access the policy on your behalf.
  - **Use an existing IAM role** to choose an existing IAM role and to set up the access policy manually. In the **IAM role** box, enter the Amazon Resource Name (ARN) for the role used to access your bucket. For information about IAM roles, see [IAM roles](#) in the *AWS Identity and Access Management User Guide*.
- For more information about access to your S3 bucket, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).
15. For **Encryption**, choose the type of encryption keys to use to encrypt objects that your file gateway stores in Amazon S3:
  - Choose **S3-Managed Keys (SSE-S3)** to use server-side encryption managed with Amazon S3 (SSE-S3).
  - Choose **KMS-Managed Keys (SSE-KMS)** to use server-side encryption managed with AWS Key Management Service (SSE-KMS). In the **Master key** box, choose an existing master KMS key or choose **Create a new KMS key** to create a new KMS key in the AWS Key Management Service (AWS KMS) console. For more information about AWS KMS, [What is AWS Key Management Service?](#) in the *AWS Key Management Service Developer Guide*.

**Note**

To specify an AWS KMS key with an alias is not listed or to use an AWS KMS key from a different Amazon Web Services account, you must use the AWS Command Line Interface

(AWS CLI). For more information, see [CreateSMBFileShare](#) in the *AWS Storage Gateway API Reference*.

Asymmetric customer master keys (CMKs) are not supported.

16. Choose **Next** to review configuration settings for your file share. Your file gateway applies default settings to your file share.

### To change the configuration settings for your SMB file share

1. Choose **Edit** for the settings that you want to change. Choose **Close** to enforce your settings.
2. For **SMB share settings**, you can edit the authentication method, export as, file and directory access, and admin user and groups.

For **Select authentication method**, choose one of the following:

- **Active Directory** (the default value) to use your corporate Microsoft AD for user authenticated access to your SMB file share.
- **Guest access** to provide only guest access; your file gateway doesn't have to be part of a Microsoft AD domain. You can also use a file gateway that is a member of an AD domain to create file shares with guest access.

#### Note

For Microsoft AD access, your file gateway must be joined to a domain.

For guest access, you must set a guest access password.

Both access types are available at the same time.

For **Export as**, choose one of the following:

- **Read-write** (the default value)
- **Read-only**

#### Note

For file shares mounted on a Microsoft Windows client, if you choose **Read-only**, you might see a message about an unexpected error keeping you from creating the folder. You can ignore this message.

For **File/directory access controlled by**, choose one of the following:

- Choose **Windows Access Control List** to set fine-grained permissions on files and folders in your SMB file share. For more information, see [Using Microsoft Windows ACLs to Control Access to an SMB File Share \(p. 347\)](#).
- Choose **POSIX permissions** to use POSIX permissions to control access to files and directories that are stored through an NFS or SMB file share.

(Optional) For **Admin users/groups**, enter a comma-separated list of AD users and groups. You do this if you want the admin user to have privileges to update ACLs on all files and folders in the file share. These users and groups then have administrator rights to the file share. A group must be prefixed with the @ character, for example @group1.

(Optional) For **Case sensitivity**, select the check box to allow the gateway to control the case sensitivity, or keep the check box cleared to allow the client to control the case sensitivity.

When Case Sensitivity is not selected (the default), the gateway will process client requests in a case-sensitive or case-insensitive manner as directed by the SMB client. This setting is appropriate for most applications. This will configure the gateway to always process client requests in a case-

sensitive manner. You should select this option if Windows clients will be used to access the share and you plan to have files of mixed case in the same directory. Note: The version of Windows and the application accessing the files may impact how a Windows client handles case sensitivity.

**Note**

- If selecting, this setting applies immediately to new SMB client connections. Existing SMB client connections must disconnect from the file share and reconnect for the setting to take effect.

(Optional) For **Access based enumeration**, select the check box to make the files and folders on the share visible only to users who have read access. Keep the check box cleared to make the files and folders on the share visible to all users during directory enumeration.

**Note**

Access-based enumeration is a system that filters the enumeration of files and folders on an SMB file share based on the share's access control lists (ACLs).

3. (Optional) For **Allowed/denied users and groups**, choose **Add entry** and provide the list of AD users or groups that you want to allow or deny file share access.

**Note**

The **Allowed/denied users and groups** section appears only if **Active Directory** is selected. Enter only the AD user or group name. The domain name is implied by the membership of the gateway in the specific AD that the gateway is joined to.

If you don't specify valid or invalid users or groups, any authenticated AD user can export the file share.

4. For **Tags**, you add new tags or remove existing tags.

5. Review your file share configuration settings, and then choose **Create file share**.

After your SMB file share is created, you can see your file share settings in the file share's **Details** tab.

The preceding procedure creates a Microsoft AD file share. Anyone with domain credentials can access this file share. To limit access to certain users and groups, see [Using Active Directory to authenticate users \(p. 170\)](#).

**Next Step**

[Mounting your SMB file share on your client \(p. 63\)](#)

## Using your file share

**Note**

The documentation for the file gateway that supports a file interface into Amazon Simple Storage Service has moved to [What is Amazon S3 File Gateway?](#).

Following, you can find instructions about how to mount your file share on your client, use your share, test your file gateway, and clean up resources as needed. For more information about supported Network File System (NFS) clients, see [Supported NFS clients for a file gateway \(p. 22\)](#). For more information about supported Service Message Block (SMB) clients, see [Supported SMB clients for a file gateway \(p. 23\)](#).

You can find example commands to mount your file share on the AWS Management Console. In following sections, you can find details on how to mount your file share on your client, use your share, test your file gateway, and clean up resources as needed.

**Topics**

- [Mounting your NFS file share on your client \(p. 62\)](#)
- [Mounting your SMB file share on your client \(p. 63\)](#)

- Working with file shares on a bucket with pre-existing objects (p. 65)
- Testing your file gateway (p. 65)
- Where do I go from here? (p. 66)

## Mounting your NFS file share on your client

Now you mount your NFS file share on a drive on your client and map it to your Amazon S3 bucket.

### To mount a file share and map it to an Amazon S3 bucket

1. If you are using a Microsoft Windows client, we recommend that you [create an SMB file share](#) and access it using an SMB client that is already installed on Windows client. If you use NFS, turn on Services for NFS in Windows.
2. Mount your NFS file share:

- For Linux clients, type the following command at the command prompt.

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

- For MacOS clients, type the following command at the command prompt.

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

- For Windows clients, type the following command at the command prompt.

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

For example, suppose that on a Windows client your VM's IP address is 123.123.1.2 and your Amazon S3 bucket name is test-bucket. Suppose also that you want to map to drive T. In this case, your command looks like the following.

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

#### Note

When mounting file shares, be aware of the following:

- You might have a case where a folder and an object exist in an Amazon S3 bucket and have the same name. In this case, if the object name doesn't contain a trailing slash, only the folder is visible in a file gateway. For example, if a bucket contains an object named test or test/ and a folder named test/test1, only test/ and test/test1 are visible in a file gateway.
- You might need to remount your file share after a reboot of your client.
- By default Windows uses a soft mount for mounting your NFS share. Soft mounts time out more easily when there are connection issues. We recommend using a hard mount because a hard mount is safer and better preserves your data. The soft mount command omits the **-o mtype=hard** switch. The Windows hard mount command uses the **-o mtype=hard** switch.
- If you are using Windows clients, check your mount options after mounting by running the mount command with no options. The response should confirm the file share was mounted using the latest options you provided. It also should confirm that you are not using cached old entries, which take at least 60 seconds to clear.

### Next Step

[Testing your file gateway \(p. 65\)](#)

## Mounting your SMB file share on your client

Now you mount your SMB file share and map to a drive accessible to your client. The console's file gateway section shows the supported mount commands that you can use for SMB clients. Following, you can find some additional options to try.

You can use several different methods for mounting SMB file shares, including the following:

- The `net use` command – Doesn't persist across system reboots, unless you use the `/persistent: (yes|no)` switch. The specific command that you use depends on whether you plan to use your file share for Microsoft Active Directory (AD) access or guest access.
- The `CmdKey` command line utility – Creates a persistent connection to a mounted SMB file share that remains after a reboot.
- A network drive mapped in File Explorer – Configures the mounted file share to reconnect at sign-in and to require that you enter your network credentials.
- PowerShell script – Can be persistent, and can be either visible or invisible to the operating system while mounted.

### Note

If you are a Microsoft AD user, check with your administrator to ensure that you have access to the SMB file share before mounting the file share to your local system.

If you are a guest user, make sure that you have the guest user account password before attempting to mount the file share.

### To mount your SMB file share for Microsoft AD users using the `net use` command

1. Make sure that you have access to the SMB file share before mounting the file share to your local system.
2. For Microsoft AD clients, type the following command at the command prompt:

`net use [WindowsDriveLetter]: \\[Gateway IP Address]\[File share name]`

### To mount your SMB file share for guest users using the `net use` command

1. Make sure that you have the guest user account password before mounting the file share.
2. For Windows guest clients, type the following command at the command prompt.

`net use [WindowsDriveLetter]: \\$[Gateway IP Address]\$[path] /user: $[Gateway ID]\smbguest`

### To mount an SMB file share on Windows using `CmdKey`

1. Press the Windows key and type `cmd` to view the command prompt menu item.
2. Open the context (right-click) menu for **Command Prompt** and choose **Run as administrator**.
3. Type the following command:

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

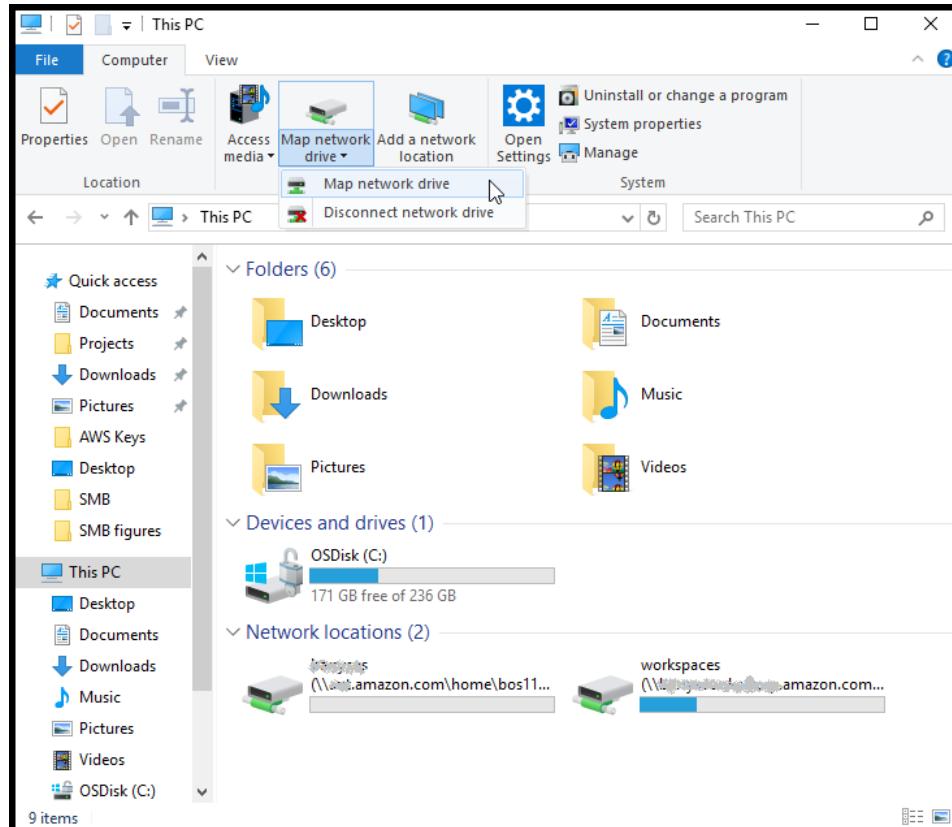
### Note

When mounting file shares, be aware of the following:

- You might have a case where a folder and an object exist in an Amazon S3 bucket and have the same name. In this case, if the object name doesn't contain a trailing slash, only the folder is visible in a file gateway. For example, if a bucket contains an object named test or test/ and a folder named test/test1, only test/ and test/test1 are visible in a file gateway.
- You might need to remount your file share after a reboot of your client.

## To mount an SMB file share using Windows File Explorer

1. Press the Windows key and type **File Explorer** in the **Search Windows** box, or press **Win+E**.
2. In the navigation pane, choose **This PC**, then choose **Map Network Drive** for **Map Network Drive** in the **Computer** tab, as shown in the following screenshot.



3. In the **Map Network Drive** dialog box, choose a drive letter for **Drive**.
4. For **Folder**, type **\[File Gateway IP]\[SMB File Share Name]**, or choose **Browse** to select your SMB file share from the dialog box.
5. (Optional) Select **Reconnect at sign-up** if you want your mount point to persist after reboots.
6. (Optional) Select **Connect using different credentials** if you want a user to enter the Microsoft AD logon or guest account user password.
7. Choose **Finish** to complete your mount point.

You can edit file share settings, edit allowed and denied users and groups, and change the guest access password from the Storage Gateway Management Console. You can also refresh the data in the file share's cache and delete a file share from the console.

## To modify your SMB file share's properties

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.

2. On the navigation pane, choose **File Shares**.
3. On the **File Share** page, select the check box by the SMB file share that you want to modify.
4. For Actions, choose the action that you want:
  - Choose **Edit file share settings** to modify share access.
  - Choose **Edit allowed/denied users** to add or delete users and groups, and then type the allowed and denied users and groups into the **Allowed Users**, **Denied Users**, **Allowed Groups**, and **Denied Groups** boxes. Use the **Add Entry** buttons to create new access rights, and the **(X)** button to remove access.
5. When you're finished, choose **Save**.

When you enter allowed users and groups, you are creating an allow list. Without an allow list, all authenticated Microsoft AD users can access the SMB file share. Any users and groups that are marked as denied are added to a deny list and can't access the SMB file share. In instances where a user or group is on both the deny list and allow list, the deny list takes precedence.

You can enable Access Control Lists(ACLs) on your SMB file share. For information about how to enable ACLs, see [Using Microsoft Windows ACLs to Control Access to an SMB File Share \(p. 347\)](#).

#### Next Step

[Testing your file gateway \(p. 65\)](#)

## Working with file shares on a bucket with pre-existing objects

You can export a file share on an Amazon S3 bucket with objects created outside of the file gateway using either NFS or SMB. Objects in the bucket that were created outside of the gateway display as files in either the NFS or SMB file system when your file system clients access them. Standard Portable Operating System Interface (POSIX) access and permissions are used in the file share. When you write files back to an Amazon S3 bucket, the files assume the properties and access rights that you give them.

You can upload objects to an S3 bucket at any time. For the file share to display these newly added objects as files, you need to refresh the S3 bucket. For more information, see [the section called "Refreshing objects in your Amazon S3 bucket" \(p. 173\)](#).

#### Note

We don't recommend having multiple writers for one Amazon S3 bucket. If you do, be sure to read the section "Can I have multiple writers to my Amazon S3 bucket?" in the [Storage Gateway FAQ](#).

To assign metadata defaults to objects accessed using NFS, see [Editing Metadata Defaults in the section called "Managing your file gateway" \(p. 162\)](#).

For SMB, you can export a share using Microsoft AD or guest access for an Amazon S3 bucket with pre-existing objects. Objects exported through an SMB file share inherits POSIX ownership and permissions from the parent directory right above it. For objects under the root folder, root Access Control Lists (ACL) are inherited. For Root ACL, the owner is `smbguest` and the permissions for files are 666 and the directories are 777. This applies to all forms of authenticated access (Microsoft AD and guest).

## Testing your file gateway

You can copy files and folders to your mapped drive. The files automatically upload to your Amazon S3 bucket.

#### To upload files from your Windows client to Amazon S3

1. On your Windows client, navigate to the drive that you mounted your file share on. The name of your drive is preceded by the name of your S3 bucket.

2. Copy files or a folder to the drive.
3. On the Amazon S3 Management Console, navigate to your mapped bucket. You should see the files and folders that you copied in the Amazon S3 bucket that you specified.

You can see the file share that you created in the **File shares** tab in the AWS Storage Gateway Management Console.

Your NFS or SMB client can write, read, delete, rename, and truncate files.

**Note**

File gateways don't support creating hard or symbolic links on a file share.

Keep in mind these points about how file gateways work with S3:

- Reads are served from a read-through cache. In other words, if data isn't available, it's fetched from S3 and added to the cache.
- Writes are sent to S3 through optimized multipart uploads by using a write-back cache.
- Read and writes are optimized so that only the parts that are requested or changed are transferred over the network.
- Deletes remove objects from S3.
- Directories are managed as folder objects in S3, using the same syntax as in the Amazon S3 console. You can rename empty directories.
- Recursive file system operation performance (for example `ls -1`) depends on the number of objects in your bucket.

**Next Step**

[Where do I go from here? \(p. 66\)](#)

## Where do I go from here?

In the preceding sections, you created and started using a file gateway, including mounting a file share and testing your setup.

Other sections of this guide include information about how to do the following:

- To manage your file gateway, see [Managing your file gateway \(p. 162\)](#).
- To optimize your file gateway, see [Optimizing Gateway Performance \(p. 327\)](#).
- To troubleshoot gateway problems, see [Troubleshooting your gateway \(p. 360\)](#).
- To learn about Storage Gateway metrics and how you can monitor how your gateway performs, see [Monitoring Storage Gateway \(p. 215\)](#).

## Cleaning up resources you don't need

If you created your gateway as an example exercise or a test, consider cleaning up to avoid incurring unexpected or unnecessary charges.

### To clean up resources you don't need

1. Unless you plan to continue using the gateway, delete it. For more information, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).
2. Delete the Storage Gateway VM from your on-premises host. If you created your gateway on an Amazon EC2 instance, terminate the instance.

# Creating a Volume Gateway

In this section, you can find instructions about how to create and use a volume gateway.

## Topics

- [Creating a Gateway \(p. 67\)](#)
- [Creating a volume \(p. 72\)](#)
- [Using Your Volume \(p. 74\)](#)
- [Backing Up Your Volumes \(p. 81\)](#)

## Creating a Gateway

In this section, you can find instructions about how to download, deploy, and activate a volume gateway.

## Topics

- [Choosing a Gateway Type \(p. 67\)](#)
- [Choosing a Host Platform and Downloading the VM \(p. 68\)](#)
- [Choosing a Service Endpoint \(p. 69\)](#)
- [Connecting to Your Gateway \(p. 70\)](#)
- [Activating Your Gateway \(p. 71\)](#)
- [Configuring Local Disks \(p. 71\)](#)
- [Configuring Amazon CloudWatch Logging \(p. 72\)](#)
- [Verifying VMware High Availability \(VMware HA Clusters Only\) \(p. 72\)](#)

## Choosing a Gateway Type

With a volume gateway, you can create storage volumes in the Amazon Web Services Cloud that your on-premises applications can access as Internet Small Computer System Interface (iSCSI) targets. There are two options:

- [Cached volumes \(p. 4\)](#)—Store your data in AWS and retain a copy of frequently accessed data subsets locally.
- [Stored volumes \(p. 6\)](#)—Store all your data locally and asynchronously back up point-in-time snapshots to AWS.

### To choose a gateway type

1. Open the Amazon Web Services Management Console at <https://console.aws.amazon.com/storagegateway/home>, and choose the AWS Region that you want to create your gateway in.

If you have previously created a gateway in this AWS Region, the console shows your gateway. Otherwise, the service homepage appears.

2. If you haven't created a gateway in the AWS Region you selected, choose **Get started**. If you already have a gateway in the AWS Region you chose, choose **Gateways** from the navigation pane, and then choose **Create gateway**.
3. On the **Select gateway type** page, choose **Volume gateway**, choose the type of volume, and then choose **Next**.

## Choosing a Host Platform and Downloading the VM

If you create your gateway on-premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see [Supported hypervisors and host requirements \(p. 22\)](#).

**Note**

You can run only file, cached volume, and tape gateways on an Amazon EC2 instance.

### To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:
  - If you choose the hardware appliance, activate it by following the instructions in [Activating your hardware appliance \(p. 33\)](#).
  - If you choose one of the other options, choose **Download image** next to your virtualization platform to download a .zip file that contains the .ova file for your virtualization platform.

**Note**

The .zip file is over 500 MB in size and might take some time to download, depending on your network connection.

For Amazon EC2, you create an instance from the provided AMI.

3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache and one local disk for your upload buffer during the deployment. A file gateway requires only one local disk for a cache. For information about local disk requirements, see [Hardware and storage requirements \(p. 12\)](#).

Depending your hypervisor, set certain options:

- If you choose VMware, do the following:
  - Store your disk using the **Thick provisioned format** option. When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in thick-provisioned format.
  - Configure your gateway VM to use paravirtualized disk controllers. For more information, see [Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers \(p. 395\)](#).
- If you choose Microsoft Hyper-V, do the following:
  - Configure the disk type using the **Fixed size** option. When you use fixed-size provisioning, the disk storage is allocated immediately, resulting in better performance. If you don't use fixed-size provisioning, the storage is allocated on demand. On-demand allocation can affect the functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in fixed-size provisioned format.
  - When allocating disks, choose **virtual hard disk (.vhdx) file**. Storage Gateway supports the .vhdx file type. By using this file type, you can create larger virtual disks than with other file types. If you create a .vhdx type virtual disk, make sure that the size of the virtual disks that you create doesn't exceed the recommended disk size for your gateway.
- If you choose Linux Kernel-based Virtual Machine (KVM), do the following:
  - Don't configure your disk to use **sparse** formatting. When you use fixed-size (nonsparse) provisioning, the disk storage is allocated immediately, resulting in better performance.

- Use the parameter `sparse=false` to store your disk in nonsparse format when creating new virtual disks in the VM with the `virt-install` command for provisioning new virtual machines.
- Use `virtio` drivers for disk and network devices.
- We recommend that you don't set the `current_memory` option. If necessary, set it equal to the RAM provisioned to the gateway in the `--ram` parameter.

Following is an example `virt-install` command for installing KVM.

```
virt-install --name "SGW_KVM" --description "SGW KVM" --os-type=generic --  
ram=32768 --vcpus=16 --disk path=fgw-kvm.qcow2,bus=virtio,size=80,sparse=false  
--disk path=fgw-kvm-cache.qcow2,bus=virtio,size=1024,sparse=false --network  
default,model=virtio --graphics none --import
```

#### Note

For VMware, Microsoft Hyper-V, and KVM, synchronizing the VM time with the host time is required for successful gateway activation. Make sure that your host clock is set to the correct time and synchronize it with a Network Time Protocol (NTP) server.

For information about deploying your gateway to an Amazon EC2 host, see [Deploy Your Gateway to an Amazon EC2 Host \(p. 399\)](#).

## Choosing a Service Endpoint

You can activate your gateway using:

- A public service endpoint and have your gateway communicate with AWS storage services over the public internet.
- A Federal Information Processing Standards (FIPS) compliant public service endpoint and have your gateway communicate with AWS storage services over the public internet.
- A public service endpoint and have your gateway communicate with AWS storage services using a virtual private cloud (VPC) endpoint, which is private.

#### Note

If you use a VPC endpoint, all VPC endpoint communication from your gateway to AWS services occurs through the public service endpoint using your VPC in AWS.

### To choose a service endpoint

1. For **Select service endpoint**, choose one of the following:
    - To have your gateway access AWS services over the public internet using a public service endpoint, choose **Public**.
    - To have your gateway access AWS services over the public internet using a public service endpoint that complies with FIPS, choose **FIPS**.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).
- To have your gateway access AWS services over a private VPC endpoint connection using a public service endpoint, choose **VPC**.

**Note**

The FIPS service endpoint is only available in some AWS Regions. For more information, see [Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.

This procedure assumes that you are activating your gateway with a public endpoint. For information about how to activate a gateway using a VPC endpoint, see [Activating a gateway in a virtual private cloud \(p. 153\)](#).

2. Choose **Next** to connect and activate your gateway.

## Connecting to Your Gateway

To connect to your gateway, first get the IP address or activation key of your gateway VM. You use the IP address or activation key to activate your gateway. For gateways deployed and activated on an on-premises host, you can get the IP address or activation key from your gateway VM local console or your hypervisor client. For gateways deployed and activated on an Amazon EC2 instance, you can get the IP address or activation key from the Amazon EC2 console.

The activation process associates your gateway with your AWS account. Your gateway VM must be running for activation to succeed.

**Note**

Make sure that you select the correct gateway type. The .ova files and Amazon Machine Images (AMIs) for the gateway types are different and are not interchangeable.

### To get the IP address or activation key for your gateway VM from the local console

1. Log on to your gateway VM local console. For detailed instructions, see the following:
  - VMware ESXi – [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. Get the IP address from the top of the menu page, and note it for later use.

### To get the IP address or activation key from an EC2 instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then choose the EC2 instance.
3. Choose the **Details** tab at the bottom, and then note the IP address or activation key. You use one of these to activate the gateway.

**Note**

For activation with an IP address, you can use the public or private IP address assigned to a gateway. You must be able to reach the IP address that you use from the browser from which you perform the activation.

### To associate your gateway with your AWS account

1. For **Connect to gateway**, choose one of the following:
  - **IP address**
  - **Activation key**
2. Enter the IP address or activation key of your gateway, and then choose **Next**.

For detailed information about how to get a gateway IP address, see [Connecting to Your Gateway \(p. 440\)](#).

## Activating Your Gateway

The following, shown on the activation page, are the gateway settings that you selected. The activation page appears after you associate your gateway with your Amazon Web Services account, as described preceding.

- **Gateway type** specifies the type of gateway that you are activating.
- **Endpoint type** specifies the type of endpoint that you selected for your gateway.
- **AWS Region** specifies the AWS Region where your gateway will be activated and where your data will be stored. If **Endpoint type** is **VPC**, the AWS Region should be same as the Region where your VPC endpoint is located.

### To activate your gateway

1. In **Activate gateway**, do the following:

- For **Gateway time zone**, select a time zone to use for your gateway.
- For **Gateway name**, enter a name to identify your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.

**Note**

The gateway name must be between 2 and 255 characters in length.

2. (Optional) For **Add tags**, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

If activation isn't successful, see [Troubleshooting your gateway \(p. 360\)](#) for possible solutions.

## Configuring Local Disks

When you deployed the VM, you allocated local disks for your gateway. Now you configure your gateway to use these disks.

**Note**

If you allocate local disks on a VMware host, make sure to configure the disks to use paravirtualized disk controllers.

When adding a cache or upload buffer to an existing gateway, make sure to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

- For a [cached volume \(p. 4\)](#), you configure at least one disk for an upload buffer and the other for cache storage.
- For a [stored volume \(p. 6\)](#), you configure at least one disk for an upload buffer and allocate the rest of the storage for your application data.

### To configure local disks

1. For **Configure local disks**, identify the disks you allocated and decide which ones you want to use for an upload buffer and cached storage. For information about disk size quotas, see [Recommended local disk sizes for your gateway \(p. 445\)](#).
2. For **Allocated to**, choose **Upload buffer** for the disk you want to configure as upload buffer.

3. For cached volumes and tapes, choose **Cache** for the disk you want to configure as cache storage.  
If you don't see your disks, choose **Refresh**.
4. Choose **Continue to logging**.

## Configuring Amazon CloudWatch Logging

To notify you about the health of your volume gateway and its resources, you can configure an Amazon CloudWatch log group. For more information, see [Getting Volume Gateway Health Logs with CloudWatch Log Groups \(p. 237\)](#).

### To configure a CloudWatch log group for your file gateway

1. For **Configure logging - optional**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.
  - **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.

Choose a log group from the **Existing log group list**.
2. Choose **Save and continue** to save your configuration settings.

## Verifying VMware High Availability (VMware HA Clusters Only)

If your gateway is not deployed on a VMware host that is enabled for VMware High Availability (HA), you can skip this section.

If your gateway is deployed on a VMware host that is enabled for VMware High Availability (HA) cluster, you can either test the configuration when activating the gateway or after your gateway is activated. The following instructions show you how to test the configuration during activation.

### To test for VMware HA

1. For **Verify VMware High Availability configuration**, choose **Next**. Verification can take up to two minutes to complete.  
If the test is successful, a message that indicates a successful test is displayed in the banner. If the test fails, a failed message is displayed. You can make changes in your vSphere configuration and repeat the test.
2. To repeat the test, on the **Gateways** dashboard, choose your gateway, and then for **Actions**, choose **Verify VMware High Availability**.

For information about how to configure your gateway for VMware HA, see [Using VMware vSphere High Availability with Storage Gateway \(p. 329\)](#).

### Next Step

[Creating a volume \(p. 72\)](#)

## Creating a volume

Previously, you allocated local disks that you added to the VM cache storage and upload buffer. Now you create a storage volume to which your applications read and write data. The gateway maintains

the volume's recently accessed data locally in cache storage, and asynchronously transferred data to Amazon S3. For stored volumes, you allocated local disks that you added to the VM upload buffer and your application's data.

**Note**

You can use AWS Key Management Service (AWS KMS) to encrypt data written to a cached volume that is stored in Amazon S3. Currently, you can do this by using the *AWS Storage Gateway API Reference*. For more information, see [CreateCachediSCSIVolume](#) or [create-cached-iscsi-volume](#).

**To create a volume**

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the Storage Gateway console, choose **Create volume**.
3. In the **Create volume** dialog box, choose a gateway for **Gateway**.
4. For the cached volumes, enter the capacity in **Capacity**.

For stored volumes, choose a **Disk ID** value from the list.

5. For **Volume content**, your choices depend on the type of gateway that you're creating the volume for.

For cached volumes, you have the following options:

- **Create a new empty volume**.
- **Create a volume based on an Amazon EBS snapshot**. If you choose this option, provide a value for **EBS snapshot ID**.
- **Clone from last volume recovery point**. If you choose this option, choose a volume ID for **Source volume**. If there are no volumes in the Region, this option doesn't appear.

For stored volumes, you have the following options:

- **Create a new empty volume**.
  - **Create a volume based on a snapshot**. If you choose this option, provide a value for **EBS snapshot ID**.
  - **Preserve existing data on the disk**
6. Enter a name for **iSCSI target name**.

The target name can contain lowercase letters, numbers, periods (.), and hyphens (-). This target name appears as the **iSCSI target node** name in the **Targets** tab of the **iSCSI Microsoft initiator** UI after discovery. For example, the name target1 appears as iqn.1007-05.com.amazon:target1. Make sure that the target name is globally unique within your storage area network (SAN).

7. Verify that the **Network interface** setting has IP address selected, or choose an IP address for **Network interface**. For **Network interface**, one IP address appears for each adapter that is configured for the gateway VM. If the gateway VM is configured for only one network adapter, no **Network interface** list appears because there is only one IP address.

Your iSCSI target will be available on the network adapter you choose.

If you have defined your gateway to use multiple network adapters, choose the IP address that your storage applications should use to access your volume. For information about configuring multiple network adapters, see [Configuring Your Gateway for Multiple NICs \(p. 303\)](#).

**Note**

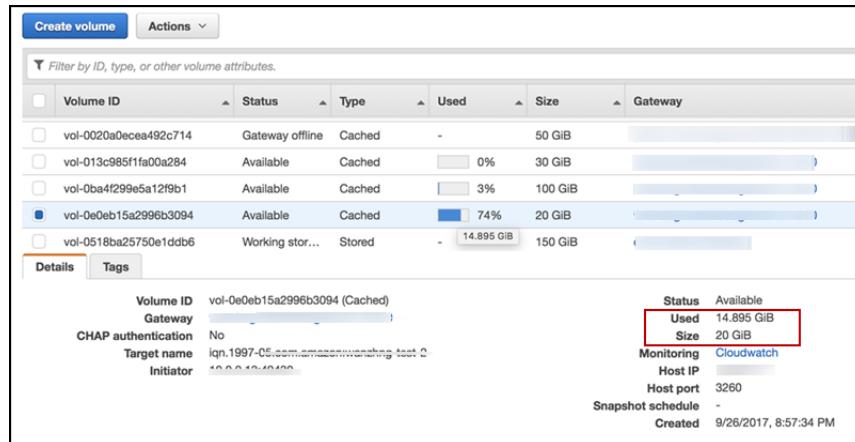
After you choose a network adapter, you can't change this setting.

8. (Optional) For **Tags**, enter a key and value to add tags to your volume. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your volumes.

9. Choose **Create volume**.

If you have previously created volumes in this Region, you can see them listed on the Storage Gateway console.

The **Configure CHAP Authentication** dialog box appears. At this point, you can configure Challenge-Handshake Authentication Protocol (CHAP) for your volume, or you can choose **Cancel** and configure CHAP later. For more information about CHAP setup, see [Configure CHAP authentication for your volumes \(p. 74\)](#).



If you don't want to set up CHAP, get started using your volume. For more information, see [Using Your Volume \(p. 74\)](#).

## Configure CHAP authentication for your volumes

CHAP provides protection against playback attacks by requiring authentication to access your storage volume targets. In the **Configure CHAP Authentication** dialog box, you provide information to configure CHAP for your volumes.

### To configure CHAP

1. Choose the volume for which you want to configure CHAP.
2. For **Actions**, choose **Configure CHAP authentication**.
3. For **Initiator Name**, enter the name of your initiator.
4. For **Initiator secret**, enter the secret phrase that you used to authenticate your iSCSI initiator.
5. For **Target secret**, enter the secret phrase used to authenticate your target for mutual CHAP.
6. Choose **Save** to save your entries.

For more information about setting up CHAP authentication, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).

### Next step

[Using Your Volume \(p. 74\)](#)

## Using Your Volume

Following, you can find instructions about how to use your volume. To use your volume, you first connect it to your client as an iSCSI target, then initialize and format it.

## Topics

- [Connecting Your Volumes to Your Client \(p. 75\)](#)
- [Initializing and Formatting Your Volume \(p. 76\)](#)
- [Testing Your Gateway \(p. 78\)](#)
- [Where Do I Go from Here? \(p. 79\)](#)

## Connecting Your Volumes to Your Client

You use the iSCSI initiator in your client to connect to your volumes. At the end of the following procedure, the volumes become available as local devices on your client.

### Important

With Storage Gateway, you can connect multiple hosts to the same volume if the hosts coordinate access by using Windows Server Failover Clustering (WSFC). You can't connect multiple hosts to the same volume without using WSFC, for example by sharing a nonclustered NTFS/ext4 file system.

## Topics

- [Connecting to a Microsoft Windows Client \(p. 75\)](#)
- [Connecting to a Red Hat Enterprise Linux Client \(p. 75\)](#)

## Connecting to a Microsoft Windows Client

The following procedure shows a summary of the steps that you follow to connect to a Windows client. For more information, see [Connecting iSCSI Initiators \(p. 414\)](#).

### To connect to a Windows client

1. Start iscsicpl.exe.
2. In the **iSCSI Initiator Properties** dialog box, choose the **Discovery** tab, and then choose **Discovery Portal**.
3. In the **Discover Target Portal** dialog box, type the IP address of your iSCSI target for IP address or DNS name.
4. Connect the new target portal to the storage volume target on the gateway.
5. Choose the target, and then choose **Connect**.
6. In the **Targets** tab, make sure that the target status has the value **Connected**, indicating the target is connected, and then choose **OK**.

## Connecting to a Red Hat Enterprise Linux Client

The following procedure shows a summary of the steps that you follow to connect to a Red Hat Enterprise Linux (RHEL) client. For more information, see [Connecting iSCSI Initiators \(p. 414\)](#).

### To connect a Linux client to iSCSI targets

1. Install the iscsi-initiator-utils RPM package.

You can use the following command to install the package.

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

2. Make sure that the iSCSI daemon is running.

For RHEL 5 or 6, use the following command.

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

For RHEL 7, use the following command.

```
sudo service iscsid status
```

3. Discover the volume or VTL device targets defined for a gateway. Use the following discovery command.

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

The output of the discovery command should look like the following example output.

For volume gateways: [GATEWAY\_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume

For tape gateways: iqn.1997-05.com.amazon:[GATEWAY\_IP]-tapedrive-01

4. Connect to a target.

Make sure to specify the correct [GATEWAY\_IP] and IQN in the connect command.

Use the following command.

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

5. Verify that the volume is attached to the client machine (the initiator). To do so, use the following command.

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

The output of the command should look like the following example output.

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

We highly recommend that after you set up your initiator you customize your iSCSI settings as discussed in [Customizing Your Linux iSCSI Settings \(p. 428\)](#).

## Initializing and Formatting Your Volume

After you use the iSCSI initiator in your client to connect to your volumes, you initialize and format your volume.

### Topics

- [Initializing and Formatting Your Volume on Microsoft Windows \(p. 76\)](#)
- [Initializing and Formatting Your Volume on Red Hat Enterprise Linux \(p. 77\)](#)

## Initializing and Formatting Your Volume on Microsoft Windows

Use the following procedure to initialize and format your volume on Windows.

### To initialize and format your storage volume

1. Start `diskmgmt.msc` to open the **Disk Management** console.
2. In the **Initialize Disk** dialog box, initialize the volume as a **MBR (Master Boot Record)** partition. When selecting the partition style, you should take into account the type of volume you are connecting to—cached or stored—as shown in the following table.

Partition Style	Use in the Following Conditions
<b>MBR (Master Boot Record)</b>	<ul style="list-style-type: none"> <li>• If your gateway is a stored volume and the storage volume is limited to 1 TiB in size.</li> <li>• If your gateway is a cached volume and the storage volume is less than 2 TiB in size.</li> </ul>
<b>GPT (GUID Partition Table)</b>	If your gateway's storage volume is 2 TiB or greater in size.

3. Create a simple volume:
  - a. Bring the volume online to initialize it. All the available volumes are displayed in the disk management console.
  - b. Open the context (right-click) menu for the disk, and then choose **New Simple Volume**.

**Important**

Be careful not to format the wrong disk. Check to make sure that the disk you are formatting matches the size of the local disk you allocated to the gateway VM and that it has a status of **Unallocated**.

- c. Specify the maximum disk size.
- d. Assign a drive letter or path to your volume, and format the volume by choosing **Perform a quick format**.

**Important**

We strongly recommend using **Perform a quick format** for cached volumes. Doing so results in less initialization I/O, smaller initial snapshot size, and the fastest time to a usable volume. It also avoids using cached volume space for the full format process.

**Note**

The time that it takes to format the volume depends on the size of the volume. The process might take several minutes to complete.

## Initializing and Formatting Your Volume on Red Hat Enterprise Linux

Use the following procedure to initialize and format your volume on Red Hat Enterprise Linux (RHEL).

### To initialize and format your storage volume

1. Change directory to the `/dev` folder.
2. Run the `sudo cfdisk` command.
3. Identify your new volume by using the following command. To find new volumes, you can list the partition layout of your volumes.

```
$ lsblk
```

An "unrecognized volumes label" error for the new unpartitioned volume appears.

4. Initialize your new volume. When selecting the partition style, you should take into account the size and type of volume you are connecting to—cached or stored—as shown in the following table.

Partition Style	Use in the Following Conditions
<b>MBR (Master Boot Record)</b>	<ul style="list-style-type: none"> <li>If your gateway is a stored volume and the storage volume is limited to 1 TiB in size.</li> <li>If your gateway is a cached volume and the storage volume is less than 2 TiB in size.</li> </ul>
<b>GPT (GUID Partition Table)</b>	If your gateway's storage volume is 2 TiB or greater in size.

For an MBR partition, use the following command: `sudo parted /dev/your volume mklabel msdos`

For a GPT partition, use the following command: `sudo parted /dev/your volume mklabel gpt`

5. Create a partition by using the following command.

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

6. Assign a drive letter to the partition and create a file system by using the following command.

`sudo mkfs drive letter datapartition /dev/your volume`

7. Mount the file system by using the following command.

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

## Testing Your Gateway

You test your volume gateway setup by performing the following tasks:

1. Write data to the volume.
2. Take a snapshot.
3. Restore the snapshot to another volume.

You verify the setup for a gateway by taking a snapshot backup of your volume and storing the snapshot in AWS. You then restore the snapshot to a new volume. Your gateway copies the data from the specified snapshot in AWS to the new volume.

### Note

Restoring data from Amazon Elastic Block Store (Amazon EBS) volumes that are encrypted is not supported.

### To create an Amazon EBS snapshot of a storage volume on Microsoft Windows

1. On your Windows computer, copy some data to your mapped storage volume.

The amount of data copied doesn't matter for this demonstration. A small file is enough to demonstrate the restore process.

2. In the navigation pane of the Storage Gateway console, choose **Volumes**.
3. Choose the storage volume that you created for the gateway.

This gateway should have only one storage volume. Choose the volume displays its properties.

4. For **Actions**, choose **Create EBS snapshot** to create a snapshot of the volume.

Depending on the amount of data on the disk and the upload bandwidth, it might take a few seconds to complete the snapshot. Note the volume ID for the volume from which you create a snapshot. You use the ID to find the snapshot.

5. In the **Create EBS Snapshot** dialog box, provide a description for your snapshot.
6. (Optional) For **Tags**, enter a key and value to add tags to the snapshot. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your snapshots.
7. Choose **Create Snapshot**. Your snapshot is stored as an Amazon EBS snapshot. Note your snapshot ID. The number of snapshots created for your volume is displayed in the snapshot column.
8. In the **EBS snapshots** column, choose the link for the volume that you created the snapshot for to see your EBS snapshot on the Amazon EC2 console.

#### To restore a snapshot to another volume

See [Creating a volume \(p. 72\)](#).

## Where Do I Go from Here?

In the preceding sections, you created and provisioned a gateway and then connected your host to the gateway's storage volume. You added data to the gateway's iSCSI volume, took a snapshot of the volume, and restored it to a new volume, connected to the new volume, and verified that the data shows up on it.

After you finish the exercise, consider the following:

- If you plan on continuing to use your gateway, read about sizing the upload buffer more appropriately for real-world workloads. For more information, see [Sizing Your Volume Gateway's Storage for Real-World Workloads \(p. 79\)](#).
- If you don't plan on continuing to use your gateway, consider deleting the gateway to avoid incurring any charges. For more information, see [Cleaning Up Resources You Don't Need \(p. 80\)](#).

Other sections of this guide include information about how to do the following:

- To learn more about storage volumes and how to manage them, see [Managing Your Gateway \(p. 162\)](#).
- To troubleshoot gateway problems, see [Troubleshooting your gateway \(p. 360\)](#).
- To optimize your gateway, see [Optimizing Gateway Performance \(p. 327\)](#).
- To learn about Storage Gateway metrics and how you can monitor how your gateway performs, see [Monitoring Storage Gateway \(p. 215\)](#).
- To learn more about configuring your gateway's iSCSI targets to store data, see [Connecting to Your Volumes to a Windows Client \(p. 415\)](#).

To learn about sizing your volume gateway's storage for real-world workloads and cleaning up resources you don't need, see the following sections.

## Sizing Your Volume Gateway's Storage for Real-World Workloads

By this point, you have a simple, working gateway. However, the assumptions used to create this gateway are not appropriate for real-world workloads. If you want to use this gateway for real-world workloads, you need to do two things:

1. Size your upload buffer appropriately.
2. Set up monitoring for your upload buffer, if you haven't done so already.

Following, you can find how to do both of these tasks. If you activated a gateway for cached volumes, you also need to size your cache storage for real-world workloads.

### To size your upload buffer and cache storage for a gateway-cached setup

- Use the formula shown in [Determining the size of upload buffer to allocate \(p. 255\)](#) for sizing the upload buffer. We strongly recommend that you allocate at least 150 GiB for the upload buffer. If the upload buffer formula yields a value less than 150 GiB, use 150 GiB as your allocated upload buffer.

The upload buffer formula takes into account the difference between throughput from your application to your gateway and throughput from your gateway to AWS, multiplied by how long you expect to write data. For example, assume that your applications write text data to your gateway at a rate of 40 MB per second for 12 hours a day and your network throughput is 12 MB per second. Assuming a compression factor of 2:1 for the text data, the formula specifies that you need to allocate approximately 675 GiB of upload buffer space.

### To size your upload buffer for a stored setup

- Use the formula discussed in [Determining the size of upload buffer to allocate \(p. 255\)](#). We strongly recommend that you allocate at least 150 GiB for your upload buffer. If the upload buffer formula yields a value less than 150 GiB, use 150 GiB as your allocated upload buffer.

The upload buffer formula takes into account the difference between throughput from your application to your gateway and throughput from your gateway to AWS, multiplied by how long you expect to write data. For example, assume that your applications write text data to your gateway at a rate of 40 MB per second for 12 hours a day and your network throughput is 12 MB per second. Assuming a compression factor of 2:1 for the text data, the formula specifies that you need to allocate approximately 675 GiB of upload buffer space.

### To monitor your upload buffer

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose the **Gateway** tab, choose the **Details** tab, and then find the **Upload Buffer Used** field to view your gateway's current upload buffer.
3. Set one or more alarms to notify you about upload buffer use.

We highly recommend that you create one or more upload buffer alarms in the Amazon CloudWatch console. For example, you can set an alarm for a level of use you want to be warned about and an alarm for a level of use that, if exceeded, is cause for action. The action might be adding more upload buffer space. For more information, see [To set an upper threshold alarm for a gateway's upload buffer \(p. 220\)](#).

## Cleaning Up Resources You Don't Need

If you created your gateway as an example exercise or a test, consider cleaning up to avoid incurring unexpected or unnecessary charges.

### To clean up resources you don't need

1. Delete any snapshots. For instructions, see [Deleting a Snapshot \(p. 185\)](#).
2. Unless you plan to continue using the gateway, delete it. For more information, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).
3. Delete the Storage Gateway VM from your on-premises host. If you created your gateway on an Amazon EC2 instance, terminate the instance.

## Backing Up Your Volumes

By using Storage Gateway, you can help protect your on-premises business applications that use Storage Gateway volumes for cloud-backed storage. You can back up your on-premises Storage Gateway volumes using the native snapshot scheduler in Storage Gateway or AWS Backup. In both cases, Storage Gateway volume backups are stored as Amazon EBS snapshots in Amazon Web Services.

### Topics

- [Using Storage Gateway to Back Up Your Volumes \(p. 81\)](#)
- [Using AWS Backup to Back Up Your Volumes \(p. 81\)](#)

## Using Storage Gateway to Back Up Your Volumes

You can use the Storage Gateway Management Console to back up your volumes by taking Amazon EBS snapshots and storing the snapshots in Amazon Web Services. You can either take an ad hoc (one-time) snapshot or set up a snapshot schedule that is managed by Storage Gateway. You can later restore the snapshot to a new volume by using the Storage Gateway console. For information about how to back up and manage your backup from the Storage Gateway, see the following topics:

- [Testing Your Gateway \(p. 78\)](#)
- [Creating a One-Time Snapshot \(p. 184\)](#)
- [Cloning a Volume \(p. 179\)](#)

## Using AWS Backup to Back Up Your Volumes

AWS Backup is a centralized backup service that makes it easy and cost-effective for you to back up your application data across AWS services in both the Amazon Web Services Cloud and on-premises. Doing this helps you meet your business and regulatory backup compliance requirements. AWS Backup makes protecting your AWS storage volumes, databases, and file systems simple by providing a central place where you can do the following:

- Configure and audit the AWS resources that you want to back up.
- Automate backup scheduling.
- Set retention policies.
- Monitor all recent backup and restore activity.

Because Storage Gateway integrates with AWS Backup, it enables customers to use AWS Backup to back up on-premises business applications that use Storage Gateway volumes for cloud-backed storage. AWS Backup supports backup and restore of both cached and stored volumes. For information about AWS Backup, see the AWS Backup documentation. For information about AWS Backup, see [What is AWS Backup?](#) in the *AWS Backup User Guide*.

You can manage Storage Gateway volumes' backup and recovery operations with AWS Backup and avoid the need to create custom scripts or manually manage point-in-time backups. With AWS Backup, you can also monitor your on-premises volume backups alongside your in-cloud AWS resources from a single AWS Backup dashboard. You can use AWS Backup to either create a one-time on-demand backup or define a backup plan that is managed in AWS Backup.

Storage Gateway volume backups taken from AWS Backup are stored in Amazon S3 as Amazon EBS snapshots. You can see the Storage Gateway volume backups from the AWS Backup console or the Amazon EBS console.

You can easily restore Storage Gateway volumes that are managed through AWS Backup to any on-premises gateway or in-cloud gateway. You can also restore such a volume to an Amazon EBS volume that you can use with Amazon EC2 instances.

### Benefits of Using AWS Backup to Back Up Storage Gateway Volumes

The benefits of using AWS Backup to back up Storage Gateway volumes are that you can meet compliance requirements, avoid operational burden, and centralize backup management. AWS Backup enables you to do the following:

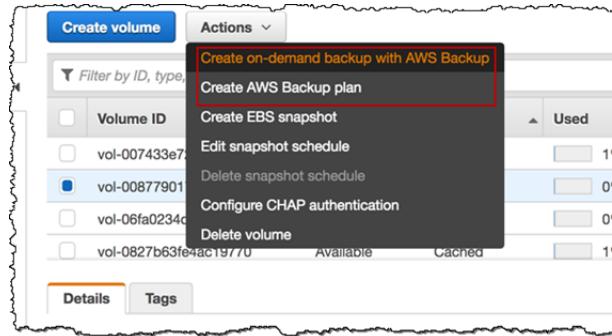
- Set customizable scheduled backup policies that meet your backup requirements.
- Set backup retention and expiration rules so you no longer need to develop custom scripts or manually manage the point-in-time backups of your volumes.
- Manage and monitor backups across multiple gateways, and other AWS resources from a central view.

### To use AWS Backup to create backups of your volumes

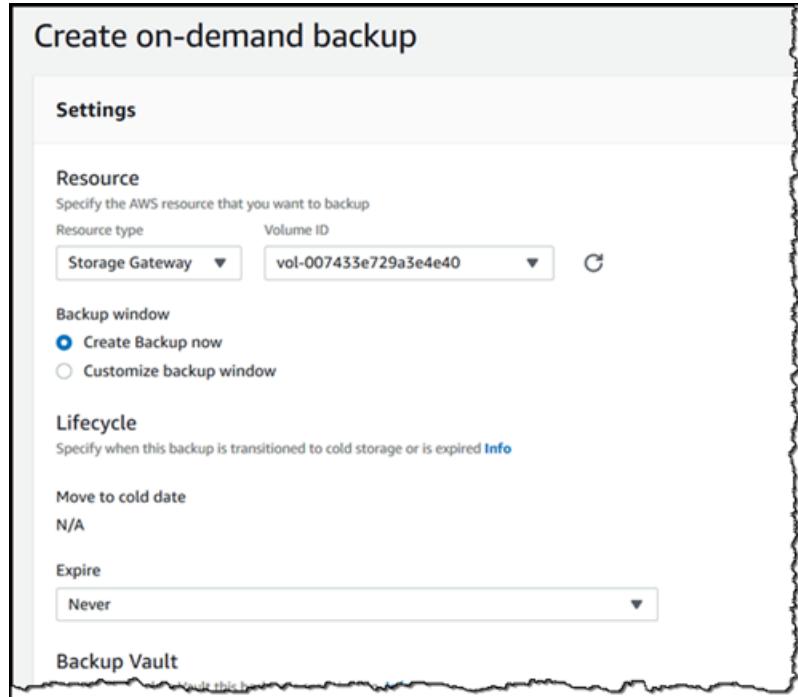
#### Note

AWS Backup requires that you choose an AWS Identity and Access Management (IAM) role that AWS Backup consumes. You need to create this role because AWS Backup doesn't create it for you. You also need to create a trust relationship between AWS Backup and this IAM role. For information about how to do this, see the *AWS Backup User Guide*. For information about how to do this, see [Creating a Backup Plan](#) in the *AWS Backup User Guide*.

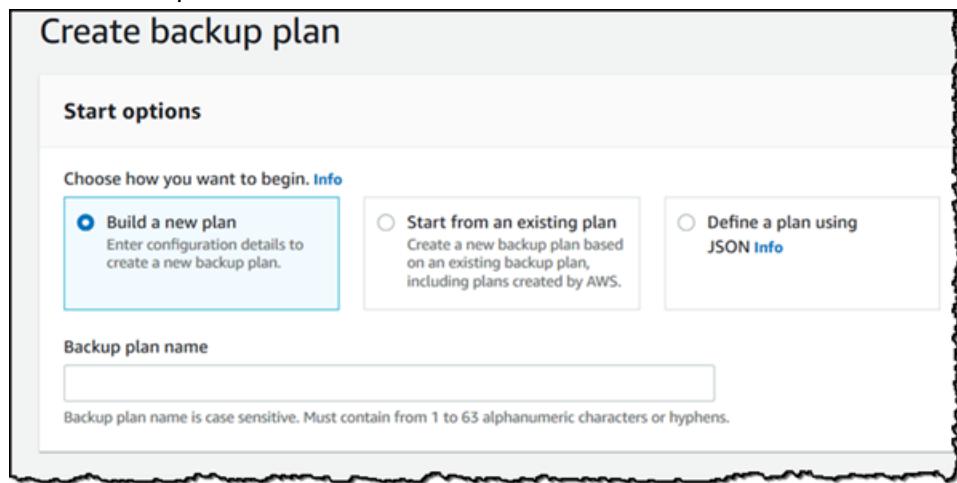
1. Open the Storage Gateway console and choose **Volumes** from the navigation pane at left.
2. For **Actions**, choose **Create on-demand backup with AWS Backup** or **Create AWS backup plan**.



If you want to create an on-demand backup of the Storage Gateway volume, choose **Create on-demand backup with AWS Backup**. You are directed to the AWS Backup console.



If you want to create a new AWS Backup plan, choose **Create AWS backup plan**. You are directed to the AWS Backup console.



On the AWS Backup console, you can create a backup plan, assign a Storage Gateway volume to the backup plan, and create a backup. You can also do ongoing backup management tasks.

## Finding and Restoring Your Volumes from AWS Backup

You can find and restore your backup Storage Gateway volumes from the AWS Backup console. For more information, see the *AWS Backup User Guide*. For more information, see [Recovery Points](#) in the *AWS Backup User Guide*.

## To find and restore your volumes

1. Open the AWS Backup console and find the Storage Gateway volume backup that you want to restore. You can restore the Storage Gateway volume backup to an Amazon EBS volume or to a Storage Gateway volume. Choose the appropriate option for your restore requirements.
2. For **Restore type**, choose to restore a stored or cached Storage Gateway volume and provide the required information:
  - For a stored volume, provide the information for **Gateway name**, **Disk ID**, and **iSCSI target name**.

The screenshot shows the 'Restore recovery point' dialog. Under 'Settings', the 'Snapshot ID' is gateway/sgw-CDEB0FA4/volume/vol-0a98befbff3c731c8. The 'Restore type' is set to 'Storage Gateway volume'. In the 'Gateway' dropdown, 'Demo-stored-SGW' is selected. In the 'Disk ID' dropdown, 'xen-vbd-51808' is selected. The 'iSCSI target name' field contains '1'. At the bottom right are 'Cancel' and 'Restore resource' buttons.

- For a cached volume, provide the information for **Gateway name**, **Capacity**, and **iSCSI target name**.

The screenshot shows the 'Restore recovery point' dialog for a cached volume. It has the same fields as the stored volume dialog: Snapshot ID, Restore type (Storage Gateway volume), Gateway (Demo-cached-SGW), Capacity (1 TiB), and iSCSI target name (1). The 'Restore resource' button is visible at the bottom right.

3. Choose **Restore resource** to restore your volume.

### Note

You can't use the Amazon EBS console to delete a snapshot that is created by AWS Backup.

## Creating a Tape Gateway

In this section, you can find instructions about how to create and use a tape gateway in AWS Storage Gateway.

### Note

The topics in this section describe the process to set up a standard Tape Gateway for copying tape data to AWS over a network connection. To set up a Tape Gateway on a Snowball Edge device to facilitate offline tape data migration, see [Using Tape Gateway on AWS Snowball Edge](#).

#### Topics

- [Creating a Gateway \(p. 85\)](#)
- [Creating a Custom Tape Pool \(p. 91\)](#)
- [Creating Tapes \(p. 93\)](#)
- [Using Your Tape Gateway \(p. 96\)](#)

## Creating a Gateway

In this section, you can find instructions about how to download, deploy, and activate a standard tape gateway. For instructions to set up Tape Gateway on Snowball Edge, see [Using Tape Gateway on AWS Snowball Edge](#)

#### Topics

- [Choosing a Gateway Type \(p. 85\)](#)
- [Choosing a Host Platform and Downloading the VM \(p. 85\)](#)
- [Choosing a Service Endpoint \(p. 87\)](#)
- [Connecting to Your Gateway \(p. 87\)](#)
- [Activating Your Gateway \(p. 88\)](#)
- [Configuring Local Disks \(p. 90\)](#)
- [Configuring Amazon CloudWatch Logging \(p. 90\)](#)
- [Verifying VMware High Availability \(VMware HA Clusters Only\) \(p. 91\)](#)

## Choosing a Gateway Type

For a tape gateway, you store and archive your data on virtual tapes in AWS. A tape gateway eliminates some of the challenges associated with owning and operating an on-premises physical tape infrastructure.

#### To create a tape gateway

1. Open the Amazon Web Services Management Console at <https://console.aws.amazon.com/storagegateway/home>, and choose **Create gateway**.
2. On the **Select gateway type** page, choose **Tape gateway**, and then choose **Next**.

## Choosing a Host Platform and Downloading the VM

If you create your gateway on-premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see [Supported hypervisors and host requirements \(p. 22\)](#).

#### Note

You can run only file, cached volume, and tape gateways on an Amazon EC2 instance.

#### To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:
  - If you choose the hardware appliance, activate it by following the instructions in [Activating your hardware appliance \(p. 33\)](#).

- If you choose one of the other options, choose **Download image** next to your virtualization platform to download a .zip file that contains the .ova file for your virtualization platform.

**Note**

The .zip file is over 500 MB in size and might take some time to download, depending on your network connection.

For Amazon EC2, you create an instance from the provided AMI.

3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache and one local disk for your upload buffer during the deployment. A file gateway requires only one local disk for a cache. For information about local disk requirements, see [Hardware and storage requirements \(p. 12\)](#).

Depending your hypervisor, set certain options:

- If you choose VMware, do the following:
  - Store your disk using the **Thick provisioned format** option. When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in thick-provisioned format.
  - Configure your gateway VM to use paravirtualized disk controllers. For more information, see [Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers \(p. 395\)](#).
- If you choose Microsoft Hyper-V, do the following:
  - Configure the disk type using the **Fixed size** option. When you use fixed-size provisioning, the disk storage is allocated immediately, resulting in better performance. If you don't use fixed-size provisioning, the storage is allocated on demand. On-demand allocation can affect the functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in fixed-size provisioned format.
  - When allocating disks, choose **virtual hard disk (.vhdx) file**. Storage Gateway supports the .vhdx file type. By using this file type, you can create larger virtual disks than with other file types. If you create a .vhdx type virtual disk, make sure that the size of the virtual disks that you create doesn't exceed the recommended disk size for your gateway.
- If you choose Linux Kernel-bases Virtual Machine (KVM), do the following:
  - Don't configure your disk to use **sparse** formatting. When you use fixed-size (nonsparse) provisioning, the disk storage is allocated immediately, resulting in better performance.
  - Use the parameter **sparse=false** to store your disk in nonsparse format when creating new virtual disks in the VM with the **virt-install** command for provisioning new virtual machines.
  - Use **virtio** drivers for disk and network devices.
  - We recommend that you don't set the **current\_memory** option. If necessary, set it equal to the RAM provisioned to the gateway in the **--ram** parameter.

Following is an example **virt-install** command for installing KVM.

```
virt-install --name "SGW_KVM" --description "SGW KVM" --os-type=generic --  
ram=32768 --vcpus=16 --disk path=fgw-kvm.qcow2,bus=virtio,size=80,sparse=false  
--disk path=fgw-kvm-cache.qcow2,bus=virtio,size=1024,sparse=false --network  
default,model=virtio --graphics none --import
```

**Note**

For VMware, Microsoft Hyper-V, and KVM, synchronizing the VM time with the host time is required for successful gateway activation. Make sure that your host clock is set to the correct time and synchronize it with a Network Time Protocol (NTP) server.

For information about deploying your gateway to an Amazon EC2 host, see [Deploy your gateway to an Amazon EC2 host \(p. 399\)](#).

## Choosing a Service Endpoint

You can activate your gateway using:

- A public service endpoint and have your gateway communicate with AWS storage services over the public internet.
- A Federal Information Processing Standards (FIPS) compliant public service endpoint and have your gateway communicate with AWS storage services over the public internet.
- A public service endpoint and have your gateway communicate with AWS storage services using a virtual private cloud (VPC) endpoint, which is private.

### Note

If you use a VPC endpoint, all VPC endpoint communication from your gateway to AWS services occurs through the public service endpoint using your VPC in AWS.

### To choose a service endpoint

1. For **Select service endpoint**, choose one of the following:

- To have your gateway access AWS services over the public internet using a public service endpoint, choose **Public**.
- To have your gateway access AWS services over the public internet using a public service endpoint that complies with FIPS, choose **FIPS**.

If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

- To have your gateway access AWS services over a private VPC endpoint connection using a public service endpoint, choose **VPC**.

### Note

The FIPS service endpoint is only available in some AWS Regions. For more information, see [Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.

This procedure assumes that you are activating your gateway with a public endpoint. For information about how to activate a gateway using a VPC endpoint, see [Activating a gateway in a virtual private cloud \(p. 153\)](#).

2. Choose **Next** to connect and activate your gateway.

## Connecting to Your Gateway

To connect to your gateway, first get the IP address or activation key of your gateway VM. You use the IP address or activation key to activate your gateway. For gateways deployed and activated on an on-premises host, you can get the IP address or activation key from your gateway VM local console or your hypervisor client. For gateways deployed and activated on an Amazon EC2 instance, you can get the IP address or activation key from the Amazon EC2 console.

The activation process associates your gateway with your AWS account. Your gateway VM must be running for activation to succeed.

**Note**

Make sure that you select the correct gateway type. The .ova files and Amazon Machine Images (AMIs) for the gateway types are different and are not interchangeable.

**To get the IP address or activation key for your gateway VM from the local console**

1. Log on to your gateway VM local console. For detailed instructions, see the following:
  - VMware ESXi – [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. Get the IP address from the top of the menu page, and note it for later use.

**To get the IP address or activation key from an EC2 instance**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then choose the EC2 instance.
3. Choose the **Details** tab at the bottom, and then note the IP address or activation key. You use one of these to activate the gateway.

**Note**

For activation with an IP address, you can use the public or private IP address assigned to a gateway. You must be able to reach the IP address that you use from the browser from which you perform the activation.

**To associate your gateway with your AWS account**

1. For **Connect to gateway**, choose one of the following:
  - **IP address**
  - **Activation key**
2. Enter the IP address or activation key of your gateway, and then choose **Next**.

For detailed information about how to get a gateway IP address, see [Connecting to Your Gateway \(p. 440\)](#).

## Activating Your Gateway

The following, shown on the activation page, are the gateway settings that you selected. The activation page appears after you associate your gateway with your Amazon Web Services account, as described preceding.

- **Gateway type** specifies the type of gateway that you are activating.
- **Endpoint type** specifies the type of endpoint that you selected for your gateway.
- **AWS Region** specifies the AWS Region where your gateway will be activated and where your data will be stored. If **Endpoint type** is **VPC**, the AWS Region should be same as the Region where your VPC endpoint is located.

**To activate your gateway**

1. In **Activate gateway**, do the following:
  - For **Gateway time zone**, select a time zone to use for your gateway.

- For **Gateway name**, enter a name to identify your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.

**Note**

The gateway name must be between 2 and 255 characters in length.

- For **Backup application**, select the backup application you want to use. Storage Gateway automatically chooses a compatible medium changer for your backup application. If your backup application is not listed, choose **Other** and choose a medium changer type. **Medium changer type** specifies the type of medium changer to use for your backup application. For a list of available backup applications, see [Backup applications \(p. 89\)](#).

The type of medium changer you choose depends on the backup application you plan to use. The following table lists third-party backup applications that have been tested and found to be compatible with tape gateways. This table includes the medium changer type recommended for each backup application.

**Tape drive type** specifies the type of tape drive used by this gateway.

2. (Optional) For **Add tags**, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

If activation isn't successful, see [Troubleshooting your gateway \(p. 360\)](#) for possible solutions.

## Backup applications

The type of medium changer you choose depends on the backup application you plan to use. The following table lists third-party backup applications that have been tested and found to be compatible with tape gateways. This table includes the medium changer type recommended for each backup application.

Backup Application	Medium Changer Type
Arcserve Backup	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL or STK-L700
Commvault V11	STK-L700
Dell EMC NetWorker 19.5	AWS-Gateway-VTL
IBM Spectrum Protect v8.1.10	IBM-03584L32-0402
Micro Focus (HPE) Data Protector 9.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 or 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/Network 6.4 or 7.1	STK-L700
Quest NetVault Backup 12.4 or 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014 or 15 or 16 or 20.x	AWS-Gateway-VTL
Veritas Backup Exec 2012	STK-L700

Backup Application	Medium Changer Type
<b>Note</b> Veritas has ended support for Backup Exec 2012.	
Veritas NetBackup Version 7.x or 8.x	AWS-Gateway-VTL

**Important**

We highly recommend that you choose the medium changer that's listed for your backup application. Other medium changers might not function properly. You can choose a different medium changer after the gateway is activated. For more information, see [Selecting a Medium Changer After Gateway Activation \(p. 408\)](#).

## Configuring Local Disks

When you deployed the VM, you allocated local disks for your gateway. Now you configure your gateway to use these disks.

**Note**

If you allocate local disks on a VMware host, make sure to configure the disks to use paravirtualized disk controllers.

When adding a cache or upload buffer to an existing gateway, make sure to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

### To configure local disks

1. For **Configure local disks**, identify the disks you allocated and decide which ones you want to use for an upload buffer and cached storage. For information about disk size quotas, see [Recommended local disk sizes for your gateway \(p. 445\)](#).
2. For **Allocated to**, choose **Upload buffer** for the disk you want to configure as upload buffer.
3. Choose **Cache** for the disk you want to configure as cache storage.  
  
If you don't see your disks, choose **Refresh**.
4. Choose **Save and continue** to save your configuration settings.

## Configuring Amazon CloudWatch Logging

To notify you about the health of your tape gateway and its resources, you can configure an Amazon CloudWatch log group. For more information, see [Getting Tape Gateway Health Logs with CloudWatch Log Groups \(p. 247\)](#).

### To configure a CloudWatch log group for your file gateway

1. For **Configure logging - optional**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.
  - **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.

Choose a log group from the **Existing log group list**.

2. Choose **Save and continue** to save your configuration settings.

## Verifying VMware High Availability (VMware HA Clusters Only)

If your gateway is not deployed on a VMware host that is enabled for VMware High Availability (HA), you can skip this section.

If your gateway is deployed on a VMware host that is enabled for VMware High Availability (HA) cluster, you can either test the configuration when activating the gateway or after your gateway is activated. The following instructions show you how to test the configuration during activation.

### To test for VMware HA

1. For **Verify VMware High Availability configuration**, choose **Next**. Verification can take up to two minutes to complete.

If the test is successful, a message that indicates a successful test is displayed in the banner. If the test fails, a failed message is displayed. You can make changes in your vSphere configuration and repeat the test.

2. To repeat the test, on the **Gateways** dashboard, choose your gateway, and then for **Actions**, choose **Verify VMware High Availability**.

For information about how to configure your gateway for VMware HA, see [Using VMware vSphere High Availability with Storage Gateway \(p. 329\)](#).

### Next Step

[Creating Tapes \(p. 93\)](#)

## Creating a Custom Tape Pool

In this section, you can find information about how to create a new custom tape pool in AWS Storage Gateway.

### Topics

- [Choosing a Tape Pool Type \(p. 91\)](#)
- [Using Tape Retention Lock \(p. 92\)](#)
- [Creating a Custom Tape Pool \(p. 92\)](#)

## Choosing a Tape Pool Type

Storage Gateway uses tape pools to determine the storage class that you want tapes to be archived when they are ejected. Storage Gateway provides two standard tape pools:

**Glacier Pool**—archives the tape in GLACIER. When your backup software ejects the tape, it is automatically archived in GLACIER. You use GLACIER for more active archives where you can retrieve the tapes typically within 3-5 hours. For more information, see [What Is Amazon S3 Glacier?](#)

**Deep Archive Pool**—archives the tape in DEEP\_ARCHIVE. When your backup software ejects the tape, the tape is automatically archived in DEEP\_ARCHIVE. You use DEEP\_ARCHIVE for long-term data retention and digital preservation where data is accessed once or twice a year. You can retrieve tapes archived in DEEP\_ARCHIVE typically within 12 hours. For detailed information, see [Storage classes for archiving objects](#).

If you archive a tape in GLACIER, you can move it to DEEP\_ARCHIVE later. For more information, see [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#).

Storage Gateway also supports creation of custom tape pools, which allow you to enable tape retention lock to prevent archived tapes from being deleted or moved to another pool for a fixed amount of time,

up to 100 years. This includes locking permission controls on who can delete tapes or modify retention settings.

## Using Tape Retention Lock

With tape retention lock, you can lock archived tapes. Tape retention lock is an option for tapes in a custom tape pool. Tapes that have tape retention lock enabled can't be deleted or moved to another pool for a fixed amount of time, up to 100 years.

You can configure tape retention lock in one of two modes:

- **Governance mode:** When configured in governance mode, only AWS Identity and Access Management (IAM) users with the permissions to perform `storagegateway:BypassGovernanceRetention` can remove tapes from the pool. If you're using the API to remove the tape, you must also set `BypassGovernanceRetention` to true.
- **Compliance mode:** When configured in compliance mode, the protection cannot be removed by any user, including the root Amazon Web Services account.

When a tape is locked in compliance mode, its retention lock type can't be changed, and its retention period can't be shortened. Compliance lock type helps ensure that a tape can't be overwritten or deleted for the duration of the retention period.

### Note

A custom pool's configuration cannot be changed after it is created.

Tape retention lock can be enabled when you create a custom tape pool. Any new tapes that are attached to a custom pool inherit the retention lock type, period, and storage class for that pool.

You can also enable tape retention lock on tapes that were archived before the release of this feature by moving tapes between the default pool and a custom pool that you create. If the tape is archived, the tape retention lock is effective immediately.

### Note

If you are moving archived tapes between the Glacier and Deep Archive storage classes, you are charged a fee for moving a tape. There is no additional charge to move a tape from a default pool to a custom pool if the storage class remains the same.

## Creating a Custom Tape Pool

Use the following steps to create a custom tape pool using the console.

### To create a custom tape pool

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose the **Tape Library** tab, and then choose the **Pools** tab.
3. Choose **Create pool** to open the **Create pool** pane.
4. For **Name**, enter a unique name to identify your custom tape pool. The pool name must be between 2 and 100 characters long.
5. For **Storage class**, choose **Glacier** or **Glacier Deep Archive**.
6. For **Retention lock type**, choose **None**, **Compliance**, or **Governance**.

### Note

If you choose **Compliance**, tape retention lock cannot be removed by any user, including the root Amazon Web Services account.

7. If you choose a tape retention lock type, enter the **Retention period** in days. The maximum retention period is 36,500 days (100 years).

8. (Optional) For **Tags**, choose **Add new tag** to add a tag to your custom tape pool. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your custom tape pools.  
Enter a **Key**, and optionally, a **Value** for your tag. You can add up to 50 tags to the tape pool
9. Choose **Create pool** to create your new custom tape pool.

## Creating Tapes

In this section, you can find information about how to create new virtual tapes using AWS Storage Gateway. You can create new virtual tapes manually with the AWS Storage Gateway console, and you can also create them automatically.

Storage Gateway automates creating new virtual tapes, helping decrease the need for manual tape management, and making your large deployments simpler. Automatic tape creation also helps scale on-premises and archive storage needs.

Storage Gateway supports *write once, read many* (WORM) and *tape retention lock* on virtual tapes. WORM-enabled virtual tapes help ensure that the data on active tapes in your virtual tape library cannot be overwritten or erased. For more information about WORM protection for virtual tapes, see the section following, [the section called "WORM Tape Protection" \(p. 93\)](#).

With tape retention lock, you can specify the retention mode and period on archived virtual tapes, preventing them from being deleted for a fixed amount of time up to 100 years. It includes permission controls on who can delete tapes or modify the retention settings. For more information about tape retention lock, see [the section called "Tape Retention Lock" \(p. 92\)](#).

### Note

You are charged only for the amount of data that you write to the tape, not the tape capacity. You can use AWS Key Management Service (AWS KMS) to encrypt data written to a virtual tape that is stored in Amazon Simple Storage Service (Amazon S3). Currently, you can do this by using the AWS Storage Gateway API Reference. For more information, see [CreateTapes](#) or [create-tapes](#).

### Topics

- [Write Once, Read Many \(WORM\) Tape Protection \(p. 93\)](#)
- [Creating Tapes Manually \(p. 93\)](#)
- [Creating Tapes Automatically \(p. 94\)](#)

## Write Once, Read Many (WORM) Tape Protection

You can prevent virtual tapes from being overwritten or erased by enabling WORM protection for virtual tapes in AWS Storage Gateway. WORM protection for virtual tapes is enabled when creating tapes.

Data that is written to WORM virtual tapes can't be overwritten. Only new data can be appended to WORM virtual tapes, and existing data can't be erased. Enabling WORM protection for virtual tapes helps protect those tapes while they are in active use, before they are ejected and archived.

WORM configuration can only be set when tapes are created, and that configuration cannot be changed after the tapes are created.

## Creating Tapes Manually

Use the following steps to create virtual tapes manually using the console.

### To create virtual tapes manually

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.

2. In the navigation pane, choose the **Gateways** tab.
3. Choose **Create tapes** to open the **Create tapes** pane.
4. For **Gateway**, choose a gateway. The tape is created for this gateway.
5. For **Tape type**, choose **Standard** to create standard virtual tapes. Choose **WORM** to create *write once read many* (WORM) virtual tapes.
6. For **Number of tapes**, choose the number of tapes that you want to create. For more information about tape quotas, see [AWS Storage Gateway quotas \(p. 444\)](#).
7. For **Capacity**, enter the size of the virtual tape that you want to create. Tapes must be larger than 100 GiB. For information about capacity quotas, see [AWS Storage Gateway quotas \(p. 444\)](#).
8. For **Barcode prefix**, enter the prefix that you want to prepend to the barcode of your virtual tapes.

**Note**

Virtual tapes are uniquely identified by a barcode, and you can add a prefix to the barcode. You can use a prefix to help identify your virtual tapes. The prefix must be uppercase letters (A–Z) and must be one to four characters long.

9. For **Pool**, choose **Glacier Pool**, **Deep Archive Pool**, or a custom pool that you have created. The pool determines the storage class in which your tape is stored when it is ejected by your backup software.
  - Choose **Glacier Pool** if you want to archive the tape in GLACIER. When your backup software ejects the tape, it is automatically archived in GLACIER. You use GLACIER for more active archives where you can retrieve a tape typically within 3–5 hours. For more information, see [Storage classes for archiving objects](#) in the *Amazon S3 Developer Guide*.
  - Choose **Deep Archive Pool** if you want to archive the tape in DEEP\_ARCHIVE. When your backup software ejects the tape, the tape is automatically archived in DEEP\_ARCHIVE. You use DEEP\_ARCHIVE for long-term data retention and digital preservation where data is accessed once or twice a year. You can retrieve a tape archived in DEEP\_ARCHIVE typically within 12 hours. For more information, see [Storage classes for archiving objects](#) in the *Amazon S3 Developer Guide*.
  - Choose a custom pool, if any are available. You configure custom tape pools to use either **Deep Archive Pool** or **Glacier Pool**. Tapes are archived to the configured storage class when they are ejected by your backup software.

If you archive a tape in GLACIER, you can move it to DEEP\_ARCHIVE later. For more information, see [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#).

**Note**

Tapes created before March 27, 2019, are archived directly in Amazon S3 Glacier when your backup software ejects it.

10. (Optional) For **Tags**, choose **Add new tag** and enter a key and value to add tags to your tape. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your tapes.
11. Choose **Create tapes**.
12. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.

The status of the virtual tapes is initially set to **CREATING** when the virtual tapes are being created. After the tapes are created, their status changes to **AVAILABLE**. For more information, see [Managing Your Tape Gateway \(p. 200\)](#).

## Creating Tapes Automatically

The tape gateway automatically creates new virtual tapes to maintain the minimum number of available tapes that you configure. It then makes these new tapes available for import by the backup application

so that your backup jobs can run without interruption. Automatic tape creation removes the need for custom scripting in addition to the manual process of creating new virtual tapes.

The tape gateway spawns a new tape automatically when it has fewer tapes than the minimum number of available tapes specified for automatic tape creation. A new tape is spawned when:

- A tape is imported from an import/export slot.
- A tape is imported to the tape drive.

The gateway maintains a minimum number of tapes with the barcode prefix specified in the automatic tape creation policy. If there are fewer tapes than the minimum number of tapes with the barcode prefix, the gateway automatically creates enough new tapes to equal the minimum number of tapes specified in the automatic tape creation policy.

When you eject a tape and it goes into the import/export slot, that tape does not count toward the minimum number of tapes specified in your automatic tape creation policy. Only tapes in the import/export slot are counted as being "available." Exporting a tape does not trigger automatic tape creation. Only imports affect the number of available tapes.

Moving a tape from the import/export slot to a tape drive or storage slot reduces the number of tapes in the import/export slot with the same barcode prefix. The gateway creates new tapes to maintain the minimum number of available tapes for that barcode prefix.

### To enable automatic tape creation

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose the **Gateways** tab.
3. Choose the gateway that you want to automatically create tapes for.
4. In the **Actions** menu, choose **Configure tape auto-create**.

The **Tape auto-create** page appears. You can add, change, or remove tape auto-create options here.

5. To enable automatic tape creation, choose **Add new item** then configure the settings for automatic tape creation.
6. For **Tape type**, choose **Standard** to create standard virtual tapes. Choose **WORM** to create *write-once-read-many* (WORM) virtual tapes.
7. For **Minimum number of tapes**, enter the minimum number of virtual tapes that should be available on the tape gateway at all times. The valid range for this value is a minimum of 1 and a maximum of 10.
8. For **Capacity**, enter the size, in bytes, of the virtual tape capacity. The valid range is a minimum of 100 GiB and a maximum of 5 TiB.
9. For **Barcode prefix**, enter the prefix that you want to prepend to the barcode of your virtual tapes.

#### Note

Virtual tapes are uniquely identified by a barcode, and you can add a prefix to the barcode.

The prefix is optional, but you can use it to help identify your virtual tapes. The prefix must be uppercase letters (A–Z) and must be one to four characters long.

10. For **Pool**, choose **Glacier Pool**, **Deep Archive Pool**, or a custom pool that you have created. The pool determines the storage class in which your tape is stored when it is ejected by your backup software.
  - Choose **Glacier Pool** if you want to archive the tape in GLACIER. When your backup software ejects the tape, it is automatically archived in GLACIER. You use S3 Glacier for more active archives where you can retrieve a tape typically within 3–5 hours. For detailed information, see [Storage classes for archiving objects](#) in the *Amazon S3 Developer Guide*.
  - Choose **Deep Archive Pool** if you want to archive the tape in DEEP\_ARCHIVE. When your backup software ejects the tape, the tape is automatically archived in DEEP\_ARCHIVE. You use

DEEP\_ARCHIVE for long-term data retention and digital preservation where data is accessed once or twice a year. You can retrieve a tape archived in DEEP\_ARCHIVE typically within 12 hours. For detailed information, see [Storage classes for archiving objects](#) in the *Amazon S3 Developer Guide*.

- Choose a custom pool, if any are available. You configure custom tape pools to use either **Deep Archive Pool** or **Glacier Pool**. Tapes are archived to the configured storage class when they are ejected by your backup software.

If you archive a tape in GLACIER, you can move it to DEEP\_ARCHIVE later. For more information, see [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#).

**Note**

Tapes created before March 27, 2019, are archived directly in Amazon S3 Glacier when your backup software ejects it.

11. When finished configuring settings, choose **Save changes**.
12. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.

The status of available virtual tapes is initially set to **CREATING** when the tapes are being created. After the tapes are created, their status changes to **AVAILABLE**. For more information, see [Managing Your Tape Gateway \(p. 200\)](#).

For more information about changing automatic tape creation policies, or deleting automatic tape creation from a tape gateway, see [Managing Automatic Tape Creation \(p. 201\)](#).

**Next Step**

[Using Your Tape Gateway \(p. 96\)](#)

## Using Your Tape Gateway

Following, you can find instructions about how to use your tape gateway.

**Topics**

- [Connecting Your VTL Devices \(p. 96\)](#)
- [Using Your Backup Software to Test Your Gateway Setup \(p. 99\)](#)
- [Where Do I Go from Here? \(p. 148\)](#)

## Connecting Your VTL Devices

Following, you can find instructions about how to connect your virtual tape library (VTL) devices to your Microsoft Windows or Red Hat Enterprise Linux (RHEL) client.

**Topics**

- [Connecting to a Microsoft Windows Client \(p. 96\)](#)
- [Connecting to a Linux Client \(p. 97\)](#)

## Connecting to a Microsoft Windows Client

The following procedure shows a summary of the steps that you follow to connect to a Windows client.

## To connect your VTL devices to a Windows client

1. Start `iscsicpl.exe`.

### Note

You must have administrator rights on the client computer to run the iSCSI initiator.

2. Start the Microsoft iSCSI initiator service.
3. In the **iSCSI Initiator Properties** dialog box, choose the **Discovery** tab, and then choose **Discover Portal**.
4. Provide the IP address of your tape gateway for **IP address or DNS name**.
5. Choose the **Targets** tab, and then choose **Refresh**. All 10 tape drives and the medium changer appear in the **Discovered targets** box. The status for the targets is **Inactive**.
6. Choose the first device and connect it. You connect the devices one at a time.
7. Connect all of the targets.

On a Windows client, the driver provider for the tape drive must be Microsoft. Use the following procedure to verify the driver provider, and update the driver and provider if necessary:

## To verify and update the driver and provider

1. On your Windows client, start Device Manager.
2. Expand **Tape drives**, open the context (right-click) menu for a tape drive, and choose **Properties**.
3. In the **Driver** tab of the **Device Properties** dialog box, verify **Driver Provider** is Microsoft.
4. If **Driver Provider** is not Microsoft, set the value as follows:
  - a. Choose **Update Driver**.
  - b. In the **Update Driver Software** dialog box, choose **Browse my computer for driver software**.
  - c. In the **Update Driver Software** dialog box, choose **Let me pick from a list of device drivers on my computer**.
  - d. Choose **LTO Tape drive** and choose **Next**.
5. Choose **Close** to close the **Update Driver Software** window, and verify that the **Driver Provider** value is now set to Microsoft.
6. Repeat the steps to update driver and provider for all the tape drives.

## Connecting to a Linux Client

The following procedure shows a summary of the steps that you follow to connect to an RHEL client.

## To connect a Linux client to VTL devices

1. Install the `iscsi-initiator-utils` RPM package.

You can use the following command to install the package.

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

2. Make sure that the iSCSI daemon is running.

For RHEL 5 or 6, use the following command.

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

For RHEL 7, use the following command.

```
sudo service iscsid status
```

3. Discover the volume or VTL device targets defined for a gateway. Use the following discovery command.

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

The output of the discovery command looks like the following example output.

For volume gateways: [GATEWAY\_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume

For tape gateways: iqn.1997-05.com.amazon:[GATEWAY\_IP]-tapedrive-01

4. Connect to a target.

Be sure to specify the correct [GATEWAY\_IP] and IQN in the connect command.

Use the following command.

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

5. Verify that the volume is attached to the client machine (the initiator). To do so, use the following command.

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

The output of the command should look like the following example output.

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

For volume gateways, we highly recommend that after you set up your initiator, you customize your iSCSI settings as discussed in [Customizing Your Linux iSCSI Settings \(p. 428\)](#).

Verify that the VTL device is attached to the client machine (the initiator). To do so, use the following command.

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

The output of the command should look like the following example output.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
```

```
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x00000000000000001c-lun-0 -
> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x00000000000000001c-lun-0-nst
-> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x00000000000000001f-lun-0 -
> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x00000000000000001f-lun-0-nst
-> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000000022-lun-0 -
> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000000022-lun-0-nst
-> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000000025-lun-0 -
> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000000025-lun-0-nst
-> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000000028-lun-0 -
> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000000028-lun-0-nst
-> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x00000000000000002b-lun-0 -
> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x00000000000000002b-lun-0-nst
-> ../../nst4
```

## Next Step

[Using Your Backup Software to Test Your Gateway Setup \(p. 99\)](#)

## Using Your Backup Software to Test Your Gateway Setup

You test your tape gateway setup by performing the following tasks using your backup application:

1. Configure the backup application to detect your storage devices.

**Note**

To improve I/O performance, we recommend setting the block size of the tape drives in your backup application to 1 MB. For more information, see [Use a Larger Block Size for Tape Drives \(p. 328\)](#).

2. Back up data to a tape.
3. Archive the tape.
4. Retrieve the tape from the archive.
5. Restore data from the tape.

To test your setup, use a compatible backup application, as described following.

**Note**

Unless otherwise stated, all backup applications were qualified on Microsoft Windows.

**Topics**

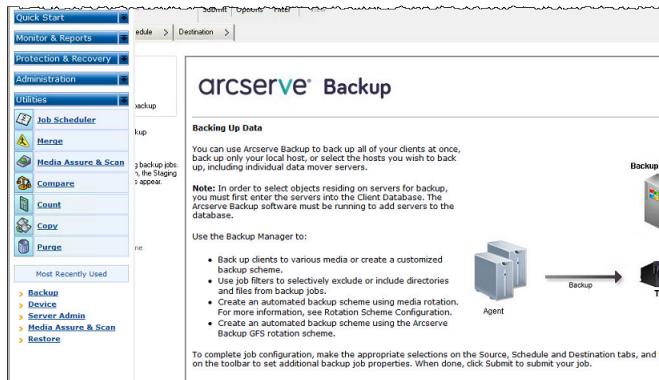
- [Testing Your Setup by Using Arcserve Backup r17.0 \(p. 100\)](#)
- [Testing Your Setup by Using Bacula Enterprise \(p. 103\)](#)
- [Testing Your Setup by Using Commvault \(p. 105\)](#)
- [Testing Your Setup by Using Dell EMC NetWorker \(p. 109\)](#)
- [Testing Your Setup by Using IBM Spectrum Protect \(p. 112\)](#)
- [Testing Your Setup by Using Micro Focus \(HPE\) Data Protector \(p. 114\)](#)
- [Testing Your Setup by Using Microsoft System Center Data Protection Manager \(p. 120\)](#)
- [Testing Your Setup by Using NovaStor DataCenter/Network \(p. 123\)](#)
- [Testing Your Setup by Using Quest NetVault Backup \(p. 127\)](#)
- [Testing Your Setup by Using Veeam Backup & Replication \(p. 130\)](#)
- [Testing Your Setup by Using Veritas Backup Exec \(p. 133\)](#)
- [Testing Your Setup by Using Veritas NetBackup \(p. 137\)](#)

For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

## Testing Your Setup by Using Arcserve Backup r17.0

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Arcserve Backup r17.0. In this topic, you can find basic documentation to configure Arcserve Backup with a tape gateway and perform a backup and restore operation. For detailed information about to use Arcserve Backup r17.0, see [Arcserve Backup r17 documentation](#) in the [Arcserve Administration Guide](#).

The following screenshot shows the Arcserve menus.



## Topics

- [Configuring Arcserve to Work with VTL Devices \(p. 101\)](#)
- [Loading Tapes into a Media Pool \(p. 101\)](#)
- [Backing Up Data to a Tape \(p. 102\)](#)
- [Archiving a Tape \(p. 102\)](#)
- [Restoring Data from a Tape \(p. 102\)](#)

## Configuring Arcserve to Work with VTL Devices

After you have connected your virtual tape library (VTL) devices to your client, you scan for your devices.

### To scan for VTL devices

1. In the Arcserve Backup Manager, choose the **Utilities** menu.
2. Choose **Media Assure and Scan**.

### Loading Tapes into a Media Pool

When the Arcserve software connects to your gateway and your tapes become available, Arcserve automatically loads your tapes. If your gateway is not found in the Arcserve software, try restarting the tape engine in Arcserve.

### To restart the tape engine

1. Choose **Quick Start**, choose **Administration**, and then choose **Device**.
2. On the navigation menu, open the context (right-click) menu for your gateway and choose an import/export slot.
3. Choose **Quick Import** and assign your tape to an empty slot.
4. Open the context (right-click) menu for your gateway and choose **Inventory/Offline Slots**.
5. Choose **Quick Inventory** to retrieve media information from the database.

If you add a new tape, you need to scan your gateway for the new tape to have it appear in Arcserve. If the new tapes don't appear, you must import the tapes.

### To import tapes

1. Choose the **Quick Start** menu, choose **Back up**, and then choose **Destination tap**.
2. Choose your gateway, open the context (right-click) menu for one tape, and then choose **Import/Export Slot**.

3. Open the context (right-click) menu for each new tape and choose **Inventory**.
4. Open the context (right-click) menu for each new tape and choose **Format**.

Each tape's barcode now appears in your Storage Gateway console, and each tape is ready to use.

### Backing Up Data to a Tape

When your tapes have been loaded into Arcserve, you can back up data. The backup process is the same as backing up physical tapes.

#### To back up data to a tape

1. From the **Quick Start** menu, open the restore a backup session.
2. Choose the **Source** tab, and then choose the file system or database system that you want to back up.
3. Choose the **Schedule** tab and choose the repeat method you want to use.
4. Choose the **Destination** tab and then choose the tape you want to use. If the data you are backing up is larger than the tape can hold, Arcserve prompts you to mount a new tape.
5. Choose **Submit** to back up your data.

### Archiving a Tape

When you archive a tape, your tape gateway moves the tape from the tape library to the offline storage. Before you eject and archive a tape, you might want to check the content on it.

#### To archive a tape

1. From the **Quick Start** menu, open the restore a backup session.
2. Choose the **Source** tab, and then choose the file system or database system you want to back up.
3. Choose the **Schedule** tab and choose the repeat method you want to use.
4. Choose your gateway, open the context (right-click) menu for one tape, and then choose **Import/Export Slot**.
5. Assign a mail slot to load the tape. The status in the Storage Gateway console changes to **Archive**. The archive process might take some time.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL but is archived in S3 Glacier or S3 Glacier Deep Archive.

### Restoring Data from a Tape

Restoring your archived data is a two-step process.

#### To restore data from an archived tape

1. Retrieve the archived tape to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use Arcserve to restore the data. This process is the same as restoring data from physical tapes. For instructions, see the [Arcserve Backup r17 documentation](#).

To restore data from a tape, use the following procedure.

#### To restore data from a tape

1. From the **Quick Start** menu, open the restore a restore session.

2. Choose the **Source** tab, and then choose the file system or database system you want to restore.
3. Choose the **Destination** tab and accept the default settings.
4. Choose the **Schedule** tab, choose the repeat method that you want to use, and then choose **Submit**.

### Next Step

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

## Testing Your Setup by Using Bacula Enterprise

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Bacula Enterprise version 10. In this topic, you can find basic documentation on how to configure the Bacula version 10 backup application for a tape gateway and perform backup and restore operations. For detailed information about how to use Bacula version 10, see [Bacula Systems Manuals and Documentation](#) or contact Bacula Systems.

#### Note

Bacula is only supported on Linux.

### Setting Up Bacula Enterprise

After you have connected your virtual tape library (VTL) devices to your Linux client, you configure the Bacula software to recognize your devices. For information about how to connect VTL devices to your client, see [Connecting Your VTL Devices \(p. 96\)](#).

#### To set up Bacula

1. Get a licensed copy of the Bacula Enterprise backup software from Bacula Systems.
2. Install the Bacula Enterprise software on your on-premises or in-cloud computer.

For information about how to get the installation software, see [Enterprise Backup for Amazon S3 and Storage Gateway](#). For additional installation guidance, see the Bacula whitepaper [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#).

### Configuring Bacula to Work with VTL Devices

Next, configure Bacula to work with your VTL devices. Following, you can find basic configuration steps.

#### To configure Bacula

1. Install the Bacula Director and the Bacula Storage daemon. For instructions, see chapter 7 of the [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula white paper.
2. Connect to the system that is running Bacula Director and configure the iSCSI initiator. To do so, use the script provided in step 7.4 in the [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula whitepaper.
3. Configure the storage devices. Use the script provided in the Bacula whitepaper discussed preceding.
4. Configure the local Bacula Director, add storage targets, and define media pools for your tapes. Use the script provided in the Bacula whitepaper discussed preceding.

### Backing Up Data to Tape

1. Create tapes in the Storage Gateway console. For information on how to create tapes, see [Creating Tapes \(p. 93\)](#).
2. Transfer tapes from the I/E slot to the storage slot by using the following command.

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

For example, the following command transfers tapes from I/E slot 1601 to storage slot 1.

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

3. Launch the Bacula console by using the following command.

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

**Note**

When you create and transfer a tape to Bacula, use the Bacula console (bconsole) command update slots storage=VTL so that Bacula knows about the new tapes that you created.

4. Label the tape with the barcode as the volume name or label by using the following bconsole command.

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

5. Mount the tape by using the following command.

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

6. Create a backup job that uses the media pools you created, and then write data to the virtual tape by using the same procedures that you do with physical tapes.

7. Unmount the tape from the Bacula console by using the following command.

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

## Archiving a Tape

When all backup jobs for a particular tape are done and you can archive the tape, use the mtx-changer script to move the tape from the storage slot to the I/E slot. This action is similar to the eject action in other backup applications.

### To archive a tape

1. Transfer the tape from the storage slot to the I/E slot by using the /opt/bacula/scripts/mtx-changer command.

For example, the following command transfers a tape from the storage slot 1 to I/E slot 1601.

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

2. Verify that the tape is archived in the offline storage (GLACIER or DEEP\_ARCHIVE) and that the tape has the status **Archived**.

## Restoring Data from an Archived and Retrieved Tape

Restoring your archived data is a two-step process.

### To restore data from an archived tape

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Restore your data by using the Bacula software:

- a. Import the tapes into the storage slot by using the /opt/bacula/scripts/mtx-changer command to transfer tapes from the I/E slot.

For example, the following command transfers tapes from I/E slot 1601 to storage slot 1.

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

- b. Use the Bacula console to update the slots, and then mount the tape.
- c. Run the restore command to restore your data. For instructions, see the Bacula documentation.

## Testing Your Setup by Using Commvault

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Commvault version 11. In this topic, you can find basic documentation on how to configure the Commvault backup application for a tape gateway, perform a backup archive, and retrieve your data from archived tapes. For detailed information about how to use Commvault, see the [Commvault documentation](#) on the Commvault website.

### Topics

- [Configuring Commvault to Work with VTL Devices \(p. 105\)](#)
- [Creating a Storage Policy and a Subclient \(p. 106\)](#)
- [Backing Up Data to a Tape in Commvault \(p. 107\)](#)
- [Archiving a Tape in Commvault \(p. 107\)](#)
- [Restoring Data from a Tape \(p. 108\)](#)

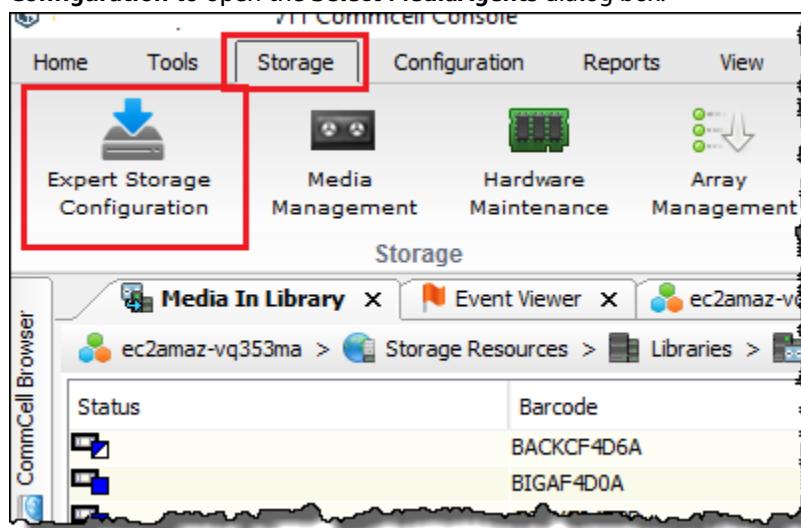
### Configuring Commvault to Work with VTL Devices

After you connect the VTL devices to the Windows client, you configure Commvault to recognize them. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices to a Windows client \(p. 418\)](#).

The Commvault backup application doesn't automatically recognize VTL devices. You must manually add devices to expose them to the Commvault backup application and then discover the devices.

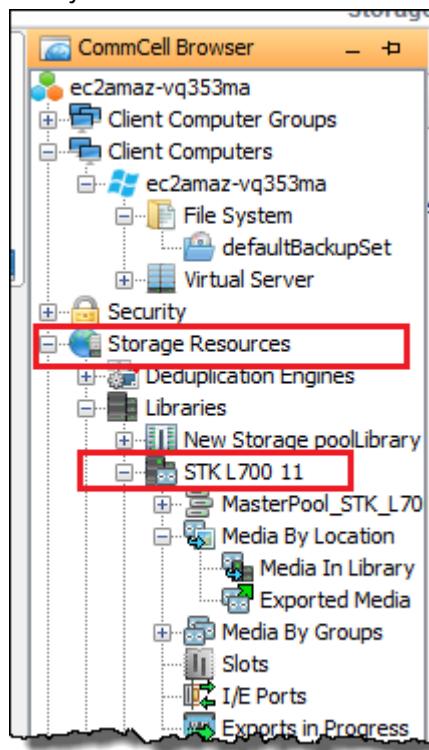
### To configure Commvault

1. In the CommCell console main menu, choose **Storage**, and then choose **Expert Storage Configuration** to open the **Select MediaAgents** dialog box.



2. Choose the available media agent you want to use, choose **Add**, and then choose **OK**.
3. In the **Expert Storage Configuration** dialog box, choose **Start**, and then choose **Detect/Configure Devices**.

4. Leave the **Device Type** options selected, choose **Exhaustive Detection**, and then choose **OK**.
5. In the **Confirm Exhaustive Detection** confirmation box, choose **Yes**.
6. In the **Device Selection** dialog box, choose your library and all its drives, and then choose **OK**. Wait for your devices to be detected, and then choose **Close** to close the log report.
7. Right-click your library, choose **Configure**, and then choose **Yes**. Close the configuration dialog box.
8. In the **Does this library have a barcode reader?** dialog box, choose **Yes**, and then for device type, choose **IBM ULTRIUM V5**.
9. In the CommCell browser, choose **Storage Resources**, and then choose **Libraries** to see your tape library.



10. To see your tapes in your library, open the context (right-click) menu for your library, and then choose **Discover Media**, **Media location**, **Media Library**.
11. To mount your tapes, open the context (right-click) menu for your media, and then choose **Load**.

### Creating a Storage Policy and a Subclient

Every backup and restore job is associated with a storage policy and a subclient policy.

A storage policy maps the original location of the data to your media.

#### To create a storage policy

1. In the CommCell browser, choose **Policies**.
2. Open the context (right-click) menu for **Storage Policies**, and then choose **New Storage Policy**.
3. In the Create Storage Policy wizard, choose **Data Protection and Archiving**, and then choose **Next**.
4. Type a name for **Storage Policy Name**, and then choose **Incremental Storage Policy**. To associate this storage policy with incremental loads, choose one of the options. Otherwise, leave the options unchecked, and then choose **Next**.

5. In the **Do you want to Use Global Deduplication Policy?** dialog box, choose your **Deduplication** preference, and then choose **Next**.
6. From **Library for Primary Copy**, choose your VTL library, and then choose **Next**.
7. Verify that your media agent settings are correct, and then choose **Next**.
8. Verify that your scratch pool settings are correct, and then choose **Next**.
9. Configure your retention policies in **iData Agent Backup data**, and then choose **Next**.
10. Review the encryption settings, and then choose **Next**.
11. To see your storage policy, choose **Storage Policies**.

You create a subclient policy and associate it with your storage policy. A subclient policy enables you to configure similar file system clients from a central template, so that you don't have to set up many similar file systems manually.

#### To create a subclient policy

1. In the CommCell browser, choose **Client Computers**, and then choose your client computer. Choose **File System**, and then choose **defaultBackupSet**.
2. Right-click **defaultBackupSet**, choose **All Tasks**, and then choose **New Subclient**.
3. In the **Subclient** properties box, type a name in **SubClient Name**, and then choose **OK**.
4. Choose **Browse**, navigate to the files that you want to back up, choose **Add**, and then close the dialog box.
5. In the **Subclient** property box, choose the **Storage Device** tab, choose a storage policy from **Storage policy**, and then choose **OK**.
6. In the **Backup Schedule** window that appears, associate the new subclient with a backup schedule.
7. Choose **Do Not Schedule** for one time or on-demand backups, and then choose **OK**.

You should now see your subclient in the **defaultBackupSet** tab.

#### Backing Up Data to a Tape in Commvault

You create a backup job and write data to a virtual tape by using the same procedures you use with physical tapes. For detailed information about how to back up data, see the [Commvault documentation](#).

#### Archiving a Tape in Commvault

You start the archiving process by ejecting the tape. When you archive a tape, tape gateway moves the tape from the tape library to offline storage. Before you eject and archive a tape, you might want to first check the content on the tape.

#### To archive a tape

1. In the CommCell browser, choose **Storage Resources, Libraries**, and then choose **Your library**. Choose **Media By Location**, and then choose **Media In Library**.
2. Open the context (right-click) menu for the tape you want to archive, choose **All Tasks**, choose **Export**, and then choose **OK**.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL.

In the Commvault software, verify that the tape is no longer in the storage slot.

In the navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your archived tape's status is **ARCHIVED**.

## Restoring Data from a Tape

You can restore data from a tape that has never been archived and retrieved, or from a tape that has been archived and retrieved. For tapes that have never been archived and retrieved (nonretrieved tapes), you have two options to restore the data:

- Restore by subclient
- Restore by job ID

### To restore data from a nonretrieved tape by subclient

1. In the CommCell browser, choose **Client Computers**, and then choose your client computer. Choose **File System**, and then choose **defaultBackupSet**.
2. Open the context (right-click) menu for your subclient, choose **Browse and Restore**, and then choose **View Content**.
3. Choose the files you want to restore, and then choose **Recover All Selected**.
4. Choose **Home**, and then choose **Job Controller** to monitor the status of your restore job.

### To restore data from a nonretrieved tape by job ID

1. In the CommCell browser, choose **Client Computers**, and then choose your client computer. Right-click **File System**, choose **View**, and then choose **Backup History**.
2. In the **Backup Type** category, choose the type of backup jobs you want, and then choose **OK**. A tab with the history of backup jobs appears.
3. Find the **Job ID** you want to restore, right-click it, and then choose **Browse and Restore**.
4. In the **Browse and Restore Options** dialog box, choose **View Content**.
5. Choose the files that you want to restore, and then choose **Recover All Selected**.
6. Choose **Home**, and then choose **Job Controller** to monitor the status of your restore job.

### To restore data from an archived and retrieved tape

1. In the CommCell browser, choose **Storage Resources**, choose **Libraries**, and then choose **Your library**. Choose **Media By Location**, and then choose **Media In Library**.
2. Right-click the retrieved tape, choose **All Tasks**, and then choose **Catalog**.
3. In the **Catalog Media** dialog box, choose **Catalog only**, and then choose **OK**.
4. Choose **CommCell Home**, and then choose **Job Controller** to monitor the status of your restore job.
5. After the job succeeds, open the context (right-click) menu for your tape, choose **View**, and then choose **View Catalog Contents**. Take note of the **Job ID** value for use later.
6. Choose **Recatalog/Merge**. Make sure that **Merge only** is chosen in the **Catalog Media** dialog box.
7. Choose **Home**, and then choose **Job Controller** to monitor the status of your restore job.
8. After the job succeeds, choose **CommCell Home**, choose **Control Panel**, and then choose **Browse/Search/Recovery**.
9. Choose **Show aged data during browse and recovery**, choose **OK**, and then close the **Control Panel**.
10. In the CommCell browser, right-click **Client Computers**, and then choose your client computer. Choose **View**, and then choose **Job History**.
11. In the **Job History Filter** dialog box, choose **Advanced**.
12. Choose **Include Aged Data**, and then choose **OK**.
13. In the **Job History** dialog box, choose **OK** to open the **history of jobs** tab.

14. Find the job that you want to restore, open the context (right-click) menu for it, and then choose **Browse and Restore**.
15. In the **Browse and Restore** dialog box, choose **View Content**.
16. Choose the files that you want to restore, and then choose **Recover All Selected**.
17. Choose **Home**, and then choose **Job Controller** to monitor the status of your restore job.

## Testing Your Setup by Using Dell EMC NetWorker

You can back up your data to virtual tapes, archive the tapes and manage your virtual tape library (VTL) devices by using Dell EMC NetWorker 19.5. In this topic, you can find basic documentation on how to configure the Dell EMC NetWorker software to work with a tape gateway and perform a backup, including how to configure storage devices, write data to a tape, archive a tape and restore data from a tape.

For detailed information about how to install and use the Dell EMC NetWorker software, see the [Administration Guide](#).

For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

### Topics

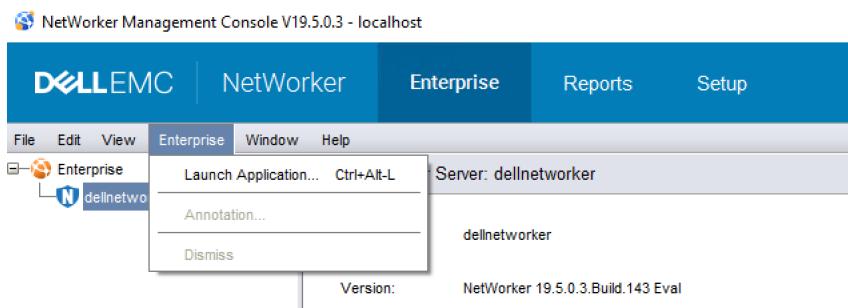
- [Configuring to Work with VTL Devices \(p. 109\)](#)
- [Enabling Import of WORM Tapes into Dell EMC NetWorker \(p. 111\)](#)
- [Backing Up Data to a Tape in Dell EMC NetWorker \(p. 111\)](#)
- [Archiving a Tape in Dell EMC NetWorker \(p. 112\)](#)
- [Restoring Data from an Archived Tape in Dell EMC NetWorker \(p. 112\)](#)

### Configuring to Work with VTL Devices

After you have connected your virtual tape library (VTL) devices to your Microsoft Windows client, you configure to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

doesn't automatically recognize tape gateway devices. To expose your VTL devices to the NetWorker software and get the software to discover them, you manually configure the software. Following, we assume that you have correctly installed the software and that you are familiar with the Management Console. For more information about the Management Console, see the NetWorker Management Console interface section of the [Dell EMC NetWorker Administration Guide](#).

The following screenshot shows Dell EMC NetWorker 19.5.



### To configure the Dell EMC NetWorker software for VTL devices

1. Start the Dell EMC NetWorker Management Console application, choose **Enterprise** from the menu, and then choose **localhost** from the left pane.

2. Open the context (right-click) menu for **localhost**, and then choose **Launch Application**.
3. Choose the **Devices** tab, open the context (right-click) menu for **Libraries**, and then choose **Scan for Devices**.
4. In the Scan for Devices wizard, choose **Start Scan**, and then choose **OK** from the dialog box that appears.
5. Expand the **Libraries** folder tree to see all your libraries and hit F5 to refresh. This process might take a few seconds to load the devices into the library.
6. Open a command window (CMD.exe) with admin privileges and run "jbconfig" utility that is installed with Dell EMC NetWorker 19.5.

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

C:\Users\Administrator>jbconfig

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

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

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

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

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

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

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

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

Jukebox has been added successfully

The following configuration options have been set:

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

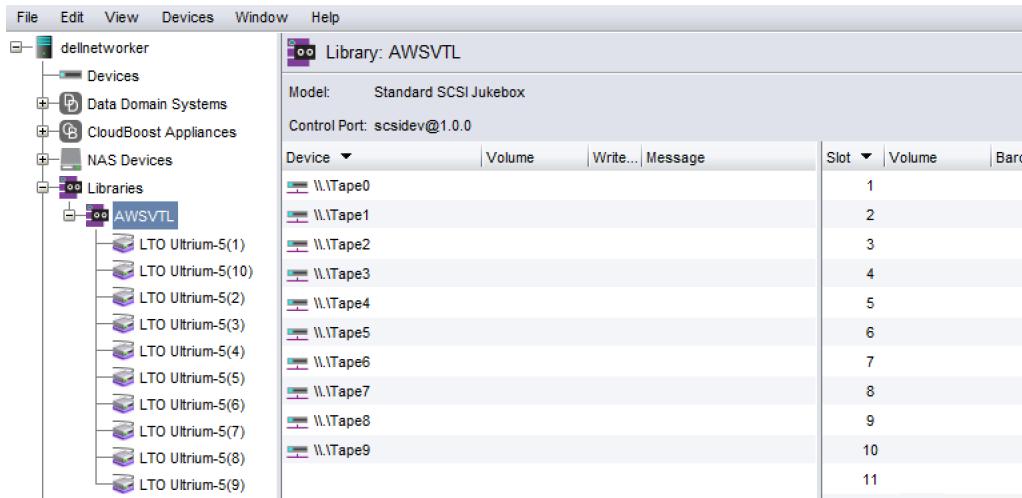
You can review and change the characteristics of the autochanger and its
associated devices using the NetWorker Management Console.

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

C:\Users\Administrator>
```

7. When "jbconfig" completes, return to the Networker GUI and hit F5 to refresh.

8. Choose your library to see your tapes in the left pane and the corresponding empty volume slots list in the right pane. In this screenshot, the "AWSVTL" library is selected.



9. In the volume list, select the volumes you want to enable (selected volumes are highlighted), open the context (right-click) menu for the selected volumes, and then choose **Deposit**. This action moves the tape from the I/E slot into the volume slot.
10. In the dialog box that appears, choose **Yes**, and then in the **Load the Cartridges into** dialog box, choose **Yes**.
11. If you don't have any more tapes to deposit, choose **No** or **Ignore**. Otherwise, choose **Yes** to deposit additional tapes.

### Enabling Import of WORM Tapes into Dell EMC NetWorker

You are now ready to import tapes from your tape gateway into the Dell EMC NetWorker library.

The virtual tapes are write once read many (WORM) tapes, but Dell EMC NetWorker expects non-WORM tapes. For Dell EMC NetWorker to work with your virtual tapes, you must enable import of tapes into non-WORM media pools.

### To enable import of WORM tapes into non-WORM media pools

1. On NetWorker Console, choose **Media**, open the context (right-click) menu for **localhost**, and then choose **Properties**.
2. In the **NetWorker Sever Properties** window, choose the **Configuration** tab.
3. In the **Worm tape handling** section, clear the **WORM tapes only in WORM pools** box, and then choose **OK**.

### Backing Up Data to a Tape in Dell EMC NetWorker

Backing up data to a tape is a two-step process.

1. Label the tapes you want to back up your data to, create the target media pool, and add the tapes to the pool.

You create a media pool and write data to a virtual tape by using the same procedures you do with physical tapes. For detailed information, see the Backing Up Data section of the *Dell EMC NetWorker Administration Guide*.

2. Write data to the tape. You back up data by using the Dell EMC NetWorker User application instead of the Dell EMC NetWorker Management Console. The Dell EMC NetWorker User application installs as part of the NetWorker installation.

**Note**

You use the Dell EMC NetWorker User application to perform backups, but you view the status of your backup and restore jobs in the EMC Management Console. To view status, choose the **Devices** menu and view the status in the **Log** window.

### Archiving a Tape in Dell EMC NetWorker

When you archive a tape, tape gateway moves the tape from the Dell EMC NetWorker tape library to the offline storage. You begin tape archival by ejecting a tape from the tape drive to the storage slot. You then withdraw the tape from the slot to the archive by using your backup application—that is, the Dell EMC NetWorker software.

#### To archive a tape by using Dell EMC NetWorker

1. On the **Devices** tab in the NetWorker Administration window, choose **localhost** or your EMC server, and then choose **Libraries**.
2. Choose the library you imported from your virtual tape library.
3. From the list of tapes that you have written data to, open the context (right-click) menu for the tape you want to archive, and then choose **Eject/Withdraw**.
4. In the confirmation box that appears, choose **OK**.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL.

In the Dell EMC NetWorker software, verify that the tape is no longer in the storage slot.

In the navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your archived tape's status is **ARCHIVED**.

### Restoring Data from an Archived Tape in Dell EMC NetWorker

Restoring your archived data is a two-step process:

1. Retrieve the archived tape a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the Dell EMC NetWorker software to restore the data. You do this by creating a restoring a folder file, as you do when restoring data from physical tapes. For instructions, see the Using the NetWorker User program section of the [Dell EMC NetWorker Administration Guide](#).

#### Next Step

##### [Cleaning Up Resources You Don't Need \(p. 149\)](#)

### Testing Your Setup by Using IBM Spectrum Protect

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using IBM Spectrum Protect with AWS Storage Gateway. (IBM Spectrum Protect was formerly known as Tivoli Storage Manager.)

This topic contains basic information about how to configure the IBM Spectrum Protect version 8.1.10 backup software for a tape gateway. It also includes basic information about performing backup and restore operations with IBM Spectrum Protect. For more information about how to administer IBM Spectrum Protect backup software, see IBM's [Overview of administration tasks](#) for IBM Spectrum Protect.

The IBM Spectrum Protect backup software supports AWS Storage Gateway on the following operating systems.

- **Microsoft Windows Server**
- **Red Hat Linux**
- **SUSE Linux**

For information about IBM Spectrum Protect supported devices for Windows, see [IBM Spectrum Protect \(formerly Tivoli Storage Manager\) Supported Devices for AIX, HP-UX, Solaris, and Windows](#).

For information about IBM Spectrum Protect supported devices for Linux, see [IBM Spectrum Protect \(formerly Tivoli Storage Manager\) Supported Devices for Linux](#).

### Topics

- [Setting Up IBM Spectrum Protect \(p. 113\)](#)
- [Configuring IBM Spectrum Protect to Work with VTL Devices \(p. 113\)](#)
- [Writing Data to a Tape in IBM Spectrum Protect \(p. 114\)](#)
- [Restoring Data from a Tape Archived in IBM Spectrum Protect \(p. 114\)](#)

### Setting Up IBM Spectrum Protect

After you connect your VTL devices to your client, you configure the IBM Spectrum Protect version 8.1.10 software to recognize them. For more information about connecting VTL devices to your client, see [Connecting Your VTL Devices \(p. 96\)](#).

#### To set up IBM Spectrum Protect

1. Get a licensed copy of the IBM Spectrum Protect version 8.1.10 software from IBM.
2. Install the IBM Spectrum Protect software on your on-premises environment or in-cloud Amazon EC2 instance. For more information, see IBM's [Installing and upgrading](#) documentation for IBM Spectrum Protect.

For more information about configuring IBM Spectrum Protect software, see [Configuring AWS Tape Gateway virtual tape libraries for an IBM Spectrum Protect server](#).

### Configuring IBM Spectrum Protect to Work with VTL Devices

Next, configure IBM Spectrum Protect to work with your VTL devices. You can configure IBM Spectrum Protect to work with VTL devices on Microsoft Windows Server, Red Hat Linux, or SUSE Linux.

#### Configuring IBM Spectrum Protect for Windows

For complete instructions on how to configure IBM Spectrum Protect on Windows, see [Tape Device Driver-W12 6266 for Windows 2012](#) on the Lenovo website. Following is basic documentation on the process.

#### To configure IBM Spectrum Protect for Microsoft Windows

1. Get the correct driver package for your media changer. For the tape-device driver, IBM Spectrum Protect requires version W12 6266 for Windows 2012. For instructions on how to get the drivers, see [Tape Device Driver-W12 6266 for Windows 2012](#) on the Lenovo website.

#### Note

Make sure that you install the "non-exclusive" set of drivers.

2. On your computer, open **Computer Management**, expand **Media Changer devices**, and verify that the media changer type is listed as **IBM 3584 Tape Library**.
3. Ensure that the barcode for any tape in the virtual tape library is eight characters or less. If you try to assign your tape a barcode that is longer than eight characters, you get this error message: "Tape barcode is too long for media changer".
4. Ensure that all your tape drives and media changer appear in IBM Spectrum Protect. To do so, use the following command: `\Tivoli\TSM\server>tsmdlst.exe`

## Configure IBM Spectrum Protect for Linux

Following is basic documentation on configuring IBM Spectrum to work with VTL devices on Linux.

### To configure IBM Spectrum Protect for Linux

1. Go to [IBM Fix Central](#) on the IBM Support website, and choose **Select product**.
2. For **Product Group**, choose **System Storage**.
3. For **Select from System Storage**, choose **Tape systems**.
4. For **Tape systems**, choose **Tape drivers and software**.
5. For **Select from Tape drivers and software**, choose **Tape device drivers**.
6. For **Platform**, choose your operating system and choose **Continue**.
7. Choose the device driver version that you want to download. Then follow the instructions on the [Fix Central](#) download page to download and configure IBM Spectrum Protect.
8. Ensure that the barcode for any tape in the virtual tape library is eight characters or less. If you try to assign your tape a barcode that is longer than eight characters, you get this error message: "Tape barcode is too long for media changer".

## Writing Data to a Tape in IBM Spectrum Protect

You write data to a tape gateway virtual tape by using the same procedure and backup policies that you do with physical tapes. Create the necessary configuration for backup and restore jobs. For more information about configuring IBM Spectrum Protect, see [Overview of administration tasks](#) for IBM Spectrum Protect.

## Restoring Data from a Tape Archived in IBM Spectrum Protect

Restoring your archived data is a two-step process.

### To restore data from an archived tape

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Restore the data by using the IBM Spectrum Protect backup software. You do this by creating a recovery point, as you do when restoring data from physical tapes. For more information about configuring IBM Spectrum Protect, see [Overview of administration tasks](#) for IBM Spectrum Protect.

## Next Step

### [Cleaning Up Resources You Don't Need \(p. 149\)](#)

## [Testing Your Setup by Using Micro Focus \(HPE\) Data Protector](#)

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Micro Focus (HPE) Data Protector v9.x. In this topic, you can find basic documentation

on how to configure the Micro Focus (HPE) Data Protector software for a tape gateway and perform a backup and restore operation. For detailed information about how to use the Micro Focus (HPE) Data Protector software, see the Hewlett Packard documentation. For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

## Topics

- [Configuring Micro Focus \(HPE\) Data Protector to Work with VTL Devices \(p. 115\)](#)
- [Preparing Virtual Tapes for Use with HPE Data Protector \(p. 116\)](#)
- [Loading Tapes into a Media Pool \(p. 117\)](#)
- [Backing Up Data to a Tape \(p. 118\)](#)
- [Archiving a Tape \(p. 118\)](#)
- [Restoring Data from a Tape \(p. 119\)](#)

## Configuring Micro Focus (HPE) Data Protector to Work with VTL Devices

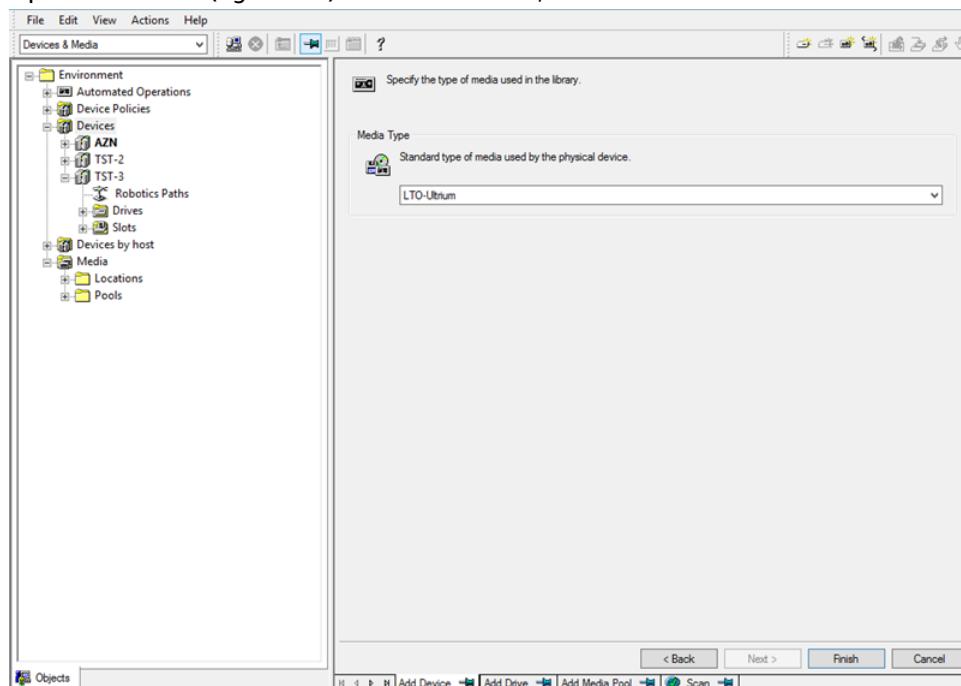
After you have connected the virtual tape library (VTL) devices to the client, you configure Micro Focus (HPE) Data Protector to recognize your devices. For information about how to connect VTL devices to the client, see [Connecting Your VTL Devices \(p. 96\)](#).

The Micro Focus (HPE) Data Protector software doesn't automatically recognize tape gateway devices. To have the software recognize these devices, manually add the devices and then discover the VTL devices, as described following.

### To add the VTL devices

1. In the Micro Focus (HPE) Data Protector main window, choose the **Devices & Media** shelf in the list at top left.

Open the context (right-click) menu for **Devices**, and choose **Add Device**.



2. On the **Add Device** tab, type a value for **Device Name**. For **Device Type**, choose **SCSI Library**, and then choose **Next**.

3. On the next screen, do the following:
  - a. For **SCSI address of the library robotic**, select your specific address.
  - b. For **Select what action Data Protector should take if the drive is busy**, choose "Abort" or your preferred action.
  - c. Choose to enable these options:
    - **Barcode reader support**
    - **Automatically discover changed SCSI address**
    - **SCSI Reserve/Release (robotic control)**
  - d. Leave **Use barcode as medium label on initialization** clear (unchecked), unless your system requires it.
  - e. Choose **Next** to continue.
4. On the next screen, specify the slots that you want to use with HP Data Protector. Use a hyphen ("–") between numbers to indicate a range of slots, for example 1–6. When you've specified slots to use, choose **Next**.
5. For the standard type of media used by the physical device, choose **LTO\_Ultrium**, and then choose **Finish** to complete the setup.

Your tape library is now ready to use. To load tapes into it, see the next section.

### [Preparing Virtual Tapes for Use with HPE Data Protector](#)

Before you can back up data to a virtual tape, you need to prepare the tape for use. Doing this involves the following actions:

- Load a virtual tape into a tape library
- Load the virtual tape into a slot
- Create a media pool
- Load the virtual tape into media pool

In the following sections, you can find steps to guide you through this process.

### [Loading Virtual Tapes into a Tape Library](#)

Your tape library should now be listed under **Devices**. If you don't see it, press F5 to refresh the screen. When your library is listed, you can load virtual tapes into the library.

#### **To load virtual tapes into your tape library**

1. Choose the plus sign next to your tape library to display the nodes for robotics paths, drives, and slots.
2. Open the context (right-click) menu for **Drives**, choose **Add Drive**, type a name for your tape, and then choose **Next** to continue.
3. Choose the tape drive you want to add for **SCSI address of data drive**, choose **Automatically discover changed SCSI address**, and then choose **Next**.
4. On the following screen, choose **Advanced**. The **Advanced Options** pop-up screen appears.
  - a. On the **Settings** tab, you should consider the following options:
    - **CRC Check** (to detect accidental data changes)
    - **Detect dirty drive** (to ensure the drive is clean before backup)
    - **SCSI Reserve/Release(drive)** (to avoid tape contention)

- For testing purposes, you can leave these options disabled (unchecked).
- b. On the **Sizes** tab, set the **Block size (kB)** to **Default (256)**.
  - c. Choose **OK** to close the advanced options screen, and then choose **Next** to continue.
  5. On the next screen, choose these options under **Device Policies**:
    - **Device may be used for restore**
    - **Device may be used as source device for object copy**
  6. Choose **Finish** to finish adding your tape drive to your tape library.

## Loading Virtual Tapes into Slots

Now that you have a tape drive in your tape library, you can load virtual tapes into slots.

### To load a tape into a slot

1. In the tape library tree node, open the node labeled **Slots**. Each slot has a status represented by an icon:
  - A green tape means that a tape is already loaded into the slot.
  - A gray slot means that the slot is empty.
  - A cyan question mark means that the tape in that slot is not formatted.
2. For an empty slot, open the context (right-click) menu, and then choose **Enter**. If you have existing tapes, choose one to load into that slot.

## Creating a Media Pool

A *media pool* is a logical group used to organize your tapes. To set up tape backup, you create a media pool.

### To create a media pool

1. In the **Devices & Media** shelf, open the tree node for **Media**, open the context (right-click) menu for the **Pools** node, and then choose **Add Media Pool**.
2. For **Pool name**, type a name.
3. For **Media Type**, choose **LTO\_Ultrium**, and then choose **Next**.
4. On the following screen, accept the default values, and then choose **Next**.
5. Choose **Finish** to finish creating a media pool.

## Loading Tapes into a Media Pool

Before you can back up data onto your tapes, you must load the tapes into the media pool that you created.

### To load a virtual tape into a media pool

1. On your tape library tree node, choose the **Slots** node.
2. Choose a loaded tape, one that has a green icon showing a loaded tape. Open the context (right-click) menu and choose **Format**, and then choose **Next**.
3. Choose the media pool you created, and then choose **Next**.
4. For **Medium Description**, choose **Use barcode**, and then choose **Next**.
5. For **Options**, choose **Force Operation**, and then choose **Finish**.

You should now see your chosen slot change from a status of unassigned (gray) to a status of tape inserted (green). A series of messages appear to confirm that your media is initialized.

At this point, you should have everything configured to begin using your virtual tape library with HPE Data Protector. To double-check that this is the case, use the following procedure.

### To verify that your tape library is configured for use

- Choose **Drives**, then open the context (right-click) menu for your drive, and choose **Scan**.

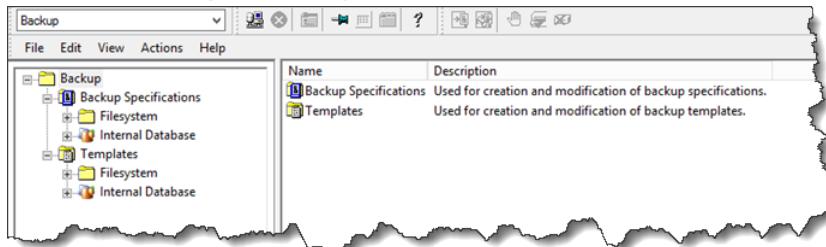
If your configuration is correct, a message confirms that your media was successfully scanned.

### Backing Up Data to a Tape

When your tapes have been loaded into a media pool, you can back up data to them.

### To back up data to a tape

- Choose the **Backup** shelf at top left of the screen.



- Open the context (right-click) menu for **Filesystem**, and choose **Add Backup**.
- On the **Create New Backup** screen, under **Filesystem**, choose **Blank File System Backup**, and then choose **OK**.
- On the tree node that shows your host system, select the file system or file systems that you want to back up, and choose **Next** to continue.
- Open the tree node for the tape library you want to use, open the context (right-click) menu for the tape drive you want to use, and then choose **Properties**.
- Choose your media pool, choose **OK**, and then choose **Next**.
- For the next three screens, accept the default settings and choose **Next**.
- On the **Perform finishing steps in your backup/template design** screen, choose **Save as** to save this session. In the pop-up window, give the backup a name and assign it to the group where you want to save your new backup specification.
- Choose **Start Interactive Backup**.

If the host system contains a database system, you can choose it as your target backup system. The screens and selections are similar to the file-system backup just described.

### Archiving a Tape

When you archive a tape, tape gateway moves the tape from the tape library to the offline storage. Before you eject and archive a tape, you might want to check the content on it.

### To check a tape's content before archiving it

- Choose **Slots** and then choose the tape you want to check.

2. Choose **Objects** and check what content is on the tape.

When you have chosen a tape to archive, use the following procedure.

#### To eject and archive a tape

1. Open the context (right-click) menu for that tape, and choose **Eject**.
2. On the Storage Gateway console, choose your gateway, and then choose **VTL Tape Cartridges** and verify the status of the virtual tape you are archiving.

After the tape is ejected, it will be automatically archived in the offline storage (GLACIER or DEEP\_ARCHIVE). The archiving process can take some time to complete. The initial status of the tape is shown as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL but is archived in GLACIER or DEEP\_ARCHIVE.

#### Restoring Data from a Tape

Restoring your archived data is a two-step process.

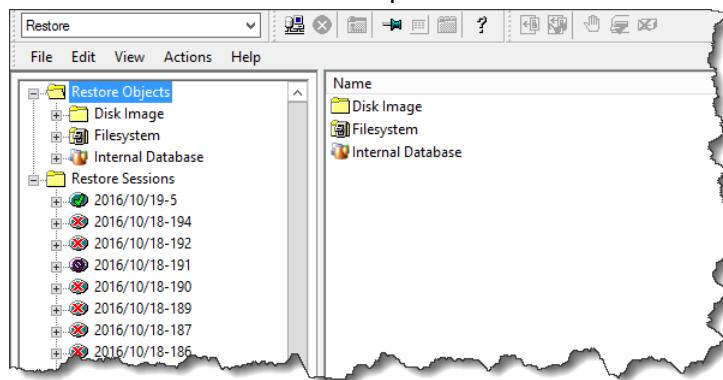
#### To restore data from an archived tape

1. Retrieve the archived tape to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use HPE Data Protector to restore the data. This process is the same as restoring data from physical tapes.

To restore data from a tape, use the following procedure.

#### To restore data from a tape

1. Choose the **Restore** shelf at the top left of the screen.



2. Choose the file system or database system you want to restore. For the backup that you want to restore, make sure that the box is selected. Choose **Restore**.
3. In the **Start Restore Session** window, choose **Needed Media**. Choose **All media**, and you should see the tape originally used for the backup. Choose that tape, and then choose **Close**.
4. In the **Start Restore Session** window, accept the default settings, choose **Next**, and then choose **Finish**.

#### Next Step

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

## Testing Your Setup by Using Microsoft System Center Data Protection Manager

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Microsoft System Center 2012 R2 or 2016 Data Protection Manager (DPM). In this topic, you can find basic documentation on how to configure the DPM backup application for a tape gateway and perform a backup and restore operation.

For detailed information about how to use DPM, see the [DPM documentation](#) on the Microsoft System Center website. For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

### Topics

- [Configuring DPM to Recognize VTL Devices \(p. 120\)](#)
- [Importing a Tape into DPM \(p. 121\)](#)
- [Writing Data to a Tape in DPM \(p. 122\)](#)
- [Archiving a Tape by Using DPM \(p. 122\)](#)
- [Restoring Data from a Tape Archived in DPM \(p. 122\)](#)

### Configuring DPM to Recognize VTL Devices

After you have connected the virtual tape library (VTL) devices to the Windows client, you configure DPM to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

By default, the DPM server does not recognize tape gateway devices. To configure the server to work with the tape gateway devices, you perform the following tasks:

1. Update the device drivers for the VTL devices to expose them to the DPM server.
2. Manually map the VTL devices to the DPM tape library.

#### To update the VTL device drivers

- In Device Manager, update the driver for the medium changer. For instructions, see [Updating the Device Driver for Your Medium Changer \(p. 409\)](#).

You use the DPMDriveMappingTool to map your tape drives to the DPM tape library.

#### To map tape drives to the DPM server tape library

1. Create at least one tape for your gateway. For information on how to do this on the console, see [Creating Tapes \(p. 93\)](#).
2. Import the tape into the DPM library. For information on how to do this, see [Importing a Tape into DPM \(p. 121\)](#).
3. If the DPMLA service is running, stop it by opening a command terminal and typing the following on the command line.

**net stop DPMLA**

4. Locate the following file on the DPM server: %ProgramFiles%\System Center 2016 R2\DPM\DPMLA\Config\DPMLA.xml.

#### Note

If this file exists, the DPMDriveMappingTool overwrites it. If you want to preserve your original file, create a backup copy.

5. Open a command terminal, change the directory to %ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin, and run the following command.

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

The output for the command looks like the following.

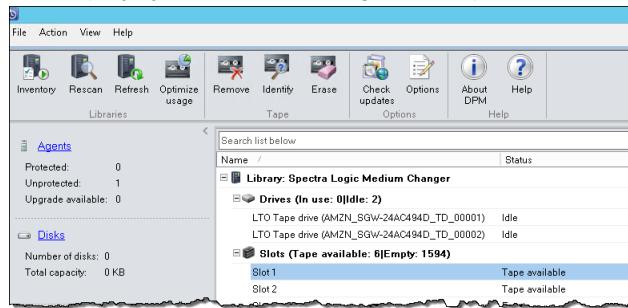
```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

## Importing a Tape into DPM

You are now ready to import tapes from your tape gateway into the DPM backup application library.

### To import tapes into the DPM backup application library

1. On the DPM server, open the Management Console, choose **Rescan**, and then choose **Refresh**. Doing this displays your medium changer and tape drives.



2. Open the context (right-click) menu for the media changer in the **Library** section, and then choose **Add tape (I/E port)** to add a tape to the **Slots** list.

#### Note

The process of adding tapes can take several minutes to complete.

The tape label appears as **Unknown**, and the tape is not usable. For the tape to be usable, you must identify it.

3. Open the context (right-click) menu for the tape you want to identify, and then choose **Identify unknown tape**.

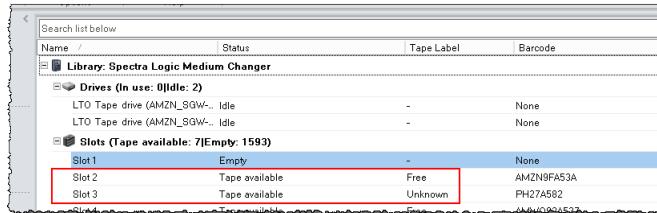
#### Note

The process of identifying tapes can take a few seconds or a few minutes.

If the tapes don't display barcodes correctly, you need to change the media changer driver to Sun/StorageTek Library. For more information, see [Displaying Barcodes for Tapes in Microsoft System Center DPM \(p. 411\)](#).

When identification is complete, the tape label changes to **Free**. That is, the tape is free for data to be written to it.

In the following screenshot, the tape in slot 2 has been identified and is free to use but the tape in slot 3 is not.



Name /	Status	Tape Label	Barcode
<b>Library: Spectra Logic Medium Changer</b>			
Drives (In use: 0 Idle: 2)	-	-	-
LTO Tape drive (AMZN_SGVA-..) Idle	-	None	
LTO Tape drive (AMZN_SGVA-..) Idle	-	None	
<b>Slots (Tape available: 7 Empty: 1593)</b>			
Slot 1	Empty	-	None
Slot 2	Tape available	Free	AMZN9FA53A
Slot 3	Tape available	Unknown	PH27A582
Slot 4	Empty	-	AMWVQ92A537
Slot 5	Empty	-	PHL9EA53B
Slot 6	Empty	-	PHL89A53C
Slot 7	Tape available	Users	
Slot 8	Tape available	Free	
Slot 9	Empty	-	
Slot 10	Empty	-	
Slot 11	Empty	-	

## Writing Data to a Tape in DPM

You write data to a tape gateway virtual tape by using the same protection procedures and policies you do with physical tapes. You create a protection group and add the data you want to back up, and then back up the data by creating a recovery point. For detailed information about how to use DPM, see the [DPM documentation](#) on the Microsoft System Center website.

By default, the capacity of a tape is 30GB. When you backup data that is larger than a tape's capacity, a device I/O error occurs. If the position where the error occurred is larger than the size of the tape, Microsoft DPM treats the error as an indication of end of tape. If the position where the error occurred is less than the size of the tape, the backup job fails. To resolve the issue, change the `TapeSize` value in the registry entry to match the size of your tape. For information about how to do this, see [Error ID: 30101](#) at the Microsoft System Center.

## Archiving a Tape by Using DPM

When you archive a tape, tape gateway moves the tape from the DPM tape library to offline storage. You begin tape archival by removing the tape from the slot using your backup application—that is, DPM.

### To archive a tape in DPM

1. Open the context (right-click) menu for the tape you want to archive, and then choose **Remove tape (I/E port)**.



2. In the dialog box that appears, choose **Yes**. Doing this ejects the tape from the medium changer's storage slot and moves the tape into one of the gateway's I/E slots. When a tape is moved into the gateway's I/E slot, it is immediately sent for archiving.
3. On the Storage Gateway console, choose your gateway, and then choose **VTL Tape Cartridges** and verify the status of the virtual tape you are archiving.

The archiving process can take some time to complete. The initial status of the tape is shown as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL.

## Restoring Data from a Tape Archived in DPM

Restoring your archived data is a two-step process.

### To restore data from an archived tape

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the DPM backup application to restore the data. You do this by creating a recovery point, as you do when restoring data from physical tapes. For instructions, see [Recovering Client Computer Data](#) on the DPM website.

### Next Step

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

## Testing Your Setup by Using NovaStor DataCenter/Network

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using NovaStor DataCenter/Network version 6.4 or 7.1. In this topic, you can find basic documentation on how to configure the NovaStor DataCenter/Network version 7.1 backup application for a tape gateway and perform backup and restore operations. For detailed information about how to use NovaStor DataCenter/Network version 7.1, see [Documentation NovaStor DataCenter/Network](#).

### Setting Up NovaStor DataCenter/Network

After you have connected your virtual tape library (VTL) devices to your Microsoft Windows client, you configure the NovaStor software to recognize your devices. For information about how to connect VTL devices to your Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

NovaStor DataCenter/Network requires drivers from the driver manufacturers. You can use the Windows drivers, but you must first deactivate other backup applications.

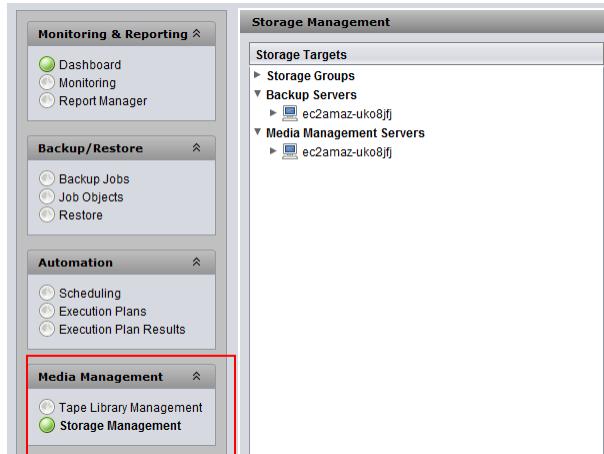
### Configuring NovaStor DataCenter/Network to Work with VTL Devices

When configuring your VTL devices to work with NovaStor DataCenter/Network version 6.4 or 7.1, you might see an error message that reads `External Program did not exit correctly`. This issue requires a workaround, which you need to perform before you continue.

You can prevent the issue by creating the workaround before you start configuring your VTL devices. For information about how to create the workaround, see [Resolving an "External Program Did Not Exit Correctly" Error \(p. 126\)](#).

### To configure NovaStor DataCenter/Network to work with VTL devices

1. In the NovaStor DataCenter/Network Admin console, choose **Media Management**, and then choose **Storage Management**.



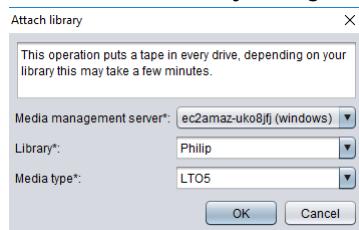
2. In the **Storage Targets** menu, open the context menu (right-click) for **Media Management Servers**, choose **New**, and choose **OK** to create and prepopulate a **storage** node.

If you see an error message that says `External Program did not exit correctly`, resolve the issue before you continue. This issue requires a workaround. For information about how to resolve this issue, see [Resolving an "External Program Did Not Exit Correctly" Error \(p. 126\)](#).

**Important**

This error occurs because the element assignment range from AWS Storage Gateway for storage drives and tape drives exceeds the number that NovaStor DataCenter/Network allows.

3. Open the context (right-click) menu for the **storage** node that was created, and choose **New Library**.
4. Choose the library server from the list. The library list is automatically populated.
5. Name the library and choose **OK**.
6. Choose the library to display all the properties of the Storage Gateway virtual tape library.
7. In the **Storage Targets** menu, expand **Backup Servers**, open the context (right-click) menu for the server, and choose **Attach Library**.
8. In the **Attach Library** dialog box that appears, choose the **LTO5** media type, and then choose **OK**.



9. Expand **Backup Servers** to see the Storage Gateway virtual tape library and the library partition that shows all the mounted tape drives.

## Creating a Tape Pool

A tape pool is dynamically created in the NovaStor DataCenter/Network software and so doesn't contain a fixed number of media. A tape pool that needs a tape gets it from its scratch pool. A *scratch pool* is a reservoir of tapes that are freely available for one or more tape pools to use. A tape pool returns to the scratch pool any media that have exceeded their retention times and that are no longer needed.

Creating a tape pool is a three-step task:

1. You create a scratch pool.
2. You assign tapes to the scratch pool.
3. You create a tape pool.

### To create a scratch pool

1. In the left navigation menu, choose the **Scratch Pools** tab.
2. Open the context (right-click) menu for **Scratch Pools**, and choose **Create Scratch Pool**.
3. In the **Scratch Pools** dialog box, name your scratch pool, and then choose your media type.
4. Choose **Label Volume**, and create a low water mark for the scratch pool. When the scratch pool is emptied down to the low water mark, a warning appears.
5. In the warning dialog box that appears, choose **OK** to create the scratch pool.

### To assign tapes to a scratch pool

1. In the left navigation menu, choose **Tape Library Management**.
2. Choose the **Library** tab to see your library's inventory.
3. Choose the tapes that you want to assign to the scratch pool. Make sure that the tapes are set to the correct media type.
4. Open the context (right-click) menu for the library and choose **Add to Scratch Pool**.

You now have a filled scratch pool that you can use for tape pools.

### To create a tape pool

1. From the left navigation menu, choose **Tape Library Management**.
2. Open the context (right-click) menu for the **Media Pools** tab and choose **Create Media Pool**.
3. Name the media pool and choose **Backup Server**.
4. Choose a library partition for the media pool.
5. Choose the scratch pool that you want the pool to get the tapes from.
6. For **Schedule**, choose **Not Scheduled**.

## Configuring Media Import and Export to Archive Tapes

NovaStor DataCenter/Network can use import/export slots if they are part of the media changer.

For an export, NovaStor DataCenter/Network must know which tapes are going to be physically taken out of the library.

For an import, NovaStor DataCenter/Network recognizes tape media that are exported in the tape library and offers to import them all, either from a data slot or an export slot. Your tape gateway archives tapes in the offline storage (GLACIER or DEEP\_ARCHIVE).

### To configure media import and export

1. Navigate to **Tape Library Management**, choose a server for **Media Management Server**, and then choose **Library**.
2. Choose the **Off-site Locations** tab.
3. Open the context (right-click) menu for the white area, and choose **Add** to open a new panel.
4. In the panel, type **S3 Glacier** or **S3 Glacier Deep Archive** and add an optional description in the text box.

## Backing Up Data to Tape

You create a backup job and write data to a virtual tape by using the same procedures that you do with physical tapes. For detailed information about how to back up data using the NovaStor software, see [Documentation NovaStor DataCenter/Network](#).

## Archiving a Tape

When you archive a tape, a tape gateway ejects the tape from the tape drive to the storage slot. It then exports the tape from the slot to the archive by using your backup application—that is, NovaStor DataCenter/Network.

### To archive a tape

1. In the left navigation menu, choose **Tape Library Management**.

2. Choose the **Library** tab to see the library's inventory.
3. Highlight the tapes you want to archive, open the context (right-click) menu for the tapes, and choose your off-site archive location.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL.

In NovaStor DataCenter/Network, verify that the tape is no longer in the storage slot.

In the navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your archived tape's status is **ARCHIVED**.

### [Restoring Data from an Archived and Retrieved Tape](#)

Restoring your archived data is a two-step process.

#### **To restore data from an archived tape**

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the NovaStor DataCenter/Network software to restore the data. You do this by refreshing the mail slot and moving each tape you want to retrieve into an empty slot, as you do when restoring data from physical tapes. For information about restoring data, see [Documentation NovaStor DataCenter/Network](#).

### [Writing Several Backup Jobs to a Tape Drive at the Same Time](#)

In the NovaStor software, you can write several jobs to a tape drive at the same time using the multiplexing feature. This feature is available when a multiplexer is available for a media pool. For information about how to use multiplexing, see [Documentation NovaStor DataCenter/Network](#).

### [Resolving an "External Program Did Not Exit Correctly" Error](#)

When configuring your VTL devices to work with NovaStor DataCenter/Network version 6.4 or 7.1, you might see an error message that reads `External Program did not exit correctly`. This error occurs because the element assignment range from Storage Gateway for storage drives and tape drives exceeds the number that NovaStor DataCenter/Network allows.

Storage Gateway returns 3200 storage and import/export slots, which is more than the 2400 limit that NovaStor DataCenter/Network allows. To resolve this issue, you add a configuration file that enables the NovaStor software to limit the number of storage and import/export slots and preconfigures the element assignment range.

#### **To apply the workaround for an "external program did not exit correctly" error**

1. Navigate to the Tape folder on your computer where you installed the NovaStor software.
2. In the Tape folder, create a text file and name it `hijacc.ini`.
3. Copy the following content, paste it into `hijacc.ini` file, and save the file.

```
port:12001
san:no
define: A3B0SOLO
*DRIVES: 10
```

```
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Add and attach the library to the media management server.
5. Move a tape from the import/export slot into the library by using the following command as shown the screenshots below. In the command, replace VTL with the name of your library.

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

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

9 Reset Stacker
11 Move Element
88 Inventory
99 Exit

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

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

9 Reset Stacker
11 Move Element
88 Inventory
99 Exit

What (#[,#[,#]])? 11
Source Address? 30000
Destination Address? 20000

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

6. Attach the library to the backup server.
7. In the NovaStor software, import all the tapes from import/export slots into the library.

## Testing Your Setup by Using Quest NetVault Backup

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using the following Quest (formerly Dell) NetVault Backup versions:

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

In this topic, you can find basic documentation on how to configure the Quest NetVault Backup application for a tape gateway and perform a backup and restore operation.

For detailed information about how to use the Quest NetVault Backup application, see the Quest NetVault Backup – Administration Guide. For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

## Topics

- [Configuring Quest NetVault Backup to Work with VTL Devices \(p. 128\)](#)
- [Backing Up Data to a Tape in the Quest NetVault Backup \(p. 129\)](#)
- [Archiving a Tape by Using the Quest NetVault Backup \(p. 129\)](#)
- [Restoring Data from a Tape Archived in Quest NetVault Backup \(p. 130\)](#)

## Configuring Quest NetVault Backup to Work with VTL Devices

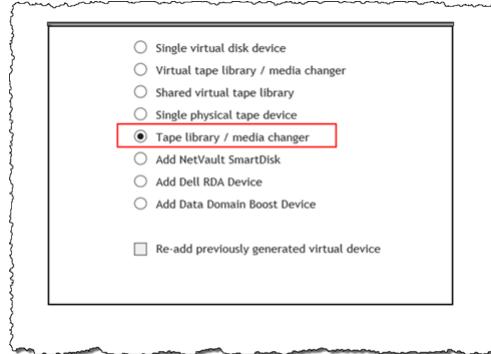
After you have connected the virtual tape library (VTL) devices to the Windows client, you configure Quest NetVault Backup to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

The Quest NetVault Backup application doesn't automatically recognize tape gateway devices. You must manually add the devices to expose them to the Quest NetVault Backup application and then discover the VTL devices.

### Adding VTL Devices

#### To add the VTL devices

1. In Quest NetVault Backup, choose **Manage Devices** in the **Configuration** tab.
2. On the **Manage Devices** page, choose **Add Devices**.
3. In the **Add Storage Wizard**, choose **Tape library / media changer**, and then choose **Next**.



4. On the next page, choose the client machine that is physically attached to the library and choose **Next** to scan for devices.
5. If devices are found, they are displayed. In this case, your medium changer is displayed in the device box.
6. Choose your medium changer and choose **Next**. Detailed information about the device is displayed in the wizard.
7. On the Add Tapes to Bays page, choose **Scan For Devices**, choose your client machine, and then choose **Next**.

All your drives are displayed on the page. Quest NetVault Backup displays the 10 bays to which you can add your drives. The bays are displayed one at a time.

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

1 - 5 of 5 Items

- Choose the drive you want to add to the bay that is displayed, and then choose **Next**.

**Important**

When you add a drive to a bay, the drive and bay numbers must match. For example, if bay 1 is displayed, you must add drive 1. If a drive is not connected, leave its matching bay empty.

- When your client machine appears, choose it, and then choose **Next**. The client machine can appear multiple times.
- When the drives are displayed, repeat steps 7 through 9 to add all the drives to the bays.
- In the **Configuration** tab, choose **Manage devices** and on the **Manage Devices** page, expand your medium changer to see the devices that you added.

## Backing Up Data to a Tape in the Quest NetVault Backup

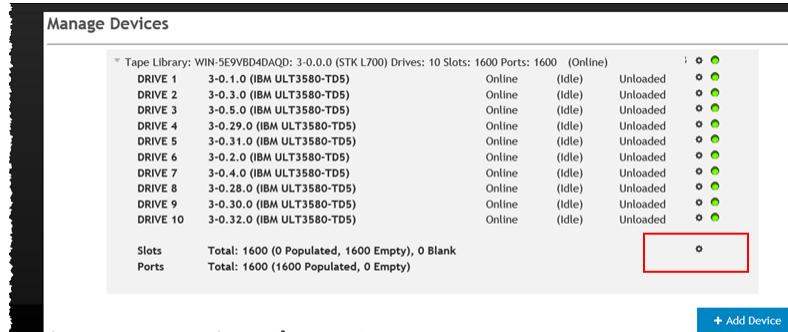
You create a backup job and write data to a virtual tape by using the same procedures you do with physical tapes. For detailed information about how to back up data, see the [Quest NetVault Backup - Administration Guide](#).

### Archiving a Tape by Using the Quest NetVault Backup

When you archive a tape, a tape gateway ejects the tape from the tape drive to the storage slot. It then exports the tape from the slot to the archive by using your backup application—that is, the Quest NetVault Backup.

#### To archive a tape in Quest NetVault Backup

- In the Quest NetVault Backup Configuration tab, choose and expand your medium changer to see your tapes.
- On the **Slots** row, choose the settings icon to open the **Slots Browser** for the medium changer.



- In the slots, locate the tape you want to archive, choose it, and then choose **Export**.

Slot ▲	Status	Barcode	Media
1	Reserved		
2	Has Blank Media	AMZND1A774	
3	Has Blank Media	AMZND6A773	
4	Empty		
5	Empty		
6	Empty		
7	Empty		
8	Empty		
9	Empty		
10	Empty		

Buttons at the bottom: Back, Ports, Set Slot, Export, Scan.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL.

In the Quest NetVault Backup software, verify that the tape is no longer in the storage slot.

In the navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your archived tape's status is **ARCHIVED**.

#### [Restoring Data from a Tape Archived in Quest NetVault Backup](#)

Restoring your archived data is a two-step process.

##### **To restore data from an archived tape**

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the Quest NetVault Backup application to restore the data. You do this by creating a restoring a folder file, as you do when restoring data from physical tapes. For instructions on creating a restore job, see [Quest NetVault Backup - Administration Guide](#).

#### **Next Step**

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

#### [Testing Your Setup by Using Veeam Backup & Replication](#)

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Veeam Backup & Replication 11A. In this topic, you can find basic documentation on how to configure the Veeam Backup & Replication software for a tape gateway and perform a backup and restore operation. For detailed information about how to use the Veeam software, see the [Veeam Backup & Replication documentation](#) in the Veeam Help Center. For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

#### **Topics**

- [Configuring Veeam to Work with VTL Devices \(p. 131\)](#)
- [Importing a Tape into Veeam \(p. 131\)](#)
- [Backing Up Data to a Tape in Veeam \(p. 132\)](#)
- [Archiving a Tape by Using Veeam \(p. 132\)](#)
- [Restoring Data from a Tape Archived in Veeam \(p. 133\)](#)

## Configuring Veeam to Work with VTL Devices

After you have connected your virtual tape library (VTL) devices to the Windows client, you configure Veeam Backup & Replication to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

### Updating VTL Device Drivers

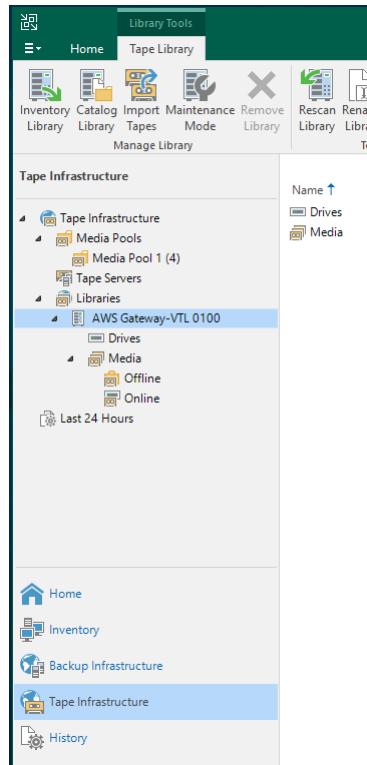
To configure the software to work with tape gateway devices, you update the device drivers for the VTL devices to expose them to the Veeam software and then discover the VTL devices. In Device Manager, update the driver for the medium changer. For instructions, see [Updating the Device Driver for Your Medium Changer \(p. 409\)](#).

### Discovering VTL Devices

You must use native SCSI commands instead of a Windows driver to discover your tape library if your media changer is unknown. For detailed instructions, see [Working with Tape Libraries](#).

### To discover VTL devices

1. In the Veeam software, choose **Tape Infrastructure**. When the tape gateway is connected, virtual tapes are listed in the **Tape Infrastructure** tab.



2. Expand the **Tape** tree to see your tape drives and medium changer.
3. Expand the medium changer tree. If your tape drives are mapped to the medium changer, the drives appear under **Drives**. Otherwise, your tape library and tape drives appear as separate devices.

If the drives are not mapped automatically, follow the [instructions on the Veeam website](#) to map the drives.

### Importing a Tape into Veeam

You are now ready to import tapes from your tape gateway into the Veeam backup application library.

## To import a tape into the Veeam library

1. Open the context (right-click) menu for the medium changer, and choose **Import** to import the tapes to the I/E slots.
2. Open the context (right-click) menu for the medium changer, and choose **Inventory Library** to identify unrecognized tapes. When you load a new virtual tape into a tape drive for the first time, the tape is not recognized by the Veeam backup application. To identify the unrecognized tape, you inventory the tapes in the tape library.

## Backing Up Data to a Tape in Veeam

Backing data to a tape is a two-step process:

1. You create a media pool and add the tape to the media pool.
2. You write data to the tape.

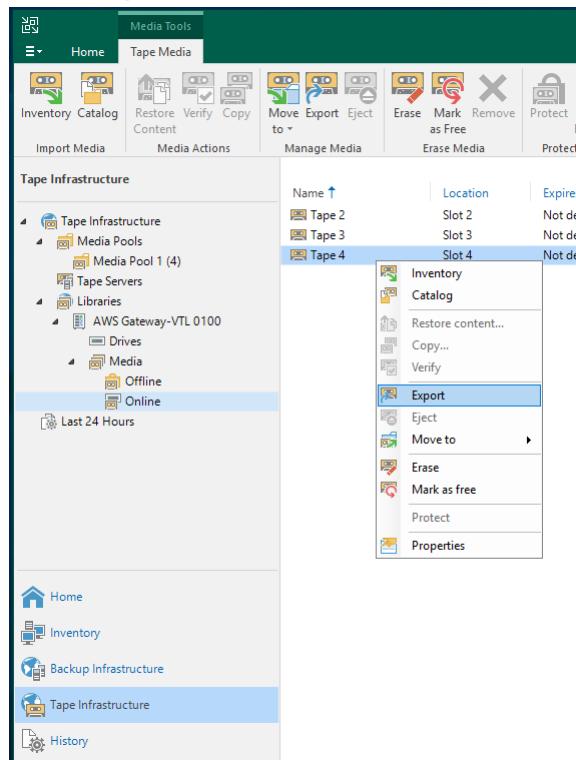
You create a media pool and write data to a virtual tape by using the same procedures you do with physical tapes. For detailed information about how to back up data, see the [Veeam documentation](#) in the Veeam Help Center.

## Archiving a Tape by Using Veeam

When you archive a tape, tape gateway moves the tape from the Veeam tape library to the offline storage. You begin tape archival by ejecting from the tape drive to the storage slot and then exporting the tape from the slot to the archive by using your backup application—that is, the Veeam software.

## To archive a tape in the Veeam library

1. Choose **Tape Infrastructure**, and choose the media pool that contains the tape you want to archive.



2. Open the context (right-click) menu for the tape that you want to archive, and then choose **Eject Tape**.
3. For **Ejecting tape**, choose **Close**. The location of the tape changes from a tape drive to a slot.
4. Open the context (right-click) menu for the tape again, and then choose **Export**. The status of the tape changes from **Tape drive** to **Offline**.
5. For **Exporting tape**, choose **Close**. The location of the tape changes from **Slot** to **Offline**.
6. On the Storage Gateway console, choose your gateway, and then choose **VTL Tape Cartridges** and verify the status of the virtual tape you are archiving.

The archiving process can take some time to complete. The initial status of the tape appears as **IN TRANSIT TO VTS**. When archiving starts, the status changes to **ARCHIVING**. When archiving is completed, the tape is no longer listed in the VTL but is archived in **GLACIER** or **DEEP\_ARCHIVE**.

## [Restoring Data from a Tape Archived in Veeam](#)

Restoring your archived data is a two-step process.

### **To restore data from an archived tape**

1. Retrieve the archived tape from archive to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the Veeam software to restore the data. You do this by creating a restoring a folder file, as you do when restoring data from physical tapes. For instructions, see [Restoring Data from Tape](#) in the Veeam Help Center.

### **Next Step**

#### [Cleaning Up Resources You Don't Need \(p. 149\)](#)

## [Testing Your Setup by Using Veritas Backup Exec](#)

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Veritas Backup Exec. In this topic, you can find basic documentation needed to perform backup and restore operations using the following versions of Backup Exec:

- Veritas Backup Exec 2014
- Veritas Backup Exec 15
- Veritas Backup Exec 16
- Veritas Backup Exec 20.x

The procedure for using these versions of Backup Exec with a tape gateway is the same. See the [Veritas support website](#) for detailed information about how to use Backup Exec, including how to create secure backups with Backup Exec, software and hardware compatibility lists, and administrator guides for Backup Exec.

For more information about supported backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

### **Topics**

- [Configuring Storage in Backup Exec \(p. 134\)](#)
- [Importing a Tape in Backup Exec \(p. 134\)](#)
- [Writing Data to a Tape in Backup Exec \(p. 136\)](#)
- [Archiving a Tape Using Backup Exec \(p. 136\)](#)

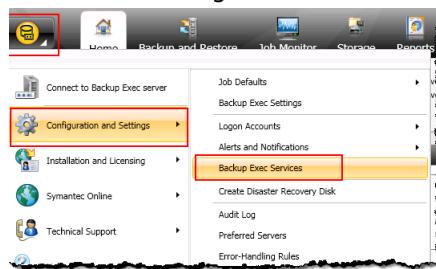
- Restoring Data from a Tape Archived in Backup Exec (p. 136)
- Disabling a Tape Drive in Backup Exec (p. 137)

## Configuring Storage in Backup Exec

After you have connected the virtual tape library (VTL) devices to the Windows client, you configure Backup Exec storage to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

### To configure storage

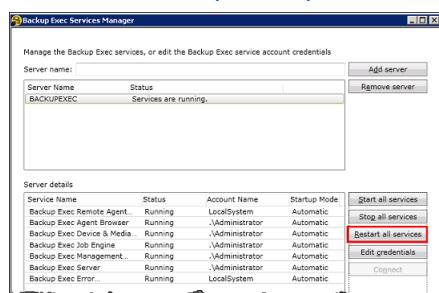
1. Start the Backup Exec software, and then choose the yellow icon in top-left corner on the toolbar.
2. Choose **Configuration and Settings**, and then choose **Backup Exec Services** to open the Backup Exec Service Manager.



3. Choose **Restart All Services**. Backup Exec then recognizes the VTL devices (that is, the medium changer and tape drives). The restart process might take a few minutes.

#### Note

Tape Gateway provides 10 tape drives. However, your Backup Exec license agreement might require your backup application to work with fewer than 10 tape drives. In that case, you must disable tape drives in the Backup Exec robotic library to leave only the number of tape drives allowed by your license agreement enabled. For instructions, see [Disabling a Tape Drive in Backup Exec \(p. 137\)](#).



4. After the restart is completed, close the Backup Exec Service Manager.

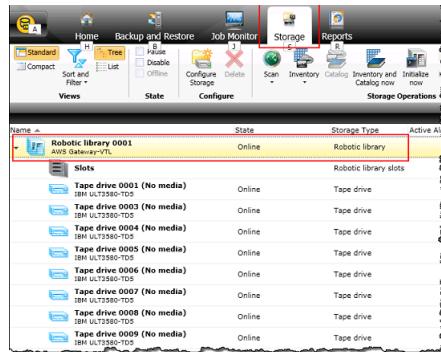
## Importing a Tape in Backup Exec

You are now ready to import a tape from your gateway into a slot.

1. Choose the **Storage** tab, and then expand the **Robotic library** tree to display the VTL devices.

#### Important

Veritas Backup Exec software requires the Tape Gateway medium changer type. If the medium changer type listed under **Robotic library** is not Tape Gateway, you must change it before you configure storage in the backup application. For information about how to select a different medium changer type, see [Selecting a Medium Changer After Gateway Activation \(p. 408\)](#).



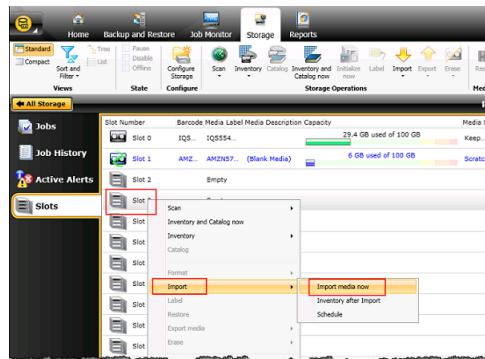
- Choose the **Slots** icon to display all slots.

**Note**

When you import tapes into the robotic library, the tapes are stored in slots instead of tape drives. Therefore, the tape drives might have a message that indicates there is no media in the drives (No media). When you initiate a backup or restore job, the tapes are moved into the tape drives.

You must have tapes available in your gateway tape library to import a tape into a storage slot. For instructions on how to create tapes, see [Adding Virtual Tapes \(p. 201\)](#).

- Open the context (right-click) menu for an empty slot, choose **Import**, and then choose **Import media now**. In the following screenshot, slot number 3 is empty. You can select more than one slot and import multiple tapes in a single import operation.



- In the **Media Request** window that appears, choose **View details**.



- In the **Action Alert: Media Intervention** window, choose **Respond OK** to insert the media into the slot.



The tape appears in the slot you selected.

**Note**

Tapes that are imported include empty tapes and tapes that have been retrieved from the archive to the gateway.

## Writing Data to a Tape in Backup Exec

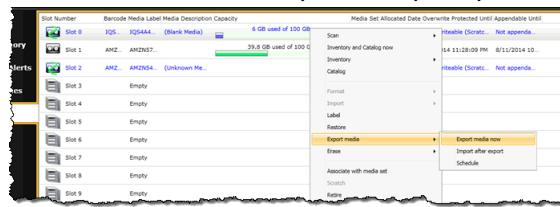
You write data to a tape gateway virtual tape by using the same procedure and backup policies you do with physical tapes. For detailed information, see the *Backup Exec Administrative Guide* in the documentation section in the Backup Exec software.

## Archiving a Tape Using Backup Exec

When you archive a tape, tape gateway moves the tape from your gateway's virtual tape library (VTL) to the offline storage. You begin tape archival by exporting the tape using your Backup Exec software.

### To archive your tape

1. Choose the **Storage** menu, choose **SLOTS**, open the context (right-click) menu for the slot you want to export the tape from, choose **Export media**, and then choose **Export media now**. You can select more than one slot and export multiple tapes in a single export operation.



2. In the **Media Request** pop-up window, choose **View details**, and then choose **Respond OK** in the **Alert: Media Intervention** window.

In the Storage Gateway console, you can verify the status of the tape you are archiving. It might take some time to finish uploading data to AWS. During this time, the exported tape is listed in the tape gateway's VTL with the status **IN TRANSIT TO VTS**. When the upload is completed and the archiving process begins, the status changes to **ARCHIVING**. When data archiving has completed, the exported tape is no longer listed in the VTL but is archived in **GLACIER** or **DEEP\_ARCHIVE**.

3. Choose your gateway, and then choose **VTL Tape Cartridges** and verify that the virtual tape is no longer listed in your gateway.
4. On the Navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your tapes status is **ARCHIVED**.

## Restoring Data from a Tape Archived in Backup Exec

Restoring your archived data is a two-step process.

### To restore data from an archived tape

1. Retrieve the archived tape to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use Backup Exec to restore the data. This process is the same as restoring data from physical tapes. For instructions, see the *Backup Exec Administrative Guide* in the documentation section in the Backup Exec software.

## Disabling a Tape Drive in Backup Exec

A tape gateway provides 10 tape drives, but you might decide to use fewer tape drives. In that case, you disable the tape drives you don't use.

1. Open Backup Exec, and choose the **Storage** tab.
2. In the **Robotic library** tree, open the context (right-click) menu for the tape drive you want to disable, and then choose **Disable**.

### Next Step

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

## Testing Your Setup by Using Veritas NetBackup

You can back up your data to virtual tapes, archive the tapes, and manage your virtual tape library (VTL) devices by using Veritas NetBackup. In this topic, you can find basic documentation on how to configure the NetBackup application for a tape gateway and perform a backup and restore operation. To do so, you can use the following versions of NetBackup:

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

The procedure for using these versions of Backup Exec with a tape gateway is similar. For detailed information about how to use NetBackup, see the [Veritas Services and Operations Readiness Tools \(SORT\)](#) on the Veritas website. For Veritas support information on hardware compatibility, see the [NetBackup 7.0 - 7.6.x Hardware Compatibility List](#), [NetBackup 8.0 - 8.1.x Hardware Compatibility List](#), or [NetBackup 8.2 - 8.x.x Hardware Compatibility List](#) on the Veritas website.

For more information about compatible backup applications, see [Supported third-party backup applications for a Tape Gateway \(p. 24\)](#).

### Topics

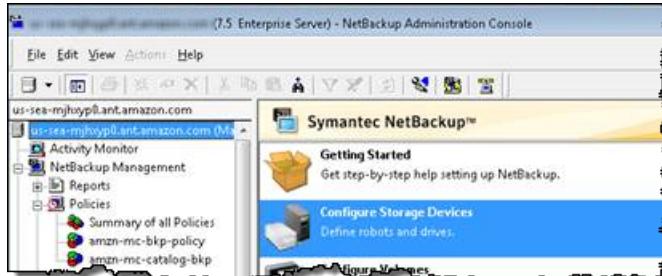
- [Configuring NetBackup Storage Devices \(p. 137\)](#)
- [Backing Up Data to a Tape \(p. 141\)](#)
- [Archiving the Tape \(p. 146\)](#)
- [Restoring Data from the Tape \(p. 148\)](#)

## Configuring NetBackup Storage Devices

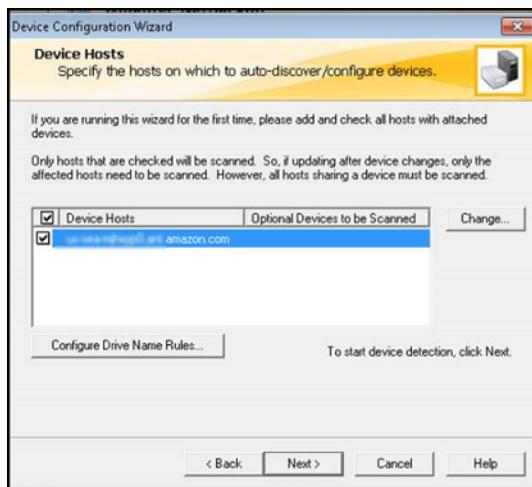
After you have connected the virtual tape library (VTL) devices to the Windows client, you configure Veritas NetBackup storage to recognize your devices. For information about how to connect VTL devices to the Windows client, see [Connecting Your VTL Devices \(p. 96\)](#).

### To configure NetBackup to use storage devices on your tape gateway

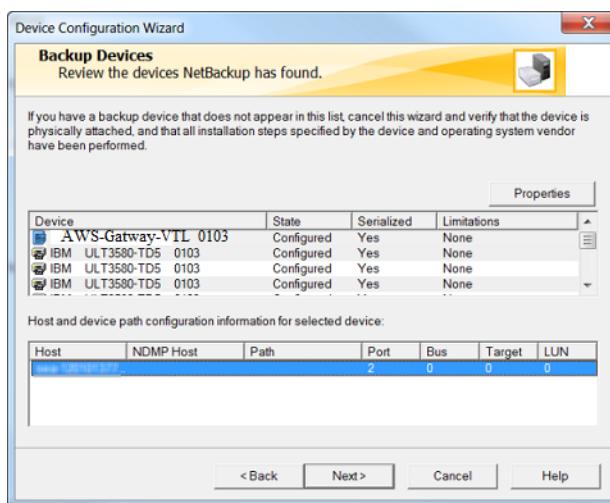
1. Open the NetBackup Administration Console and run it as an administrator.



2. Choose **Configure Storage Devices** to open the Device Configuration wizard.
3. Choose **Next**. The NetBackup application detects your computer as a device host.
4. In the **Device Hosts** column, select your computer, and then choose **Next**. The NetBackup application scans your computer for devices and discovers all devices.



5. In the **Scanning Hosts** page, choose **Next**, and then choose **Next**. The NetBackup application finds all 10 tape drives and the medium changer on your computer.

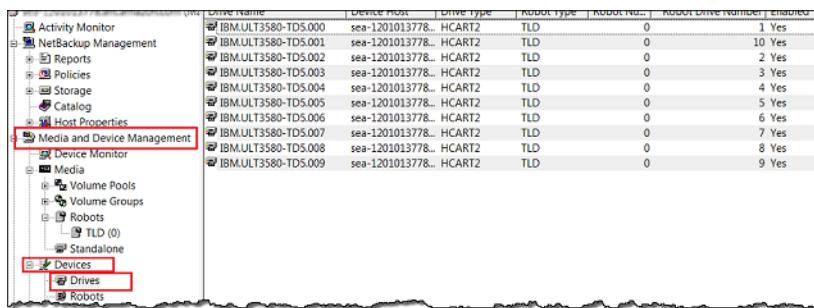


6. In the **Backup Devices** window, choose **Next**.
7. In the **Drag and Drop Configuration** window, verify that your medium changer is selected, and then choose **Next**.

8. In the dialog box that appears, choose **Yes** to save the configuration on your computer. The NetBackup application updates the device configuration.
9. When the update is completed, choose **Next** to make the devices available to the NetBackup application.
10. In the **Finished!** window, choose **Finish**.

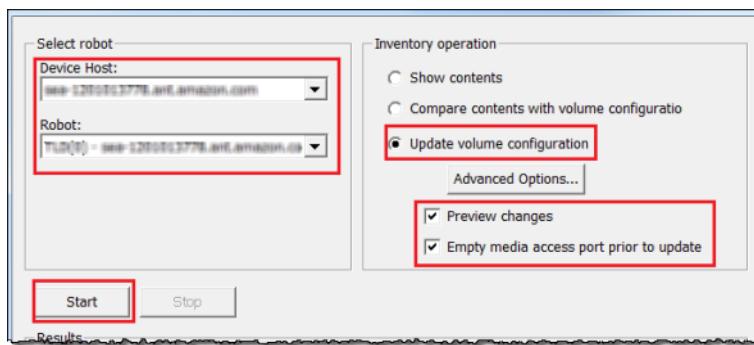
### To verify your devices in the NetBackup application

1. In the NetBackup Administration Console, expand the **Media and Device Management** node, and then expand the **Devices** node. Choose **Drives** to display all the tape drives.



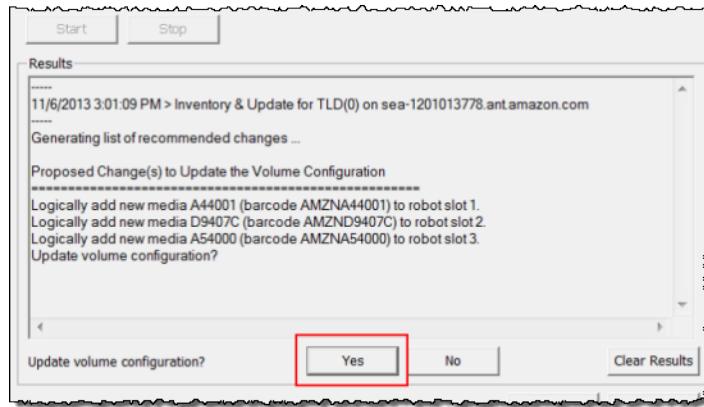
Drive Name	Device Host	Drive type	Robot type	Robot No.	Robot Drive Number	Enabled
IBM.ULT3580-TD5.000	sea-1201013778...	HCART2	TLD	0	1	Yes
IBM.ULT3580-TD5.001	sea-1201013778...	HCART2	TLD	0	10	Yes
IBM.ULT3580-TD5.002	sea-1201013778...	HCART2	TLD	0	2	Yes
IBM.ULT3580-TD5.003	sea-1201013778...	HCART2	TLD	0	3	Yes
IBM.ULT3580-TD5.004	sea-1201013778...	HCART2	TLD	0	4	Yes
IBM.ULT3580-TD5.005	sea-1201013778...	HCART2	TLD	0	5	Yes
IBM.ULT3580-TD5.006	sea-1201013778...	HCART2	TLD	0	6	Yes
IBM.ULT3580-TD5.007	sea-1201013778...	HCART2	TLD	0	7	Yes
IBM.ULT3580-TD5.008	sea-1201013778...	HCART2	TLD	0	8	Yes
IBM.ULT3580-TD5.009	sea-1201013778...	HCART2	TLD	0	9	Yes

2. In the **Devices** node, choose **Robots** to display all your medium changers. In the NetBackup application, the medium changer is called a *robot*.
3. In the **All Robots** pane, open the context (right-click) menu for **TLD(0)** (that is, your robot), and then choose **Inventory Robot**.
4. In the **Robot Inventory** window, verify that your host is selected from the **Device-Host** list located in the **Select robot** category.
5. Verify that your robot is selected from the **Robot** list.
6. In the **Robot Inventory** window, select **Update volume configuration**, select **Preview changes**, select **Empty media access port prior to update**, and then choose **Start**.

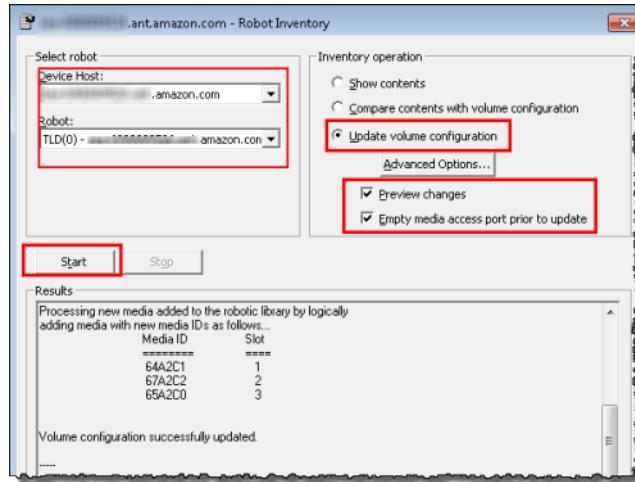


The process then inventories your medium changer and virtual tapes in the NetBackup Enterprise Media Management (EMM) database. NetBackup stores media information, device configuration, and tape status in the EMM.

7. In the **Robot Inventory** window, choose **Yes** once the inventory is complete. Choosing **Yes** here updates the configuration and moves virtual tapes found in import/export slots to the virtual tape library.



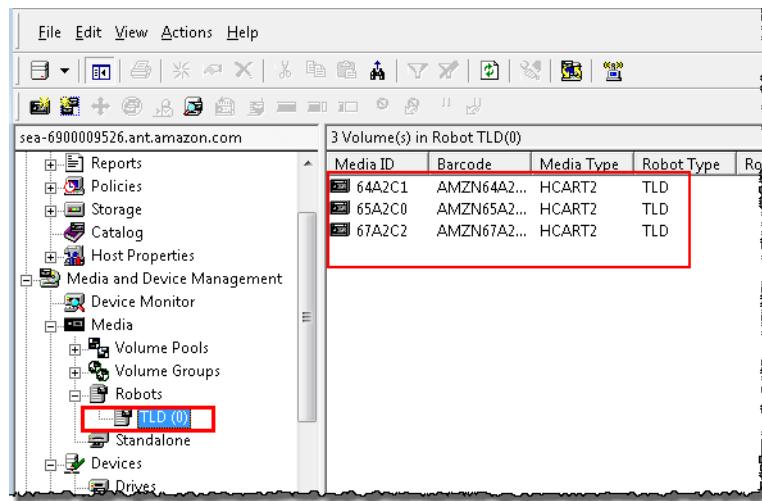
For example, the following screenshot shows three virtual tapes found in the import/export slots.



8. Close the **Robot Inventory** window.
9. In the **Media** node, expand the **Robots** node and choose **TLD(0)** to show all virtual tapes that are available to your robot (medium changer).

**Note**

If you have previously connected other devices to the NetBackup application, you might have multiple robots. Make sure that you select the right robot.



Now that you have connected your devices and made them available to your backup application, you are ready to test your gateway. To test your gateway, you back up data onto the virtual tapes you created and archive the tapes.

### Backing Up Data to a Tape

You test the tape gateway setup by backing up data onto your virtual tapes.

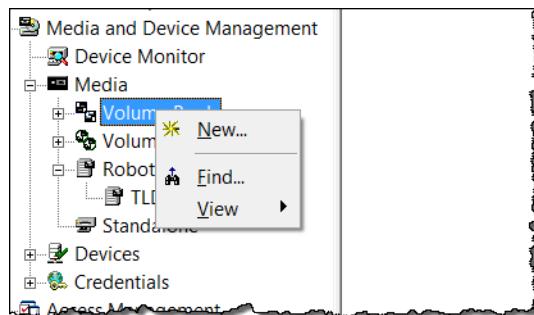
#### Note

You should back up only a small amount of data for this Getting Started exercise, because there are costs associated with storing, archiving, and retrieving data. For pricing information, see [Pricing](#) on the Storage Gateway detail page.

### To create a volume pool

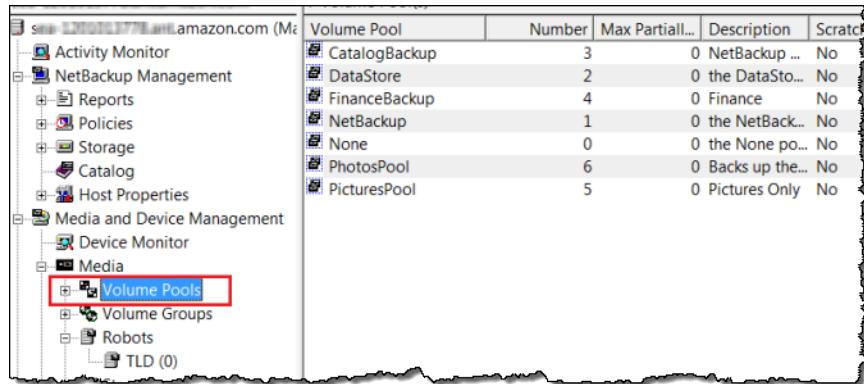
A *volume pool* is a collection of virtual tapes to use for a backup.

1. Start the NetBackup Administration Console.
2. Expand the **Media** node, open the context (right-click) menu for **Volume Pool**, and then choose **New**. The **New Volume Pool** dialog box appears.



3. For **Name**, type a name for your volume pool.
4. For **Description**, type a description for the volume pool, and then choose **OK**. The volume pool you just created is added to the volume pool list.

The following screenshot shows a list of volume pools.

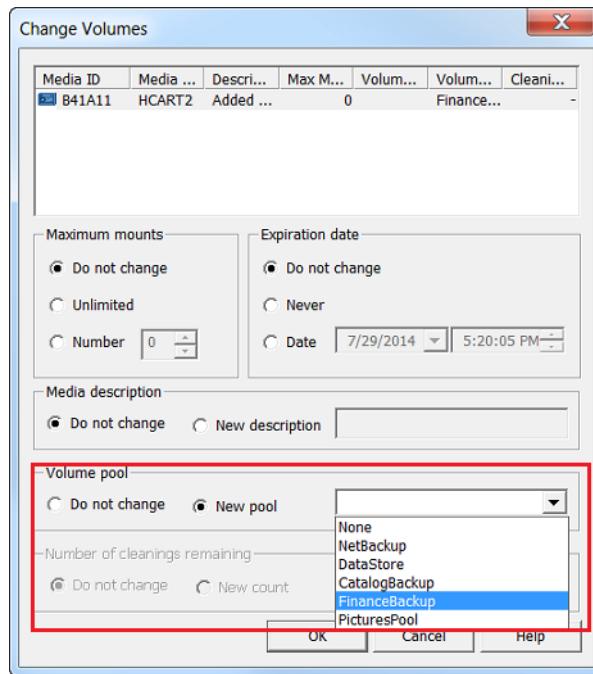


### To add virtual tapes to a volume pool

1. Expand the **Robots** node, and select the **TLD(0)** robot to display the virtual tapes this robot is aware of.

If you have previously connected a robot, your tape gateway robot might have a different name.

2. From the list of virtual tapes, open the context (right-click) menu for the tape you want to add to the volume pool, and choose **Change** to open the **Change Volumes** dialog box. The following screenshot shows the **Change Volumes** dialog box.



3. For **Volume Pool**, choose **New pool**.
4. For **New pool**, select the pool you just created, and then choose **OK**.

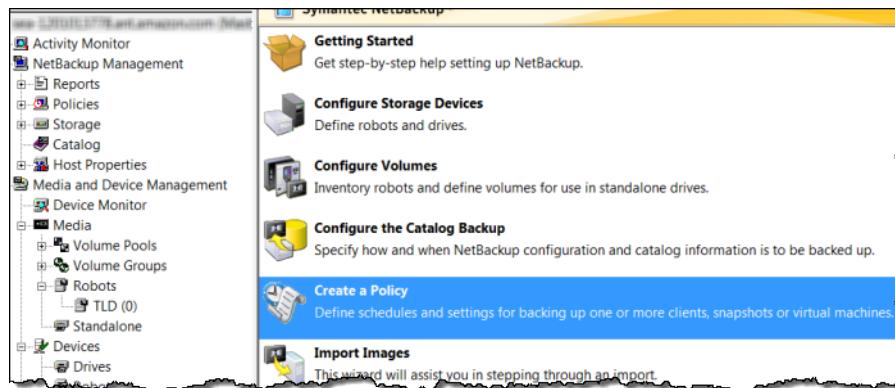
You can verify that your volume pool contains the virtual tape that you just added by expanding the **Media** node and choosing your volume pool.

## To create a backup policy

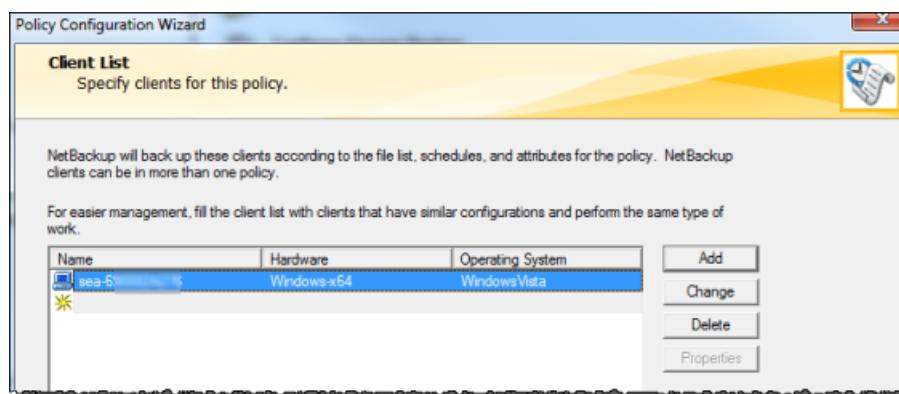
The backup policy specifies what data to back up, when to back it up, and which volume pool to use.

1. Choose your **Master Server** to return to the Veritas NetBackup console.

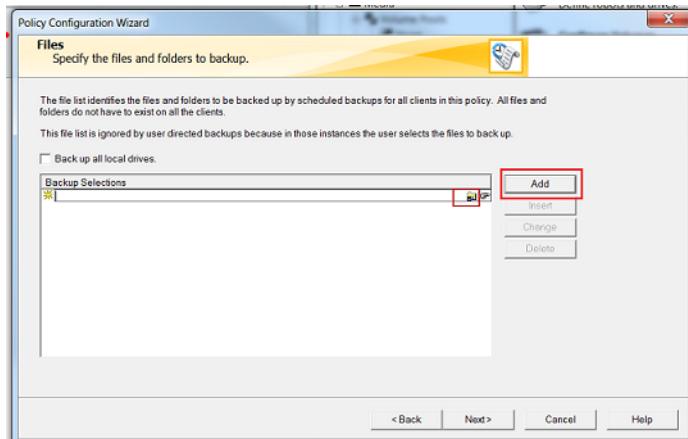
The following screenshot shows the NetBackup console with **Create a Policy** selected.



2. Choose **Create a Policy** to open the **Policy Configuration Wizard** window.
3. Select **File systems, databases, applications**, and choose **Next**.
4. For **Policy Name**, type a name for your policy and verify that **MS-Windows** is selected from the **Select the policy type** list, and then choose **Next**.
5. In the **Client List** window, choose **Add**, type the host name of your computer in the **Name** column, and then choose **Next**. This step applies the policy you are defining to localhost (your client computer).



6. In the **Files** window, choose **Add**, and then choose the folder icon.

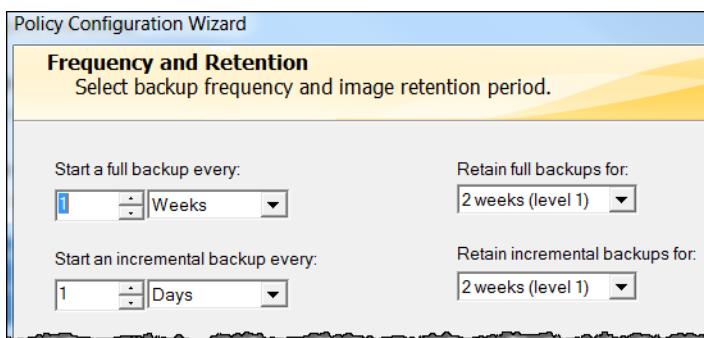


7. In the **Browse** window, browse to the folder or files you want to back up, choose **OK**, and then choose **Next**.
8. In the **Backup Types** window, accept the defaults, and then choose **Next**.

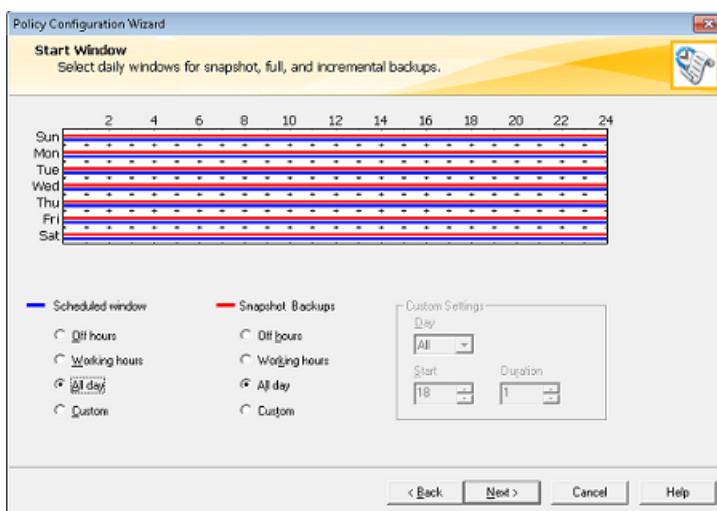
**Note**

If you want to initiate the backup yourself, select **User Backup**.

9. In the **Frequency and Retention** window, select the frequency and retention policy you want to apply to the backup. For this exercise, you can accept all the defaults and choose **Next**.



10. In the **Start** window, select **Off hours**, and then choose **Next**. This selection specifies that your folder should be backed up during off hours only.

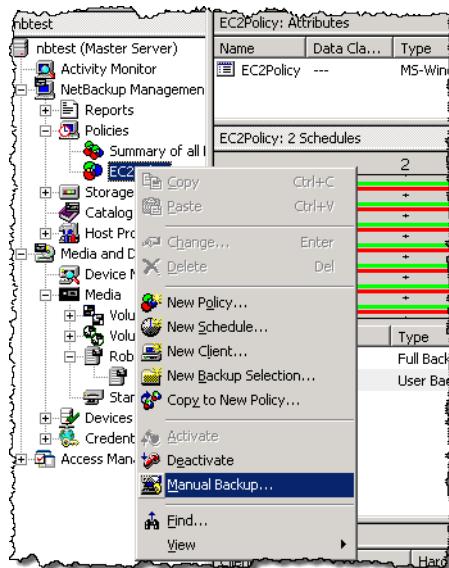


11. In the **Policy Configuration** wizard, choose **Finish**.

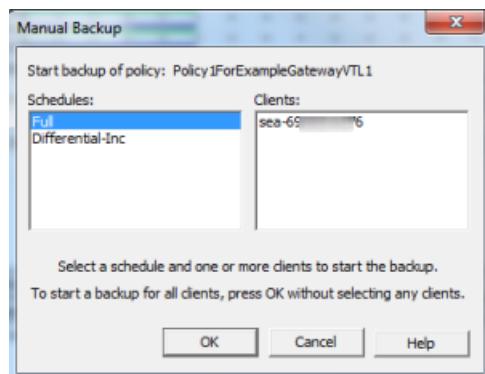
The policy runs the backups according to the schedule. You can also perform a manual backup at any time, which we do in the next step.

#### To perform a manual backup

1. On the navigation pane of the NetBackup console, expand the **NetBackup Management** node.
2. Expand the **Policies** node.
3. Open the context (right-click) menu for your policy, and choose **Manual Backup**.



4. In the **Manual Backup** window, select a schedule, select a client, and then choose **OK**.



5. In the **Manual Backup Started** dialog box that appears, choose **OK**.
6. On the navigation pane, choose **Activity Monitor** to view the status of your backup in the **Job ID** column.

nbtest: 11 Jobs (0 Queued 0 Active 0 Waiting for Retry 0 Suspended 0 Incomplete 11 Done)							
Job ID	Type	Job State	State Details	Status	Job Policy	Job Schedule	Client
18	Backup	Done		0	EC2Policy	Full	localhost
17	Backup	Done		0	EC2Policy	Full	localhost
14	Backup	Done		0	EC2Policy	Full	localhost
10	Image Cleanup	Done		1			
11	Image Cleanup	Done		1			

To find the barcode of the virtual tape where NetBackup wrote the file data during the backup, look in the **Job Details** window as described in the following procedure. You need this barcode in the procedure in the next section, where you archive the tape.

### To find the barcode of a tape

1. In **Activity Monitor**, open the context (right-click) menu for the identifier of your backup job in the **Job ID** column, and then choose **Details**.
2. In the **Job Details** window, choose the **Detailed Status** tab.
3. In the **Status** box, locate the media ID. For example, in the following screenshot, the media ID is **87A222**. This ID helps you determine which tape you have written data to.

```

Status:
10/16/2013 3:29:53 PM - Info bptm(pid=6940) using 65536 data buffer size
10/16/2013 3:29:53 PM - Info bptm(pid=6940) setting receive network buffer to 263168 bytes
10/16/2013 3:29:53 PM - Info bptm(pid=6940) using 30 data buffers
10/16/2013 3:29:53 PM - Info bptm(pid=6940) start backup
10/16/2013 3:29:53 PM - Info bptm(pid=6940) Waiting for mount of media id 87A222 (copy 1) on serve
10/16/2013 3:29:53 PM - mounting 87A222
10/16/2013 3:29:59 PM - Info bptm(pid=6940) media id 87A222 mounted on drive index 20, drivepath
10/16/2013 3:29:59 PM - mounted; mount time: 00:00:06
10/16/2013 3:29:59 PM - positioning 87A222 to file 12

```

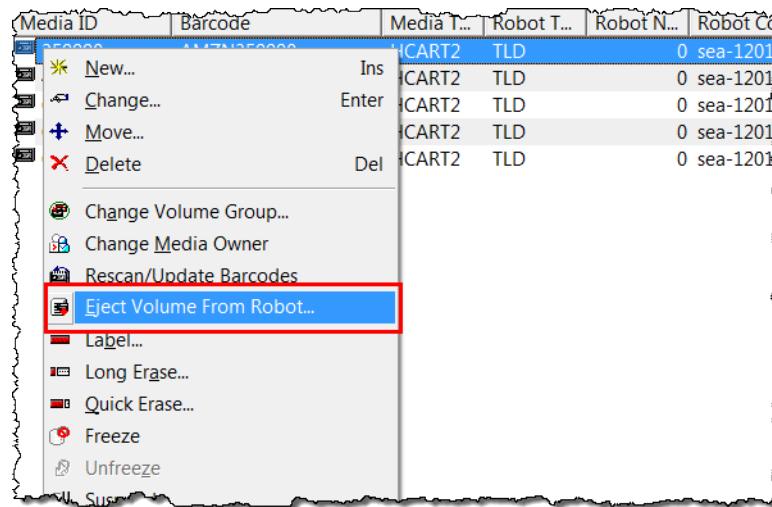
You have now successfully deployed a tape gateway, created virtual tapes, and backed up your data. Next, you can archive the virtual tapes and retrieve them from the archive.

### Archiving the Tape

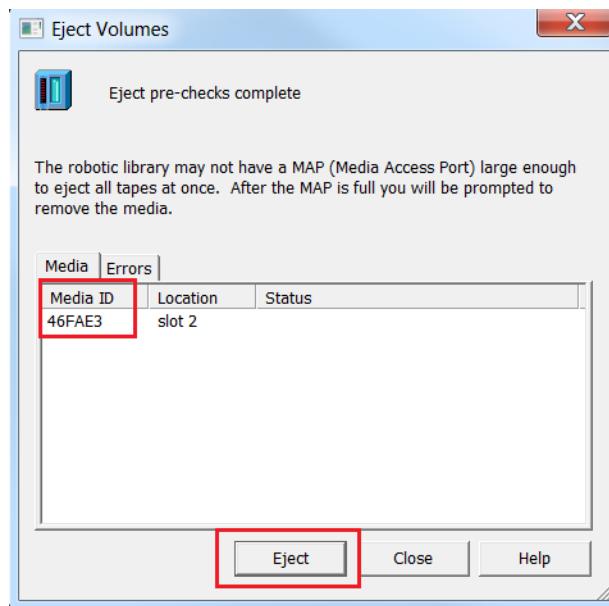
When you archive a tape, tape gateway moves the tape from your gateway's virtual tape library (VTL) to the archive, which provides offline storage. You initiate tape archival by ejecting the tape using your backup application.

### To archive a virtual tape

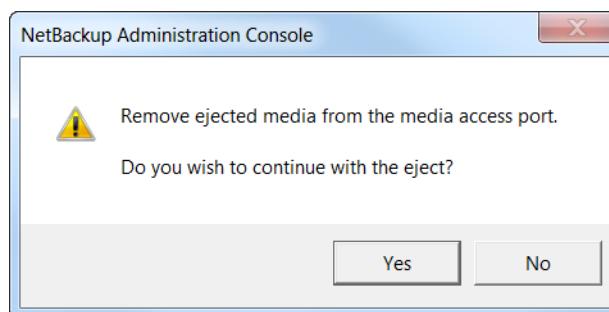
1. In the NetBackup Administration console, expand the **Media and Device Management** node, and expand the **Media** node.
2. Expand **Robots** and choose **TLD(0)**.
3. Open the context (right-click) menu for the virtual tape you want to archive, and choose **Eject Volume From Robot**.



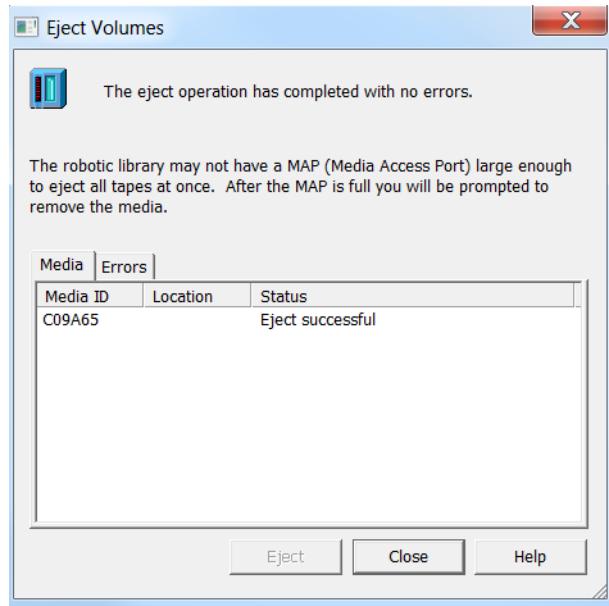
4. In the **Eject Volumes** window, make sure the **Media ID** matches the virtual tape you want to eject, and then choose **Eject**.



5. In the dialog box, choose **Yes**. The dialog box is shown following.



When the eject process is completed, the status of the tape in the **Eject Volumes** dialog box indicates that the eject succeeded.



6. Choose **Close** to close the **Eject Volumes** window.
7. In the Storage Gateway console, verify the status of the tape you are archiving in the gateway's VTL. It can take some time to finish uploading data to AWS. During this time, the ejected tape is listed in the gateway's VTL with the status **IN TRANSIT TO VTS**. When archiving starts, the status is **ARCHIVING**. Once data upload has completed, the ejected tape is no longer listed in the VTL but is archived in **GLACIER** or **DEEP\_ARCHIVE**.
8. To verify that the virtual tape is no longer listed in your gateway, choose your gateway, and then choose **VTL Tape Cartridges**.
9. In the navigation pane of the Storage Gateway console, choose **Tapes**. Verify that your archived tape's status is **ARCHIVED**.

### Restoring Data from the Tape

Restoring your archived data is a two-step process.

#### To restore data from an archived tape

1. Retrieve the archived tape to a tape gateway. For instructions, see [Retrieving Archived Tapes \(p. 203\)](#).
2. Use the Backup, Archive, and Restore software installed with the Veritas NetBackup application. This process is the same as restoring data from physical tapes. For instructions, see [Veritas Services and Operations Readiness Tools \(SORT\)](#) on the Veritas website.

#### Next Step

[Cleaning Up Resources You Don't Need \(p. 149\)](#)

## Where Do I Go from Here?

After your tape gateway is in production, you can perform several maintenance tasks, such as adding and removing tapes, monitoring and optimizing gateway performance, and troubleshooting. For general information about these management tasks, see [Managing Your Gateway \(p. 162\)](#).

You can perform some of the tape gateway maintenance tasks on the AWS Management Console, such as configuring your gateway's bandwidth rate limits and managing gateway software updates. If your tape gateway is deployed on-premises, you can perform some maintenance tasks on the gateway's local console. These include routing your tape gateway through a proxy and configuring your gateway to use a static IP address. If you are running your gateway as an Amazon EC2 instance, you can perform specific maintenance tasks on the Amazon EC2 console, such as adding and removing Amazon EBS volumes. For more information on maintaining your tape gateway, see [Managing Your Tape Gateway \(p. 200\)](#).

If you plan to deploy your gateway in production, you should take your real workload into consideration in determining the disk sizes. For information on how to determine real-world disk sizes, see [Managing local disks for your Storage Gateway \(p. 254\)](#). Also, consider cleaning up if you don't plan to continue using your tape gateway. Cleaning up lets you avoid incurring charges. For information on cleanup, see [Cleaning Up Resources You Don't Need \(p. 149\)](#).

## Cleaning Up Resources You Don't Need

If you created the gateway as an example exercise or a test, consider cleaning up to avoid incurring unexpected or unnecessary charges.

If you plan to continue using your tape gateway, see additional information in [Where Do I Go from Here? \(p. 148\)](#)

### To clean up resources you don't need

1. Delete tapes from both your gateway's virtual tape library (VTL) and archive. For more information, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).
  - a. Archive any tapes that have the **RETRIEVED** status in your gateway's VTL. For instructions, see [Archiving Tapes \(p. 412\)](#).
  - b. Delete any remaining tapes from your gateway's VTL. For instructions, see [Deleting Tapes \(p. 204\)](#).
  - c. Delete any tapes you have in the archive. For instructions, see [Deleting Tapes \(p. 204\)](#).
2. Unless you plan to continue using the tape gateway, delete it: For instructions, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).
3. Delete the Storage Gateway VM from your on-premises host. If you created your gateway on an Amazon EC2 instance, terminate the instance.

# Using a Tape Gateway on an AWS Snowball Edge device

Using a Tape Gateway on an AWS Snowball Edge device provides a secure, offline solution for migrating your tape data. With a Tape Gateway on a Snowball Edge device, you can migrate petabytes of data stored on physical tapes to AWS without changing your existing tape-based backup workflows, and without extreme network infrastructure or bandwidth-usage requirements. A standard Tape Gateway temporarily stores your tape data in the gateway cache and uses your network connection to transfer the data asynchronously to the AWS Cloud. However, a Tape Gateway on a Snowball Edge device stores your tape data on the device itself until you return it to AWS, and uses your network connection only for device-management traffic.

An AWS Snowball Edge device is one of the Snow Family Devices—a physical hardware device, shipped to you from AWS, which helps you transfer data into and out of the AWS Cloud. After you receive the device, you unlock it, set up a Tape Gateway on it, copy your tape data to it, and then ship it back to AWS. AWS then stores your tape data in secure, durable, and low-cost Amazon S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive storage. With this combination of technologies, you can migrate

your tape data to AWS in situations where you have network-connectivity limitations, bandwidth constraints, or high connection costs. Moving tape data to AWS helps you decrease your physical-tape infrastructure expenses and gain online access to your tape-based data at any time.

The following sections provide detailed instructions on creating, managing, using, and troubleshooting a Tape Gateway on a Snowball Edge device. For more information about ordering and deploying your Snowball Edge device with a Tape Gateway, see [Using an AWS Snowball Edge Device with a Tape Gateway](#) in the *AWS Snowball Edge Developer Guide*.

## Creating a Tape Gateway on your Snowball Edge device

Before you can create a Tape Gateway on a Snowball Edge device, you must order and deploy a Snowball Edge device that's preconfigured for use with Tape Gateway, and then launch the Tape Gateway application service on it. For instructions, see [Using an AWS Snowball Edge Device with a Tape Gateway](#) in the *AWS Snowball Edge Developer Guide*.

After you launch the Tape Gateway application service on your Snowball Edge device, use the following procedure to create and activate your Tape Gateway using the AWS Storage Gateway console.

### Note

Make sure that your network environment meets the network and firewall requirements for Tape Gateway. For more information, see [Network and firewall requirements \(p. 13\)](#).

### To create a gateway

1. Open the AWS Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>, select the Region where you ordered your Snowball Edge device, and then choose **Create gateway**.

#### Important

You must create and activate the Tape Gateway in the same Region where you ordered the Snowball Edge device.

#### Note

You can also open the AWS Storage Gateway console directly from within the AWS OpsHub for Snow Family Snow Family management software. To do so, choose **Open Storage Gateway management console** from the AWS OpsHub management dashboard on your Snowball Edge device.

2. For **Gateway type**, choose **Tape gateway**, then choose **Next**.
3. For **Platform options**, choose **Snowball Edge**, then choose **Next**.
4. For **Service endpoint**, choose **Public** for the type of service endpoint that your gateway will use, then choose **Next**.

#### Note

**Public** is the only service endpoint type that supports a Tape Gateway on a Snowball Edge device.

5. For **Connect to gateway**, choose **IP address** and enter the Tape Gateway IP address that you obtained when you launched the Tape Gateway application service on your Snowball Edge device, then choose **Next**. For instructions on how to obtain the Tape Gateway IP address, see [Deploying a Snowball Edge Device with a Tape Gateway](#) in the *AWS Snowball Edge Developer Guide*.
6. For **Gateway settings**, set the time zone, enter a name for your gateway, and select the backup application that you want to use to copy your tape data.
7. (Optional) Add tags to identify the gateway.
8. Choose **Activate gateway**. For more information, see [Activating Your Gateway \(p. 88\)](#).
9. (Optional) For **Gateway health log group**, configure Amazon CloudWatch logging. For more information, see [Getting Tape Gateway Health Logs with CloudWatch Log Groups \(p. 247\)](#).

10. On the **Review and finish** page, make sure that the options you selected are correct, then choose **Finish** to create your Tape Gateway.

You can check the status of your new gateway on the **Gateways** page of the Storage Gateway console, or select its name to view additional details. For a Tape Gateway on a Snowball Edge device, the **Gateway type** is **Tape (Snow)**, and the **Host platform type** is **Snowball Edge**.

Now that you have created and activated your Tape Gateway on your Snowball Edge device, you must create the virtual tapes that the gateway uses to back up your tape data. For instructions, see [Creating tapes for a Tape Gateway on a Snowball Edge device \(p. 151\)](#).

## Creating tapes for a Tape Gateway on a Snowball Edge device

After creating and activating your Tape Gateway on your Snowball Edge device, use the following procedure to create the virtual tapes that the gateway uses to back up your tape data. For more information about configuring virtual tapes, see [Creating Tapes \(p. 93\)](#).

### To create virtual tapes

1. Open the AWS Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the left navigation pane, choose **Tapes** from the navigation pane, and then choose **Create tapes**.
3. For **Select gateway**, choose the Tape Gateway that you created on your Snowball Edge device.
4. For **Tape configuration**, specify the type, quantity, capacity, barcode prefix, and pool for the tapes that you want to create.
5. (Optional) For **Tags**, add key-value pairs to describe your tapes.
6. Choose **Create tapes**.

Now that your tapes are set up, your gateway is ready to use. Before you start backing up your tape data, see [Troubleshooting and best practices for a Tape Gateway on a Snowball Edge device \(p. 151\)](#) for tips and guidelines to avoid problems and keep your gateway running smoothly.

## Troubleshooting and best practices for a Tape Gateway on a Snowball Edge device

To avoid problems and keep your Tape Gateway on Snowball Edge running smoothly, refer to the following tips and guidelines:

- After you order, receive, and deploy your Snowball Edge device, you must create and activate your Tape Gateway from the same AWS Region. Attempting to create and activate the Tape Gateway in any AWS Region other than the one where the Snowball Edge device was ordered is not supported, and will not work.
- To back up your tape data using a Tape Gateway on a Snowball Edge device, connect the virtual tape devices on the gateway to a Windows or Linux client on your network, and then access them using your preferred backup software. For more information about connecting the gateway to a client and testing it with your backup software, see [Using Your Tape Gateway \(p. 96\)](#).
- When a virtual tape is in the **Available** state in the Storage Gateway console, it is ready to be mounted using your preferred backup software, and its full capacity is reserved in physical storage on the Snowball Edge device. When you eject a virtual tape, its status changes from **Available** to **In transit to VTS**, and only the specific amount of data written to the tape remains reserved on the Snowball Edge device. You don't need to eject virtual tapes from your backup software before shipping your Snowball

Edge device back to AWS. Any virtual tapes left in the **Available** state are automatically ejected during the data-transfer process at the AWS facility.

- After you copy the data to your Snowball Edge device, you can schedule a pickup appointment to ship the device back to AWS. The E Ink shipping label is automatically updated to ensure that the device is sent to the correct AWS facility. For more information, see [Shipping an AWS Snowball Edge Device](#) in the [AWS Snowball Edge Developer Guide](#).

You can track the device by using Amazon Simple Notification Service (Amazon SNS) generated text messages and emails.

- After your tape data is successfully transferred to the AWS Cloud and your Snowball Edge job is complete, you must use the Storage Gateway console to manually delete the associated Tape Gateway.
- In rare cases, data corruption or other technical difficulties might prevent AWS from transferring specific virtual tapes to the AWS Cloud after receiving your Snowball Edge device. In such a case, you must use the Storage Gateway console to delete the virtual tapes that failed to transfer before you can re-attempt the transfer on another Snowball Edge device.
- A Tape Gateway on a Snowball Edge device supports only importing virtual tape data to AWS, and cannot be used to access data that has already been imported. To access your imported tape data, set up a standard Tape Gateway hosted on a virtual machine, hardware appliance, or Amazon EC2 instance, and then transfer the data from AWS over a network connection.
- A Snowball Edge device that is configured for Tape Gateway is not intended for use with other services or resources, such as Amazon S3, Network File System (NFS) file shares, AWS Lambda, or Amazon EC2. To use those services or resources, you must create a new Snowball Edge job to order a separate, appropriately configured device. For instructions, see [Creating an AWS Snowball Edge Job](#) in the [AWS Snowball Edge Developer Guide](#).
- To troubleshoot a Tape Gateway on a Snowball Edge device, or if directed to do so by AWS Support, you might need to connect to your gateway's local console. The local console is a configuration interface that runs on the Snowball Edge device that's hosting your gateway. You can use this local console to perform maintenance tasks specific to the gateway on that device. For more information, see [Performing Maintenance Tasks on the Local Console \(p. 264\)](#).

To access the local console for a Tape Gateway on a Snowball Edge device:

1. From the command prompt on a computer connected to the same local network as your device, run the following command:

```
ssh user_name@xxx.xxx.xxx.xxx
```

To run this command, replace `user_name` with your local console user name, and replace `xxx.xxx.xxx.xxx` with the Tape Gateway IP address that you obtained when you launched the Tape Gateway on your Snowball Edge device. For instructions on how to obtain the Tape Gateway IP address, see [Deploying a Snowball Edge Device with a Tape Gateway](#) in the [AWS Snowball Edge Developer Guide](#).

2. Enter your password.

**Note**

If this is your first time logging in to the local console on this device, the default user name is `admin`, and the default password is `password`. Change the default password immediately after you log in. For more information, see [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).

## Using the Storage Gateway API with Tape Gateway on Snowball Edge

The Storage Gateway API works the same for a Tape Gateway on a Snowball Edge device as it does for a standard Tape Gateway, with the following exceptions:

- The `GatewayType` parameter value for a Tape Gateway on a Snowball Edge device is `VTL_SNOW`. You must specify this value for the `GatewayType` parameter when using the `ActivateGateway` API operation to activate a Tape Gateway on a Snowball Edge device.
- The `HostEnvironment` parameter value for a Tape Gateway on a Snowball Edge device is `SNOWBALL`. You can activate a gateway that has the `VTL_SNOW` value for the `GatewayType` parameter only on a device that has the `SNOWBALL` value for the `HostEnvironment` parameter.
- The `HostEnvironmentId` parameter specifies the automatically generated `JobID` that's associated with the Snowball Edge device that's hosting the Tape Gateway.
- You can use the `DescribeGatewayInformation` and `ListGateways` API operations to return information about your Tape Gateway on a Snowball Edge device, including its `GatewayType`, `HostEnvironment`, and `HostEnvironmentId` parameter values.

For more detailed information about the Storage Gateway API, see the [AWS Storage Gateway API Reference](#).

## Activating a gateway in a virtual private cloud

You can create a private connection between your on-premises software appliance and cloud-based storage infrastructure. You can then use the software appliance to transfer data to AWS storage without your gateway communicating with AWS storage services over the public internet. Using the Amazon VPC service, you can launch AWS resources in a custom virtual network. You can use a virtual private cloud (VPC) to control your network settings, such as the IP address range, subnets, route tables, and network gateways. For more information about VPCs, see [What is Amazon VPC?](#) in the *Amazon VPC User Guide*.

To use a gateway with a Storage Gateway VPC endpoint in your VPC, do the following:

- Use the VPC console to create a VPC endpoint for Storage Gateway and get the VPC endpoint ID.
- If you are activating a file gateway, create a VPC endpoint for Amazon S3.
- If you are activating a file gateway, set up a HTTP proxy and configure it in the file gateway VM local console. You need this proxy for on-premises file gateways that are hypervisor-based, such as those based on VMware, Microsoft HyperV, and Linux Kernel-based Virtual Machine (KVM). In these cases, you need the proxy to enable your gateway access Amazon S3 private endpoints from outside your VPC. For information about how to configure a HTTP proxy, see [Configuring an HTTP proxy \(p. 266\)](#).
- Use the VPC endpoint ID to activate the gateway.

### Note

Your gateway must be activated in the same region where your VPC endpoint was created. For file gateway, the Amazon S3 that is configured for the file share must be in the same region where you created the VPC endpoint for S3.

## Creating a gateway using a VPC endpoint

In this section, you can find instructions about how to download, deploy, and activate your file gateway using a VPC endpoint.

### Topics

- [Creating a VPC endpoint for Storage Gateway \(p. 154\)](#)
- [Choosing a gateway type \(p. 154\)](#)
- [Choosing a host platform and downloading the VM \(p. 155\)](#)
- [Choosing a service endpoint \(p. 156\)](#)

- [Connecting to your gateway \(p. 157\)](#)
- [Activate your gateway in a VPC \(p. 159\)](#)
- [Configure local disks \(p. 161\)](#)
- [Allowing traffic to required ports in your HTTP proxy \(p. 161\)](#)

## Creating a VPC endpoint for Storage Gateway

Follow these instructions to create a VPC endpoint. If you already have a VPC endpoint for Storage Gateway, you can use it.

### To create a VPC endpoint for Storage Gateway

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Endpoints**, and then choose **Create Endpoint**.
3. On the **Create Endpoint** page, choose **AWS Services for Service** category.
4. For **Service Name**, choose `com.amazonaws.region.storagegateway`. For example `com.amazonaws.us-east-2.storagegateway`.
5. For **VPC**, choose your VPC and note its Availability Zones and subnets.
6. Verify that **Enable Private DNS Name** is not selected.
7. For **Security group**, choose the security group that you want to use for your VPC. You can accept the default security group. Verify that all of the following TCP ports are allowed in your security group:
  - TCP 443
  - TCP 1026
  - TCP 1027
  - TCP 1028
  - TCP 1031
  - TCP 2222
8. Choose **Create endpoint**. The initial state of the endpoint is **pending**. When the endpoint is created, note the ID of the VPC endpoint that you just created.
9. When the endpoint is created, choose **Endpoints**, then choose the new VPC endpoint.
10. In the **DNS Names** section, use the first DNS name that doesn't specify an Availability Zone. Your DNS name look similar to this: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Now that you have a VPC endpoint, you can create your gateway.

#### Important

If you are creating file gateway, you need to create an endpoint for Amazon S3 also. Follow the same steps as shown in To create a VPC endpoint for Storage Gateway section above but you choose `com.amazonaws.us-east-2.s3` under Service Name instead. Then you select the route table that you want the S3 endpoint associated with instead of subnet/security group. For instructions, see [Creating a gateway endpoint](#).

## Choosing a gateway type

### To choose a gateway type

1. Open the AWS Management Console at <https://console.aws.amazon.com/storagegateway/home>, and choose the AWS Region that you want to create your gateway in.

- If you have previously created a gateway in this AWS Region, the console shows your gateway. Otherwise, the service homepage appears.
2. If you haven't created a gateway in the AWS Region that you chose, choose **Get started**. If you already have a gateway in the AWS Region that you chose, choose **Gateways** from the navigation pane, and then choose **Create gateway**.
  3. For **Select gateway type**, choose a gateway type, and then choose **Next**. In this example file gateway is selected.

## Choosing a host platform and downloading the VM

If you create your gateway on-premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see [Supported hypervisors and host requirements \(p. 22\)](#).

**Note**

You can run only file, cached volume, and tape gateways on an Amazon EC2 instance.

### To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:
  - If you choose the hardware appliance, activate it by following the instructions in [Activating your hardware appliance \(p. 33\)](#).
  - If you choose one of the other options, choose **Download image** next to your virtualization platform to download a .zip file that contains the .ova file for your virtualization platform.

**Note**

The .zip file is over 500 MB in size and might take some time to download, depending on your network connection.

For Amazon EC2, you create an instance from the provided AMI.

3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache and one local disk for your upload buffer during the deployment. A file gateway requires only one local disk for a cache. For information about local disk requirements, see [Hardware and storage requirements \(p. 12\)](#).

Depending your hypervisor, set certain options:

- If you choose VMware, do the following:
  - Store your disk using the **Thick provisioned format** option. When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in thick-provisioned format.
  - Configure your gateway VM to use paravirtualized disk controllers. For more information, see [Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers \(p. 395\)](#).
- If you choose Microsoft Hyper-V, do the following:
  - Configure the disk type using the **Fixed size** option. When you use fixed-size provisioning, the disk storage is allocated immediately, resulting in better performance. If you don't use fixed-size provisioning, the storage is allocated on demand. On-demand allocation can affect the functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in fixed-size provisioned format.

- When allocating disks, choose **virtual hard disk (.vhdx) file**. Storage Gateway supports the .vhdx file type. By using this file type, you can create larger virtual disks than with other file types. If you create a .vhdx type virtual disk, make sure that the size of the virtual disks that you create doesn't exceed the recommended disk size for your gateway.
- If you choose Linux Kernel-based Virtual Machine (KVM), do the following:
  - Don't configure your disk to use sparse formatting. When you use fixed-size (nonsparse) provisioning, the disk storage is allocated immediately, resulting in better performance.
  - Use the parameter `sparse=false` to store your disk in nonsparse format when creating new virtual disks in the VM with the `virt-install` command for provisioning new virtual machines.
  - Use `virtio` drivers for disk and network devices.
  - We recommend that you don't set the `current_memory` option. If necessary, set it equal to the RAM provisioned to the gateway in the `--ram` parameter.

Following is an example `virt-install` command for installing KVM.

```
virt-install --name "SGW_KVM" --description "SGW KVM" --os-type=generic --  
ram=32768 --vcpus=16 --disk path=fgw-kvm.qcow2,bus=virtio,size=80,sparse=false  
--disk path=fgw-kvm-cache.qcow2,bus=virtio,size=1024,sparse=false --network  
default,model=virtio --graphics none --import
```

#### Note

For VMware, Microsoft Hyper-V, and KVM, synchronizing the VM time with the host time is required for successful gateway activation. Make sure that your host clock is set to the correct time and synchronize it with a Network Time Protocol (NTP) server.

For information about deploying your gateway to an Amazon EC2 host, see [Deploy your gateway to an Amazon EC2 host \(p. 401\)](#).

## Choosing a service endpoint

You can activate your gateway using a private VPC endpoint. If you use a VPC endpoint, all communication from your gateway to AWS services occurs through the VPC endpoint in your VPC in AWS.

### To choose a service endpoint

1. For **Select service endpoint**, choose **VPC**.
2. If you don't have a VPC endpoint, choose **Create a VPC endpoint** to create one in the Amazon VPC console. For instructions on the creating a VPC endpoint, see [Creating a VPC endpoint for Storage Gateway \(p. 154\)](#). A VPC endpoint allows your gateway to communicate with AWS services only through your VPC in AWS without going over the public internet.
3. In **VPC endpoint**, enter the DNS name or the IP address of the VPC endpoint for Storage Gateway. The DNS name looks similar to this:  
`vpce-1234567e1c11a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`.
4. If you already have a VPC endpoint, choose **Amazon VPC endpoints**. You can identify an existing VPC endpoint by its DNS name, IP address or VPC endpoint ID.
5. To identify the VPC endpoint by DNS name, choose **DNS name (recommended) or IP address**, provide the DNS name or the IP address. The DNS name looks similar to this:  
`vpce-1234567e1c11a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`.
6. To identify the VPC endpoint by VPC endpoint ID, choose **VPC endpoint ID** and choose the ID you want from the list.
7. Choose **Next** to connect and activate your gateway.

## Connecting to your gateway

To connect to your gateway, first get the IP address or activation key of your gateway VM. You use the IP address or activation key to activate your gateway. For gateways deployed and activated on an on-premises host, you can get the IP address or activation key from your gateway VM local console or your hypervisor client. For gateways deployed and activated on an Amazon EC2 instance, you can get the IP address or activation key from the Amazon EC2 console.

The activation process associates your gateway with your Amazon Web Services account. Your gateway VM must be running for activation to succeed.

**Note**

Make sure that you select the correct gateway type. The .ova files and Amazon Machine Images (AMIs) for the gateway types are different and are not interchangeable.

### To get the IP address or activation key for your gateway VM from the local console

1. Log on to your gateway VM local console. For detailed instructions, see the following:
  - VMware ESXi – [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. Get the IP address from the top of the menu page, and note it for later use.

### To get the IP address or activation key from an EC2 instance

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then choose the EC2 instance.
3. Choose the **Details** tab at the bottom, and then note the IP address or activation key. You use one of these to activate the gateway.

**Note**

For activation with an IP address, you can use the public or private IP address assigned to a gateway. You must be able to reach the IP address that you use from the browser from which you perform the activation.

## Setting up and configuring a HTTP proxy (on-premises file gateways only)

If you are activating a file gateway, you need to set up an HTTP proxy and configure it by using the file gateway VM local console. You need this proxy for an on-premises file gateway to access Amazon S3 private endpoints from outside your VPC. If you already have a HTTP proxy in Amazon EC2, you can use it. However, you need to verify that all of the following TCP ports are allowed in your security group:

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

If you don't have an Amazon EC2 proxy, use the following procedure to set up and configure a HTTP proxy.

### To set up a proxy server

1. Launch an Amazon EC2 Linux AMI. We recommend using an instance family that is network-optimized, such as the c5n.large.
2. Use the following command to install squid: `sudo yum install squid`. Doing this creates a default config file in `/etc/squid/squid.conf`.
3. Replace the contents of this config file with the following.

```
#  
# Recommended minimum configuration:  
  
#  
# Example rule allowing access from your local networks.  
# Adapt to list your (internal) IP networks from where browsing  
# should be allowed  
acl localnet src 10.0.0.0/8          # RFC1918 possible internal network  
acl localnet src 172.16.0.0/12        # RFC1918 possible internal network  
acl localnet src 192.168.0.0/16       # RFC1918 possible internal network  
acl localnet src fc00::/7            # RFC 4193 local private network range  
acl localnet src fe80::/10           # RFC 4291 link-local (directly plugged) machines  
  
acl SSL_ports port 443  
acl SSL_ports port 1026  
acl SSL_ports port 1027  
acl SSL_ports port 1028  
acl SSL_ports port 1031  
acl SSL_ports port 2222  
acl CONNECT method CONNECT  
  
#  
# Recommended minimum Access Permission configuration:  
#  
# Deny requests to certain unsafe ports  
http_access deny !SSL_ports  
  
# Deny CONNECT to other than secure SSL ports  
http_access deny CONNECT !SSL_ports  
  
# Only allow cachemgr access from localhost  
http_access allow localhost manager  
http_access deny manager  
  
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
http_access allow localnet  
http_access allow localhost  
  
# And finally deny all other access to this proxy  
http_access deny all  
  
# Squid normally listens to port 3128  
http_port 3128  
  
# Leave core dumps in the first cache dir  
coredump_dir /var/spool/squid  
  
#  
# Add any of your own refresh_pattern entries above these.  
#  
refresh_pattern ^ftp:                      1440      20%      10080  
refresh_pattern ^gopher:                     1440      0%       1440  
refresh_pattern -i (/cgi-bin/|\.?) 0          0%       0
```

refresh\_pattern . 0 20% 4320

4. If you don't need to lock down the proxy server and don't need to make any changes, then enable and start the proxy server using the following commands. These commands start the server when it boots up.

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

You now configure the HTTP proxy for Storage Gateway to use it. When configuring the gateway to use a proxy, use the default squid port 3128. The squid.conf file that is generated covers the following required TCP ports by default:

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

### To use the VM local console to configure the HTTP proxy

1. Log in to your gateway's VM local console. For information about how to log in, see [Logging in to the file gateway local console \(p. 265\)](#).
2. In the main menu, choose **Configure HTTP proxy**.
3. In the **Configuration** menu, choose **Configure HTTP proxy**.
4. Provide the host name and port for your proxy server.

For detailed information on how to configure a HTTP proxy, see [Configuring an HTTP proxy \(p. 266\)](#).

### To associate your gateway with your AWS account

1. For **Connect to gateway**, choose one of the following:
  - **IP address**
  - **Activation key**
2. Enter the IP address or activation key of your gateway, and then choose **Next**.

For detailed information about how to get a gateway IP address, see [Connecting to Your Gateway \(p. 440\)](#).

## Activate your gateway in a VPC

Activating a file gateway requires additional setup.

The following, shown on the activation page, are the gateway settings that you selected. The activation page appears after you associate your gateway with your Amazon Web Services account, as described preceding.

- **Gateway type** specifies the type of gateway that you are activating.
- **Endpoint type** specifies the type of endpoint that you selected for your gateway.

- **AWS Region** specifies the AWS Region where your gateway will be activated and where your data will be stored. If **Endpoint type** is **VPC**, the AWS Region should be same as the Region where your VPC endpoint is located.

### To activate your gateway

1. In **Activate gateway**, do the following:

- For **Gateway time zone**, select a time zone to use for your gateway.
- For **Gateway name**, enter a name to identify your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.

#### Note

The gateway name must be between 2 and 255 characters in length.

2. (Optional) For **Add tags**, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

If activation isn't successful, see [Troubleshooting your gateway \(p. 360\)](#) for possible solutions.

### To associate your gateway with your Amazon Web Services account

If you don't have internet access and private network access from your browser, you can still do the following.

1. Enter the fully qualified DNS name of the VPC endpoint or elastic network interface to get the activation key from the gateway. You can use curl with the following URL, or just enter this URL into your web browser.

```
http://VM IP ADDRESS/?  
gatewayType=FILE_S3&activationRegion=REGION&vpcEndpoint=VPC Endpoint DNSname&no_redirect
```

An example curl command follows.

```
curl "http://203.0.113.100/?gatewayType=FILE_S3&activationRegion=us-east-1&vpcEndpoint=vpce-12345678e91c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com&no_redirect"
```

An example activation key follows.

BME11-LQPTD-DF11P-BLLQ0-111V1

2. Use the AWS CLI to activate the gateway by specifying the activation key you received in previous step, for example:

```
aws --region us-east-1 storagegateway activate-gateway --activation-key BME11-LQPTD-DF11P-BLLQ0-111V1 --gateway-type FILE_S3 --gateway-name user-ec2-iad-pl-fgw2 --gateway-timezone GMT-4:00 --gateway-region us-east-1 --endpoint-url https://vpce-12345678e91c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Following is an example response.

```
{"GatewayARN": "arn:aws:storagegateway:us-east-1:123456789012:gateway/sgw-FFF12345"}
```

## Configure local disks

When you deployed the VM, you allocated local disks for your gateway. Now you configure your gateway to use these disks.

### To configure local disks

1. For **Configure local disks**, identify the disks you added and decide which ones you want to allocate for cached storage. For information about disk size quotas, see [Recommended local disk sizes for your gateway \(p. 445\)](#).
2. For **Allocated to**, choose **Cache** for the disk that you want to configure as cache storage.  
If you don't see your disks, choose **Refresh**.
3. Choose **Save and continue** to save your configuration settings.

## Allowing traffic to required ports in your HTTP proxy

If you use a HTTP proxy, make sure that you allow traffic from Storage Gateway to the destinations and ports listed following.

When Storage Gateway is communicating through the public endpoints, it communicates with the following Storage Gateway services.

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

### Important

Depending on your gateway's AWS Region, replace `region` in the endpoint with the corresponding region string. For example, if you create a gateway in the US West (Oregon) region, the endpoint looks like this: `storagegateway.us-west-2.amazonaws.com:443`.

When Storage Gateway is communicating through the VPC endpoint, it communicates with the AWS services through multiple ports on the Storage Gateway VPC endpoint and port 443 on the Amazon S3 private endpoint.

- TCP ports on Storage Gateway VPC endpoint.
  - 443, 1026, 1027, 1028, 1031, and 2222
- TCP port on S3 private endpoint
  - 443

You are now ready to create resources for your gateway.

### Next Step

- File gateway: [Creating a file share \(p. 46\)](#)
- Volume gateway: [Creating a volume \(p. 72\)](#)
- Tape gateway: [Creating Tapes \(p. 93\)](#)

# Managing Your Gateway

Managing your gateway includes tasks such as configuring cache storage and upload buffer space, working with volumes or virtual tapes, and doing general maintenance. If you haven't created a gateway, see [Getting Started \(p. 11\)](#).

Gateway software releases will periodically include OS updates and security patches that have been validated. These updates are applied as part of the regular gateway update process during a scheduled maintenance window, and are typically released every six months. Note: Users should treat the Storage Gateway appliance as a managed embedded device, and should not attempt to access or modify the Storage Gateway appliance instance. Attempting to install or update any software packages using other methods (ex: SSM or Hypervisor tools) than the normal gateway update mechanism may result in disruption to the proper functioning of the Gateway.

## Topics

- [Managing your file gateway \(p. 162\)](#)
- [Managing Your Volume Gateway \(p. 177\)](#)
- [Managing Your Tape Gateway \(p. 200\)](#)
- [Moving your data to a new gateway \(p. 207\)](#)

## Managing your file gateway

Following, you can find information about how to manage your file gateway resources.

## Topics

- [Adding a file share \(p. 162\)](#)
- [Deleting a file share \(p. 165\)](#)
- [Editing settings for your NFS file share \(p. 166\)](#)
- [Editing metadata defaults for your NFS file share \(p. 167\)](#)
- [Editing access settings for your NFS file share \(p. 168\)](#)
- [Editing gateway level access settings for your SMB file share \(p. 169\)](#)
- [Editing settings for your SMB file share \(p. 171\)](#)
- [Refreshing objects in your Amazon S3 bucket \(p. 173\)](#)
- [Using S3 object lock with a file gateway \(p. 175\)](#)
- [Understanding file share status \(p. 176\)](#)
- [File share best practices \(p. 176\)](#)

## Adding a file share

After your file gateway is activated and running, you can add additional file shares and grant access to Amazon S3 buckets. Buckets that you can grant access to include buckets in a different Amazon Web Services account than your file share. For information about how to add a file share, see [Creating a file share \(p. 46\)](#).

## Topics

- Granting access to an Amazon S3 bucket (p. 163)
  - Using a file share for cross-account access (p. 164)

## Granting access to an Amazon S3 bucket

When you create a file share, your file gateway requires access to upload files into your Amazon S3 bucket. To grant this access, your file gateway assumes an AWS Identity and Access Management (IAM) role that is associated with an IAM policy that grants this access.

The role requires this IAM policy and a security token service trust (STS) relationship for it. The policy determines which actions the role can perform. In addition, your S3 bucket must have an access policy that allows the IAM role to access the S3 bucket.

You can create the role and access policy yourself, or your file gateway can create them for you. If your file gateway creates the policy for you, the policy contains a list of S3 actions. For information about roles and permissions, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

The following example is a trust policy that allows your file gateway to assume an IAM role.

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

If you don't want your file gateway to create a policy on your behalf, you create your own policy and attach it to your file share. For more information about how to do this, see [Creating a file share \(p. 46\)](#).

The following example policy allows your file gateway to perform all the Amazon S3 actions listed in the policy. The first part of the statement allows all the actions listed to be performed on the S3 bucket named `TestBucket`. The second part allows the listed actions on all objects in `TestBucket`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3>ListBucket",
                "s3>ListBucketVersions",
                "s3>ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::TestBucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3>DeleteObject".
            ]
        }
    ]
}
```

```
        "s3>DeleteObjectVersion",
        "s3.GetObject",
        "s3.GetObjectAcl",
        "s3.GetObjectVersion",
        "s3>ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectAcl"
    ],
"Resource": "arn:aws:s3:::TestBucket/*",
"Effect": "Allow"
}
]
}
```

## Using a file share for cross-account access

*Cross-account* access is when an Amazon Web Services account and users for that account are granted access to resources that belong to another Amazon Web Services account. With file gateways, you can use a file share in one Amazon Web Services account to access objects in an Amazon S3 bucket that belongs to a different Amazon Web Services account.

### To use a file share owned by one Amazon Web Services account to access an S3 bucket in a different Amazon Web Services account

1. Make sure that the S3 bucket owner has granted your Amazon Web Services account access to the S3 bucket that you need to access and the objects in that bucket. For information about how to grant this access, see [Example 2: Bucket owner granting cross-account bucket permissions](#) in the *Amazon Simple Storage Service User Guide*. For a list of the required permissions, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).
2. Make sure that the IAM role that your file share uses to access the S3 bucket includes permissions for operations such as `s3:GetObjectAcl` and `s3:PutObjectAcl`. In addition, make sure that the IAM role includes a trust policy that allows your account to assume that IAM role. For an example of such a trust policy, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).

If your file share uses an existing role to access the S3 bucket, you should include permissions for `s3:GetObjectAcl` and `s3:PutObjectAcl` operations. The role also needs a trust policy that allows your account to assume this role. For an example of such a trust policy, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).

3. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
4. Choose **Give bucket owner full control** in the **Object metadata** settings in the **Configure file share setting** dialog box.

When you have created or updated your file share for cross-account access and mounted the file share on-premises, we highly recommend that you test your setup. You can do this by listing directory contents or writing test files and making sure the files show up as objects in the S3 bucket.

#### Important

Make sure to set up the policies correctly to grant cross-account access to the account used by your file share. If you don't, updates to files through your on-premises applications don't propagate to the Amazon S3 bucket that you're working with.

## Resources

For additional information about access policies and access control lists, see the following:

[Guidelines for using the available access policy options](#) in the *Amazon Simple Storage Service User Guide*

[Access Control List \(ACL\) overview](#) in the *Amazon Simple Storage Service User Guide*

## Deleting a file share

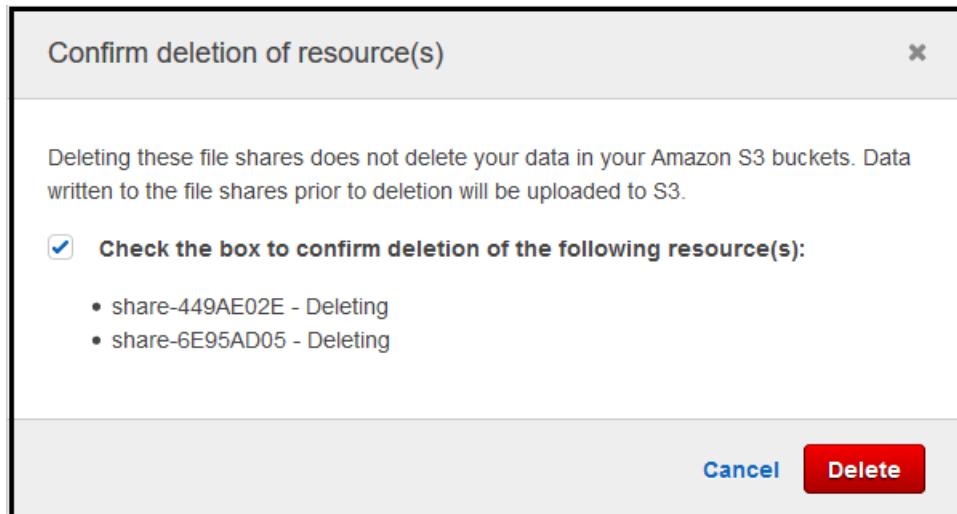
If you no longer need a file share, you can delete it from the Storage Gateway Management Console. When you delete a file share, the gateway is detached from the Amazon S3 bucket that the file share maps to. However, the S3 bucket and its contents aren't deleted.

If your gateway is uploading data to a S3 bucket when you delete a file share, the delete process doesn't complete until all the data is uploaded. The file share has the DELETING status until the data is completely uploaded.

If you want your data to be completely uploaded, use the **To delete a file share** procedure directly following. If you don't want to wait for your data to be completely uploaded, see the **To forcibly delete a file share** procedure later in this topic.

### To delete a file share

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and choose the file share that you want to delete.
3. For **Actions**, choose **Delete file share**. The following confirmation dialog box appears.



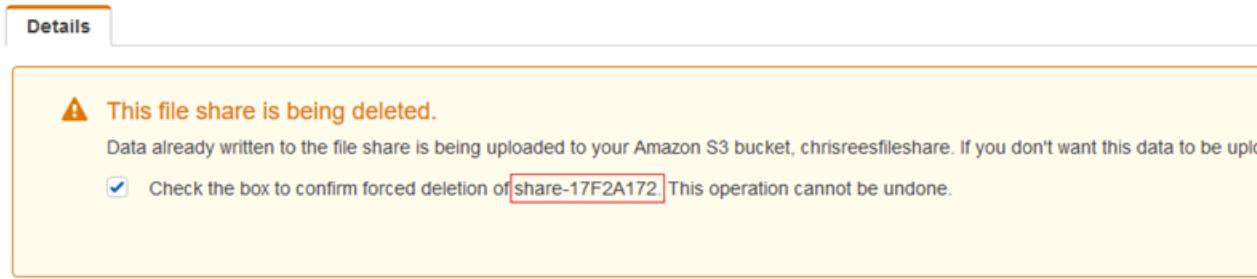
4. In the confirmation dialog box, select the check box for the file share or shares that you want to delete, and then choose **Delete**.

In certain cases, you might not want to wait until all the data written to files on the Network File System (NFS) file share is uploaded before deleting the file share. For example, you might want to intentionally discard data that was written but has not yet been uploaded. In another example, the Amazon S3 bucket or objects that back the file share might have already been deleted, meaning that uploading the specified data is no longer possible.

In these cases, you can forcibly delete the file share by using the Amazon Web Services Management Console or the `DeleteFileShare` API operation. This operation aborts the data upload process. When it does, the file share enters the FORCE\_DELETING status. To forcibly delete a file share from the console, see the procedure following.

### To forcibly delete a file share

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and choose the file share that you want to forcibly delete and wait for a few seconds. A delete message is displayed in the **Details** tab.



#### Note

You cannot undo the force delete operation.

3. In the message that appears in the **Details** tab, verify the ID of the file share that you want to forcibly delete, select the confirmation box, and choose **Force delete now**.

You can also use the [DeleteFileShare](#) API operation to forcibly delete the file share.

## Editing settings for your NFS file share

You can edit the storage class for your Amazon S3 bucket, file share name, object metadata, squash level, export as, and automated cache refresh settings.

### To edit the file share settings

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and then choose the file share that you want to update.
3. For **Actions**, choose **Edit share settings**.
4. Do one or more of the following:
  - For **Storage class for new objects**, choose a storage class to use for new objects created in your Amazon S3 bucket:
    - Choose **S3 Standard** to store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard storage class, see [Storage classes for frequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 Intelligent-Tiering** to optimize storage costs by automatically moving data to the most cost-effective storage access tier. For more information about the S3 Intelligent-Tiering storage class, see [Storage class for automatically optimizing frequently and infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 Standard-IA** to store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
    - Choose **S3 One Zone-IA** to store your infrequently accessed object data in a single Availability Zone. For more information about the S3 One Zone-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - (Optional) For **File share name**, enter a new name for the file share.
  - For **Object metadata**, choose the metadata that you want to use:
    - Choose **Guess MIME type** to enable guessing of the MIME type for uploaded objects based on file extensions.
    - Choose **Give bucket owner full control** to give full control to the owner of the S3 bucket that maps to the file's Network File System (NFS) or Server Message Block (SMB) file share. For more

information on using your file share to access objects in a bucket owned by another account, see [Using a file share for cross-account access \(p. 164\)](#).

- Choose **Enable requester pays** if you are using this file share on a bucket that requires the requester or reader instead of bucket owner to pay for access charges. For more information, see [Requester pays buckets](#).
- For **Export as**, choose an option for your file share. The default value is **Read-write**.

**Note**

For file shares mounted on a Microsoft Windows client, if you select **Read-only for Export as**, you might see an error message about an unexpected error keeping you from creating the folder. This error message is a known issue with NFS version 3. You can ignore the message.

- For **Squash level**, choose the squash level setting that you want for your NFS file share, and then choose **Save**.

**Note**

You can choose a squash level setting for NFS file shares only. SMB file shares don't use squash settings.

Possible values are the following:

- **Root squash (default)** – Access for the remote superuser (root) is mapped to UID (65534) and GID (65534).
- **No root squash** – The remote superuser (root) receives access as root.
- **All squash** – All user access is mapped to UID (65534) and GID (65534).

The default value for squash level is **Root squash**.

- (Optional) For **Automated cache refresh from S3 after**, select the check box and set the time in days, hours, and minutes to refresh the file share's cache using Time To Live (TTL). TTL is the length of time since the last refresh after which access to the directory would cause the file gateway to first refresh that directory's contents from the Amazon S3 bucket.
- (Optional) For **File upload notification**, choose the check box to be notified when a file has been fully uploaded to S3 by the file gateway. Set the **Settling Time** in seconds to control the number of seconds to wait after the last point in time a client wrote to a file before generating an **ObjectUploaded** notification. Because clients can make many small writes to files, it's best to set this parameter for as long as possible to avoid generating multiple notifications for the same file in a small time period. For more information, see [Getting file upload notification \(p. 228\)](#).

**Note**

This setting has no effect on the timing of the object uploading to S3, only the timing of the notification.

5. Choose **Save**.

## Editing metadata defaults for your NFS file share

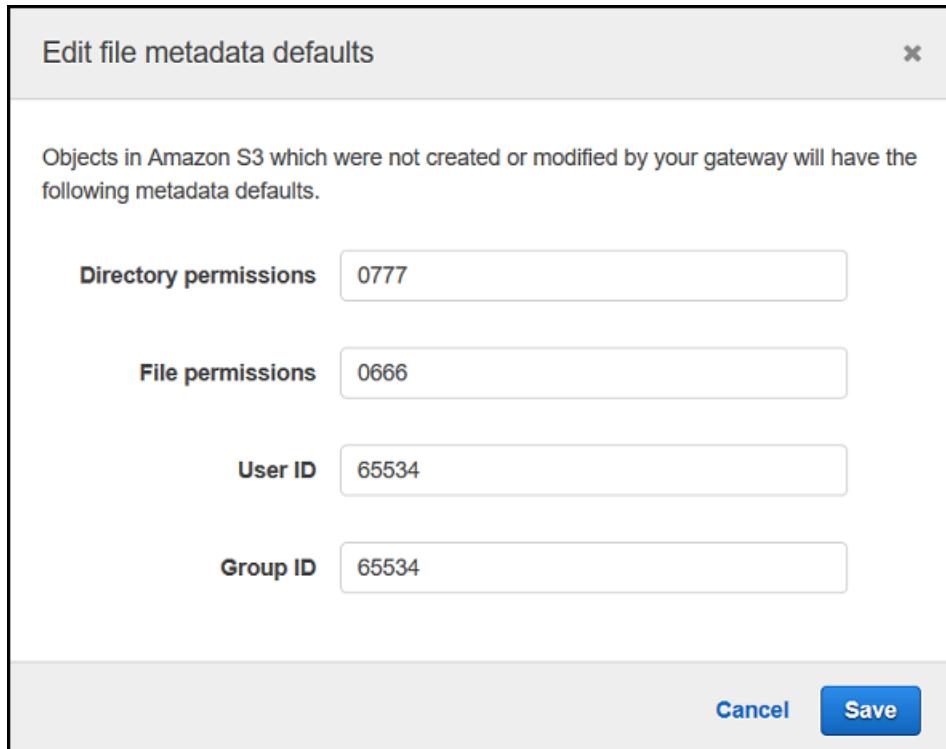
If you don't set metadata values for your files or directories in your bucket, your file gateway sets default metadata values. These values include Unix permissions for files and folders. You can edit the metadata defaults on the Storage Gateway Management Console.

When your file gateway stores files and folders in Amazon S3, the Unix file permissions are stored in object metadata. When your file gateway discovers objects that weren't stored by the file gateway, these objects are assigned default Unix file permissions. You can find the default Unix permissions in the following table.

Metadata	Description
<b>Directory permissions</b>	The Unix directory mode in the form "nnnn". For example, "0666" represents the access mode for all directories inside the file share. The default value is 0777.
<b>File permissions</b>	The Unix file mode in the form "nnnn". For example, "0666" represents the file mode inside the file share. The default value is 0666.
<b>User ID</b>	The default owner ID for files in the file share. The default value is 65534.
<b>Group ID</b>	The default group ID for the file share. The default value is 65534.

#### To edit metadata defaults

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and then choose the file share that you want to update.
3. For **Actions**, choose **Edit file metadata defaults**.
4. In the **Edit file metadata defaults** dialog box, provide the metadata information and choose **Save**.



## Editing access settings for your NFS file share

We recommend changing the allowed NFS client settings for your NFS file share. If you don't, any client on your network can mount to your file share.

### To edit NFS access settings

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and then choose the NFS file share that you want to edit.
3. For **Actions**, choose **Edit share access settings**.
4. In the **Edit allowed clients** dialog box, choose **Add entry**, provide the IP address or CIDR notation for the client that you want to allow, and then choose **Save**.

## Editing gateway level access settings for your SMB file share

You can set the security level for your gateway, set access for AD user, provide guests access, and set file share visibility for your file share.

### Topics

- [Setting a security level for your gateway \(p. 169\)](#)
- [Using Active Directory to authenticate users \(p. 170\)](#)
- [Providing guest access to your file share \(p. 171\)](#)
- [Setting file share visibility \(p. 171\)](#)

### To edit gateway level access settings for your SMB file share

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose the gateway that you want to use to join the domain.
3. For **Actions**, choose **Edit SMB settings** to open the **Edit SMB settings** dialog box and choose the action you want to perform.

## Setting a security level for your gateway

By using a file gateway, you can specify a security level for your gateway. By specifying this security level, you can set whether your gateway should require Server Message Block (SMB) signing or SMB encryption, or whether you want to enable SMB version 1.

### To configure security level

1. Choose the pencil icon in the upper right corner of the **SMB security settings** section.
2. For **Security level**, choose one of the following:

#### Note

This setting is called `SMBSecurityStrategy` in the API Reference.  
A higher security level can affect performance.

- **Force encryption** – if you choose this option, file gateway only allows connections from SMBv3 clients that have encryption enabled. This option is highly recommended for environments that handle sensitive data. This option works with SMB clients on Microsoft Windows 8, Windows Server 2012, or newer.
- **Force signing** – if you choose this option, file gateway only allows connections from SMBv2 or SMBv3 clients that have signing enabled. This option works with SMB clients on Microsoft Windows Vista, Windows Server 2008, or newer.

- **Client negotiated** – if you choose this option, requests are established based on what is negotiated by the client. This option is recommended when you want to maximize compatibility across different clients in your environment.

**Note**

For gateways activated before June 20, 2019, the default security level is **Client negotiated**. For gateways activated on June 20, 2019 and later, the default security level is **Enforce encryption**.

3. Choose **Save**.

## Using Active Directory to authenticate users

To use your corporate Active Directory for user authenticated access to your SMB file share, edit the SMB settings for your gateway with your Microsoft AD domain credentials. Doing this allows your gateway to join your Active Directory domain and allows members of the domain to access the SMB file share.

**Note**

Using AWS Directory Service, you can create a hosted Active Directory domain service in the Amazon Web Services Cloud.

Anyone who can provide the correct password gets guest access to the SMB file share.

You can also enable access control lists (ACLs) on your SMB file share. For information about how to enable ACLs, see [Using Microsoft Windows ACLs to Control Access to an SMB File Share \(p. 347\)](#).

### To enable Active Directory authentication

1. Choose the pencil icon in the upper right corner of the **Active Directory settings** section.
2. For **Domain name**, provide the domain that you want the gateway to join. You can join a domain by using its IP address or its organizational unit. An *organizational unit* is an Active Directory subdivision that can hold users, groups, computers, and other organizational units.

**Note**

If your gateway can't join an Active Directory directory, try joining with the directory's IP address by using the [JoinDomain](#) API operation.

**Note**

**Active Directory status** shows **Detached** when a gateway has never joined a domain.

3. Provide the domain user and the domain password, and then choose **Save**.

A message at the top of the **Gateways** section of your console indicates that your gateway successfully joined your AD domain.

### To limit file share access to specific AD users and groups

1. In the Storage Gateway console, choose the file share that you want to limit access to.
2. For **Actions**, choose **Edit share settings** to open the **Edit Allowed/Denied users and groups** dialog box.
3. For **Allowed users**, choose **Add entry** and provide the list of AD users that you want to allow file share access.
4. For **Allowed groups**, choose **Add entry** and provide the list of AD groups that you want to allow file share access.
5. For **Denied users**, choose **Add entry** and provide the list of AD users that you want to deny file share access.

6. For **Denied groups**, choose **Add entry** and provide the list of AD users that you want to deny file share access.
7. When you finish adding your entries, choose **Save**.

**Note**

For users and groups, enter only the AD user or group name. The domain name is implied by the membership of the gateway in the specific AD that the gateway is joined to.

If you don't specify valid or invalid users or groups, any authenticated Active Directory user can export the file share.

## Providing guest access to your file share

If you want to provide only guest access, your file gateway doesn't have to be part of a Microsoft AD domain. You can also use a file gateway that is a member of an AD domain to create file shares with guest access. Before you create a file share using guest access, you need to change the default password.

### To change the guest access password

1. Choose the pencil icon in the upper right corner of the **Guest access settings** section.
2. For **Guest password**, provide a password, and then choose **Save**.

## Setting file share visibility

File share visibility controls whether the shares on a gateway are visible when listing shares to users.

### To set file share visibility

1. In the **File share visibility settings** section, choose the pencil icon to edit.
2. For **Visibility status**, select the check box to have the shares on this gateway appear when listing shares to users. Keep the check box cleared to have the shares on this gateway not appear when listing shares to users.

## Editing settings for your SMB file share

After you have created an SMB file share, you can edit the storage class for your Amazon S3 bucket, object metadata, case sensitivity, access based enumeration, audit logs, automated cache refresh, and the export as settings for your file share.

**Note**

When Force case sensitivity is not selected (the default), the gateway will process client requests in a case-sensitive or case-insensitive manner as directed by the SMB client. This setting is appropriate for most applications. Selecting "Force case sensitivity" will configure the gateway to always process client requests in a case-sensitive manner. You should select this option if Windows clients will be used to access the share and you plan to have files of mixed case in the same directory. Note: The version of Windows and the application accessing the files may impact how a Windows client handles case sensitivity.

### To edit SMB file share settings

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and then choose the file share that you want to update.
3. For **Actions**, choose **Edit share settings**.
4. Do one or more of the following:

- For **Storage class for new objects**, choose a storage class to use for new objects created in your Amazon S3 bucket:
  - Choose **S3 Standard** to store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard storage class, see [Storage classes for frequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Intelligent-Tiering** to optimize storage costs by automatically moving data to the most cost-effective storage access tier. For more information about the S3 Intelligent-Tiering storage class, see [Storage class for automatically optimizing frequently and infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 Standard-IA** to store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated. For more information about the S3 Standard-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
  - Choose **S3 One Zone-IA** to store your infrequently accessed object data in a single Availability Zone. For more information about the S3 One Zone-IA storage class, see [Storage classes for infrequently accessed objects](#) in the *Amazon Simple Storage Service User Guide*.
- (Optional) For **File share name**, enter a new name for the file share.
- For **Object metadata**, choose the metadata that you want to use:
  - Choose **Guess MIME type** to enable guessing of the MIME type for uploaded objects based on file extensions.
  - Choose **Give bucket owner full control** to give full control to the owner of the S3 bucket that maps to the file's Network File System (NFS) or Server Message Block (SMB) file share. For more information on using your file share to access objects in a bucket owned by another account, see [Using a file share for cross-account access \(p. 164\)](#).
  - Choose **Enable requester pays** if you are using this file share on a bucket that requires the requester or reader instead of bucket owner to pay for access charges. For more information, see [Requester pays buckets](#).
- For **Export as**, choose an option for your file share. The default value is **Read-write**.

**Note**

For file shares mounted on a Microsoft Windows client, if you select **Read-only** for **Export as**, you might see an error message about an unexpected error keeping you from creating the folder. This error message is a known issue with NFS version 3. You can ignore the message.

- For **Case sensitivity**, select the check box to allow the gateway to control the case sensitivity, or clear the check box to allow the client to control the case sensitivity.

**Note**

- If you are selecting this check box, this setting applies immediately to new SMB client connections. Existing SMB client connections must disconnect from the file share and reconnect for the setting to take effect.
- If you are clearing this check box, this setting might cause you to lose access to files with names that differ only in their case.

- For **Access based enumeration**, select the check box to make the files and folders on the share visible only to users who have read access. Keep the check box cleared to make the files and folders on the share visible to all users during directory enumeration.

**Note**

Access-based enumeration is a system that filters the enumeration of files and folders on an SMB file share based on the share's access control lists (ACLs).

- For **Audit logs**, choose one of the following:
  - **Disable logging**

- **Create a new log group** to create a new audit log.
- **Use an existing log group** and choose an existing audit log from the list.

For more information about audit logs, see [Understanding file gateway audit logs \(p. 234\)](#).

- (Optional) For **Automated cache refresh from S3 after**, select the check box and set the time in days, hours, and minutes to refresh the file share's cache using Time To Live (TTL). TTL is the length of time since the last refresh after which access to the directory would cause the file gateway to first refresh that directory's contents from the Amazon S3 bucket.
- (Optional) For **File upload notification**, choose the check box to be notified when a file has been fully uploaded to S3 by the file gateway. Set the **Settling Time** in seconds to control the number of seconds to wait after the last point in time a client wrote to a file before generating an ObjectUploaded notification. Because clients can make many small writes to files, it's best to set this parameter for as long as possible to avoid generating multiple notifications for the same file in a small time period. For more information, see [Getting file upload notification \(p. 228\)](#).

**Note**

This setting has no effect on the timing of the object uploading to S3, only the timing of the notification.

5. Choose **Save**.

## Refreshing objects in your Amazon S3 bucket

As your NFS or SMB client performs file system operations, your gateway maintains an inventory of the objects in the S3 bucket associated with your file share. Your gateway uses this cached inventory to reduce the latency and frequency of S3 requests. This operation does not import files into the file gateway cache storage. It only updates the cached inventory to reflect changes in the inventory of the objects in the S3 bucket.

To refresh the S3 bucket for your file share, you can use the Storage Gateway console, the [RefreshCache](#) operation in the Storage Gateway API, or an AWS Lambda function.

### To refresh objects in an S3 bucket from the console

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **File shares**, and then choose the file share associated with the S3 bucket that you want to refresh.
3. For **Actions**, choose **Refresh cache**.

The time that the refresh process takes depends on the number of objects cached on the gateway and the number of objects that were added to or removed from the S3 bucket.

### To refresh objects in an S3 bucket using an AWS Lambda function

1. Identify the S3 bucket used by the file gateway.
2. Check that the *Event* section is blank. It populates automatically later.
3. Create an IAM role, and allow Trust Relationship for Lambda `lambda.amazonaws.com`.
4. Use the following policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "StorageGatewayPermissions",  
            "Effect": "Allow",  
            "Action": "storagegateway:RefreshCache",  
            "Resource": "arn:aws:storagegateway:  
                <region>:  
                <account>:fileshare/  
                <fileshare-id>"  
        }  
    ]  
}
```

```

        "Resource": "*"
    },
{
    "Sid": "CloudWatchLogsPermissions",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource": "*"
}
]
}

```

5. Create a Lambda function from the Lambda console.
6. Use the following function for your Lambda task.

```

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

```

7. For **Execution role**, choose the IAM role you created.
8. Optional: add a trigger for Amazon S3 and select the event **ObjectCreated** or **ObjectRemoved**.

**Note**

RefreshCache needs to complete one process before starting another. When you create or delete many objects in a bucket, performance might degrade. Therefore, we recommend against using S3 triggers. Instead, use the Amazon CloudWatch rule described following.

9. Create a CloudWatch rule on the CloudWatch console and add a schedule. Generally, we recommend a *fixed rate* of 30 minutes. However, you can use 1-2 hours on large S3 bucket.
10. Add a new trigger for CloudWatch events and choose the rule you just created.
11. Save your Lambda configuration. Choose **Test**.
12. Choose **S3 PUT** and customize the test to your requirements.
13. The test should succeed. If not, modify the JSON to your requirements and retest.
14. Open the Amazon S3 console, and verify that the event your created and the Lambda function ARN are present.
15. Upload an object to your S3 bucket using the Amazon S3 console or the AWS CLI.

The CloudWatch console generates a CloudWatch output similar to the following.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
        u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f', u'object':
        {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-NAME',
        u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}}, u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
        u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgsfq+IhvAg5M=',
        u'x-amz-request-id': u'651C2D4101D31593'}
    ]
}
```

```
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
        u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
        u'eventSource': u'aws:s3'}
    ]
}
```

The Lambda invocation gives you output similar to the following.

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

Your NFS share mounted on your client will reflect this update.

**Note**

For caches updating large object creation or deletion in large buckets with millions of objects, updates may take hours.

16. Delete your object manually using the Amazon S3 console or AWS CLI.
17. View the NFS share mounted on your client. Verify that your object is gone (because your cache refreshed).
18. Check your CloudWatch logs to see the log of your deletion with the event `ObjectRemoved:Delete`.

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

**Note**

For cron jobs or scheduled tasks, your CloudWatch log event is `u'detail-type': u'Scheduled Event'`.

Refreshing the cache only initiates the refresh operation. When the cache refresh completes, it doesn't necessarily mean that the file refresh is complete. To determine that the file refresh operation is complete before you check for new files on the gateway file share, use the `refresh-complete` notification. To do this, you can subscribe to be notified through an Amazon CloudWatch event when your [RefreshCache](#) operation completes. For more information, see [Getting notified about file operations \(p. 227\)](#).

## Using S3 object lock with a file gateway

File gateway supports accessing S3 buckets that have Amazon S3 Object Lock enabled. Amazon S3 Object Lock enables you to store objects using a "Write Once Read Many" (WORM) model. When you use Amazon S3 Object Lock, you can prevent an object in your S3 bucket from being deleted or overwritten. Amazon S3 Object Lock works together with object versioning to protect your data.

If you enable Amazon S3 Object Lock, you can still modify the object. For example, it can be written to, deleted, or renamed through a file share on a file gateway. When you modify an object in this way, file gateway places a new version of the object without affecting the previous version (that is, the locked object).

For example, If you use the file gateway NFS or SMB interface to delete a file and the corresponding S3 object is locked, the gateway places an S3 delete marker as the next version of the object, and leaves the original object version in place. Similarly, If a file gateway modifies the contents or metadata of a locked object, a new version of the object is uploaded with the changes, but the original locked version of the object remains unchanged.

For more information about Amazon S3 Object Lock, see [Locking objects using S3 Object Lock](#) in the *Amazon Simple Storage Service User Guide*.

## Understanding file share status

Each file share has an associated status that tells you at a glance what the health of the file share is. Most of the time, the status indicates that the file share is functioning normally and that no action is needed on your part. In some cases, the status indicates a problem that might or might not require action on your part.

You can see file share status on the Storage Gateway console. File share status appears in the **Status** column for each file share in your gateway. A file share that is functioning normally has the status of AVAILABLE.

In the following table, you can find a description of each file share status, and if and when you should act based on the status. A file share should have AVAILABLE status all or most of the time it's in use.

Status	Meaning
AVAILABLE	The file share is configured properly and is available to use. The AVAILABLE status is the normal running status for a file share.
CREATING	The file share is being created and is not ready for use. The CREATING status is transitional. No action is required. If file share is stuck in this status, it's probably because the gateway VM lost connection to AWS.
UPDATING	The file share configuration is being updated. If a file share is stuck in this status, it's probably because the gateway VM lost connection to AWS.
DELETING	The file share is being deleted. The file share is not deleted until all data is uploaded to AWS. The DELETING status is transitional, and no action is required.
FORCE_DELETING	The file share is being deleted forcibly. The file share is deleted immediately and uploading to AWS is aborted. The FORCE_DELETING status is transitional, and no action is required.
UNAVAILABLE	The file share is in an unhealthy state. Certain issues can cause the file share to go into an unhealthy state. For example, role policy errors can cause this, or if the file share maps to an Amazon S3 bucket that doesn't exist. When the issue that caused the unhealthy state is resolved, the file returns to AVAILABLE state.

## File share best practices

In this section, you can find information about best practices for creating file shares.

#### Topics

- [Preventing multiple file shares writing to your Amazon S3 bucket \(p. 177\)](#)
- [Allowing specific NFS clients to mount your file share \(p. 177\)](#)

## Preventing multiple file shares writing to your Amazon S3 bucket

When you create a file share, we recommend that you configure your Amazon S3 bucket so that only one file share can write to it. If you configure your S3 bucket to be written to by multiple file shares, unpredictable results can occur. To prevent this, create an S3 bucket policy that denies all roles except the role used for the file share to put or delete objects in the bucket. Then attach this policy to the S3 bucket.

The following example policy denies all roles except the role that created the bucket to write to the S3 bucket. The `s3:DeleteObject` and `s3:PutObject` actions are denied for all roles except "TestUser". The policy applies to all objects in the "`arn:aws:s3:::TestBucket/*`" bucket.

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

## Allowing specific NFS clients to mount your file share

We recommend that you change the allowed NFS client settings for your file share. If you don't, any client on your network can mount your file share. For information about how to edit your NFS client settings, see [Editing access settings for your NFS file share \(p. 168\)](#).

# Managing Your Volume Gateway

Following, you can find information about how to manage your volume gateway resources.

Cached volumes are volumes in Amazon Simple Storage Service (Amazon S3) that are exposed as iSCSI targets on which you can store your application data. You can find information following about how to add and delete volumes for your cached setup. You can also learn how to add and remove Amazon Elastic Block Store (Amazon EBS) volumes in Amazon EC2 gateways.

#### Topics

- [Adding a Volume \(p. 178\)](#)

- [Expanding the Size of a Volume \(p. 178\)](#)
- [Cloning a Volume \(p. 179\)](#)
- [Viewing Volume Usage \(p. 181\)](#)
- [Deleting a Volume \(p. 181\)](#)
- [Moving Your Volumes to a Different Gateway \(p. 182\)](#)
- [Reducing the Amount of Billed Storage on a Volume \(p. 184\)](#)
- [Creating a One-Time Snapshot \(p. 184\)](#)
- [Editing a Snapshot Schedule \(p. 184\)](#)
- [Deleting a Snapshot \(p. 185\)](#)
- [Understanding Volume Statuses and Transitions \(p. 193\)](#)

**Important**

If a cached volume keeps your primary data in Amazon S3, you should avoid processes that read or write all data on the entire volume. For example, we don't recommend using virus-scanning software that scans the entire cached volume. Such a scan, whether done on demand or scheduled, causes all data stored in Amazon S3 to be downloaded locally for scanning, which results in high bandwidth usage. Instead of doing a full disk scan, you can use real-time virus scanning—that is, scanning data as it is read from or written to the cached volume.

Resizing a volume is not supported. To change the size of a volume, create a snapshot of the volume, and then create a new cached volume from the snapshot. The new volume can be bigger than the volume from which the snapshot was created. For steps describing how to remove a volume, see [To remove a volume \(p. 182\)](#). For steps describing how to add a volume and preserve existing data, see [Deleting a Volume \(p. 181\)](#).

All cached volume data and snapshot data is stored in Amazon S3 and is encrypted at rest using server-side encryption (SSE). However, you cannot access this data by using the Amazon S3 API or other tools such as the Amazon S3 Management Console.

## Adding a Volume

As your application needs grow, you might need to add more volumes to your gateway. As you add more volumes, you must consider the size of the cache storage and upload buffer you allocated to the gateway. The gateway must have sufficient buffer and cache space for new volumes. For more information, see [Determining the size of upload buffer to allocate \(p. 255\)](#).

You can add volumes using the Storage Gateway console or Storage Gateway API. For information on using the Storage Gateway API to add volumes, see [CreateCachediSCSIVolume](#). For instructions on how to add a volume using the Storage Gateway console, see [Creating a volume \(p. 72\)](#).

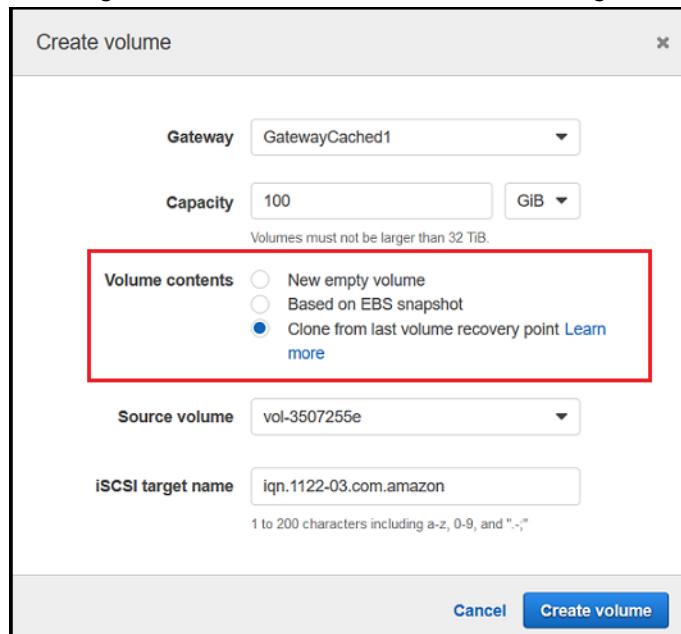
## Expanding the Size of a Volume

As your application needs grow, you might want to expand your volume instead of adding more volumes to your gateway. In this case, you can do one of the following:

- Create a snapshot of the volume you want to expand and then use the snapshot to create a new volume of a larger size. For information about how to create a snapshot, see [Creating a One-Time Snapshot \(p. 184\)](#). For information about how to use a snapshot to create a new volume, see [Creating a volume \(p. 72\)](#).
- Use the cached volume you want to expand to clone a new volume of a larger size. For information about how to clone a volume, see [Cloning a Volume \(p. 179\)](#). For information about how to create a volume, see [Creating a volume \(p. 72\)](#).

## Cloning a Volume

You can create a new volume from any existing cached volume in the same AWS Region. The new volume is created from the most recent recovery point of the selected volume. A *volume recovery point* is a point in time at which all data of the volume is consistent. To clone a volume, you choose the **Clone from last recovery point** option in the **Create volume** dialog box, then select the volume to use as the source. The following screenshot shows the **Create volume** dialog box.



Cloning from an existing volume is faster and more cost-effective than creating an Amazon EBS snapshot. Cloning does a byte-to-byte copy of your data from the source volume to the new volume, using the most recent recovery point from the source volume. Storage Gateway automatically creates recovery points for your cached volumes. To see when the last recovery point was created, check the `TimeSinceLastRecoveryPoint` metric in Amazon CloudWatch.

The cloned volume is independent of the source volume. That is, changes made to either volume after cloning have no effect on the other. For example, if you delete the source volume, it has no effect on the cloned volume. You can clone a source volume while initiators are connected and it is in active use. Doing so doesn't affect the performance of the source volume. For information about how to clone a volume, see [Creating a volume \(p. 72\)](#).

You can also use the cloning process in recovery scenarios. For more information, see [Your Cached Gateway is Unreachable And You Want to Recover Your Data \(p. 380\)](#).

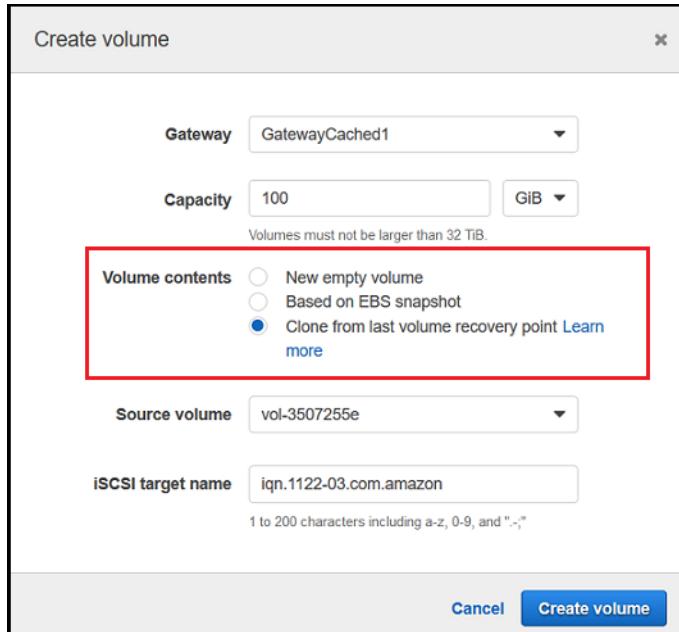
## Cloning from a Volume Recovery Point

The following procedure shows you how to clone a volume from a volume recovery point and use that volume.

### To clone and use a volume from an unreachable gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the Storage Gateway console, choose **Create volume**.
3. In the **Create volume** dialog box, choose a gateway for **Gateway**.

4. For **Capacity**, type the capacity for your volume. The capacity must be at least the same size as the source volume.
5. Choose **Clone from last recovery point** and select a volume ID for **Source volume**. The source volume can be any cached volume in the selected AWS Region.



6. Type a name for **iSCSI target name**.

The target name can contain lowercase letters, numbers, periods (.), and hyphens (-). This target name appears as the **iSCSI target node name** in the **Targets** tab of the **iSCSI Microsoft initiator UI** after discovery. For example, the name `target1` appears as `iqn.1007-05.com.amazon:target1`. Ensure that the target name is globally unique within your storage area network (SAN).

7. Verify that the **Network interface** setting is the IP address of your gateway, or choose an IP address for **Network interface**.

If you have defined your gateway to use multiple network adapters, choose the IP address that your storage applications use to access the volume. Each network adapter defined for a gateway represents one IP address that you can choose.

If the gateway VM is configured for more than one network adapter, the **Create volume** dialog box displays a list for **Network interface**. In this list, one IP address appears for each adapter configured for the gateway VM. If the gateway VM is configured for only one network adapter, no list appears because there's only one IP address.

8. Choose **Create volume**. The **Configure CHAP Authentication** dialog box appears. You can configure CHAP later. For information, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).

The next step is to connect your volume to your client. For more information, see [Connecting Your Volumes to Your Client \(p. 75\)](#).

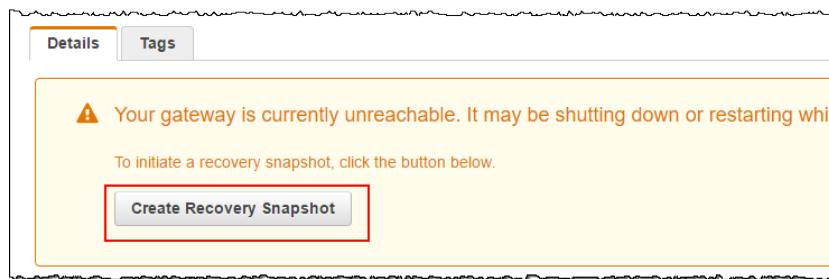
## Creating a Recovery Snapshot

The following procedure shows you how to create a snapshot from a volume recovery point and using that snapshot. You can take snapshots on a one-time, ad hoc basis or set up a snapshot schedule for the volume.

### To create and use a recovery snapshot of a volume from an unreachable gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**.
3. Choose the unreachable gateway, and then choose the **Details** tab.

A recovery snapshot message is displayed in the tab.



4. Choose **Create recovery snapshot** to open the **Create recovery snapshot** dialog box.
  5. From the list of volumes displayed, choose the volume you want to recover, and then choose **Create snapshots**.
- Storage Gateway initiates the snapshot process.
6. Find and restore the snapshot.

## Viewing Volume Usage

When you write data to a volume, you can view the amount of data stored on the volume in the Storage Gateway Management Console. The **Details** tab for each volume shows the volume usage information.

### To view amount of data written to a volume

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Volumes** and then choose the volume you are interested in.
3. Choose the **Details** tab.

The following fields provide information about the volume:

- **Size:** The total capacity of the selected volume.
- **Used:** The size of data stored on the volume.

#### Note

These values are not available for volumes created before May 13, 2015, until you store data on the volume.

## Deleting a Volume

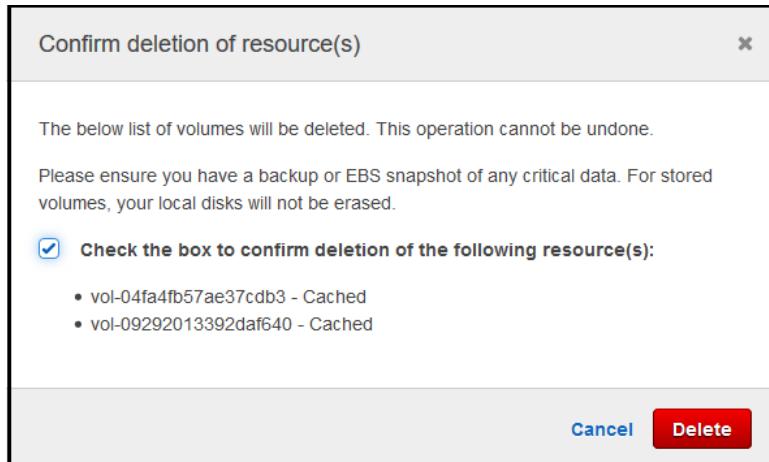
You might need to delete a volume as your application needs change—for example, if you migrate your application to use a larger storage volume. Before you delete a volume, make sure that there are no applications currently writing to the volume. Also, make sure that there are no snapshots in progress for the volume. If a snapshot schedule is defined for the volume, you can check it on the **Snapshot Schedules** tab of the Storage Gateway console. For more information, see [Editing a Snapshot Schedule \(p. 184\)](#).

You can delete volumes using the Storage Gateway console or the Storage Gateway API. For information on using the Storage Gateway API to remove volumes, see [Delete Volume](#). The following procedure demonstrates using the console.

Before you delete a volume, back up your data or take a snapshot of your critical data. For stored volumes, your local disks aren't erased. After you delete a volume, you can't get it back.

### To remove a volume

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the **Volumes** tab, choose the volume and choose the confirmation box. Make sure that the volume listed is the volume you intend to delete.



3. Choose **Delete** to delete the volume.

## Moving Your Volumes to a Different Gateway

As your data and performance needs grow, you might want to move your volumes to a different volume gateway. To do so, you can detach and attach a volume by using the Storage Gateway console or API.

By detaching and attaching a volume, you can do the following:

- Move your volumes to better host platforms or newer Amazon EC2 instances.
- Refresh the underlying hardware for your server.
- Move your volumes between hypervisor types.

When you detach a volume, your gateway uploads and stores the volume data and metadata to the Storage Gateway service in AWS. You can easily attach a detached volume to a gateway on any supported host platform later.

#### Note

A detached volume is billed at the standard volume storage rate until you delete it. For information about how to reduce your bill, see [Reducing the Amount of Billed Storage on a Volume \(p. 184\)](#).

#### Note

There are some limitations for attaching and detaching volumes:

- Detaching a volume can take a long time. When you detach a volume, the gateway uploads all the data on the volume to AWS before the volume is detached. The time it takes for the

upload to complete depends on how much data needs to be uploaded and your network connectivity into AWS.

- If you detach a cached volume, you can't reattach it as a stored volume.
- If you detach a stored volume, you can't reattach it as a cached volume.
- A detached volume can't be used until it is attached to a gateway.
- When you attach a stored volume, it needs to fully restore before you can attach it to a gateway.
- When you start attaching or detaching a volume, you need to wait till the operation completed before you use the volume.
- Currently, forcibly deleting a volume is only supported in the API.
- If you delete a gateway while your volume is detaching from that gateway, it results in data loss. Wait until the volume detach operation is complete before you delete the gateway.
- If a stored gateway is in restoring state, you can't detach a volume from it.

The following steps show you how to detach and attach a volume using the Storage Gateway console. For more information about doing this using the API, see [DetachVolume](#) or [AttachVolume](#) in the [AWS Storage Gateway API Reference](#).

### To detach a volume from a gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the navigation pane, choose **Volumes**.
3. From the list of volumes, choose the volume that you want to detach. You can choose multiple volumes to detach multiple volumes at a time.
4. For **Actions**, choose **Detach volume**. The volumes that you chose are listed in the **Detach Volume** dialog box that appears. Make sure that only the volumes you want to detach are listed.
5. Choose **Detach volume**. If a volume that you detach has a lot of data on it, it transitions from **Attached** to **Detaching** status until it finishes uploading all the data. Then the status changes to **Detached**. For small amounts of data, you might not see the **Detaching** status. If the volume doesn't have data on it, the status changes from **Attached** to **Detached**.

You can now attach the volume to a different gateway.

### To attach a volume to a gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the navigation pane, choose **Volumes**. The status of each volume that is detached shows as **Detached**.
3. From the list of detached volumes, choose the volume that you want to attach. You can attach only one volume at a time.
4. For **Actions**, choose **Attach volume**.
5. In the **Attach Volume** dialog box, choose the gateway that you want to attach the volume to, and then enter the iSCSI target that you want to connect the volume to.

If you are attaching a stored volume, enter its disk identifier for **Disk ID**.

6. Choose **Attach volume**. If a volume that you attach has a lot of data on it, it transitions from **Detached** to **Attached** if the **AttachVolume** operation succeeds.
7. In the Configure CHAP authentication wizard that appears, enter the **Initiator name**, **Initiator secret**, and **Target secret**, and then choose **Save**. For more information about working with Challenge-Handshake Authentication Protocol (CHAP) authentication, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).

## Reducing the Amount of Billed Storage on a Volume

Deleting files from your file system doesn't necessarily delete data from the underlying block device or reduce the amount of data stored on your volume. If you want to reduce the amount of billed storage on your volume, we recommend overwriting your files with zeros to compress the storage to a negligible amount of actual storage. Storage Gateway charges for volume usage based on compressed storage.

**Note**

If you use a delete tool that overwrites the data on your volume with random data, your usage will not be reduced. This is because the random data is not compressible.

## Creating a One-Time Snapshot

In addition to scheduled snapshots, for volume gateways you can take one-time, ad hoc snapshots. By doing this, you can back up your storage volume immediately without waiting for the next scheduled snapshot.

### To take a one-time snapshot of your storage volume

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Volumes**, and then choose the volume you want to create the snapshot from.
3. For **Actions**, choose **Create snapshot**.
4. In the **Create snapshot** dialog box, type the snapshot description, and then choose **Create snapshot**.

You can verify that the snapshot was created using the console.

Your snapshot is listed in the **Snapshots** in the same row as the volume.

## Editing a Snapshot Schedule

For stored volumes, AWS Storage Gateway creates a default snapshot schedule of once a day.

**Note**

You can't remove the default snapshot schedule. Stored volumes require at least one snapshot schedule. However, you can change a snapshot schedule by specifying either the time the snapshot occurs each day or the frequency (every 1, 2, 4, 8, 12, or 24 hours), or both.

For cached volumes, AWS Storage Gateway doesn't create a default snapshot schedule. No default schedule is created because your data is stored in Amazon S3, so you don't need snapshots or a snapshot schedule for disaster recovery purposes. However, you can set up a snapshot schedule at any time if you need to. Creating snapshot for your cached volume provides an additional way to recover your data if necessary.

By using the following steps, you can edit the snapshot schedule for a volume.

### To edit the snapshot schedule for a volume

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Volumes**, and then choose the volume the snapshot was created from.
3. For **Actions**, choose **Edit snapshot schedule**.
4. In the **Edit snapshot schedule** dialog box, modify the schedule, and then choose **Save**.

## Deleting a Snapshot

You can delete a snapshot of your storage volume. For example, you might want to do this if you have taken many snapshots of a storage volume over time and you don't need the older snapshots. Because snapshots are incremental backups, if you delete a snapshot, only the data that is not needed in other snapshots is deleted.

### Topics

- [Deleting Snapshots by Using the AWS SDK for Java \(p. 185\)](#)
- [Deleting Snapshots by Using the AWS SDK for .NET \(p. 187\)](#)
- [Deleting Snapshots by Using the AWS Tools for Windows PowerShell \(p. 192\)](#)

On the Amazon EBS console, you can delete snapshots one at a time. For information about how to delete snapshots using the Amazon EBS console, see [Deleting an Amazon EBS Snapshot](#) in the *Amazon EC2 User Guide*.

To delete multiple snapshots at a time, you can use one of the AWS SDKs that supports Storage Gateway operations. For examples, see [Deleting Snapshots by Using the AWS SDK for Java \(p. 185\)](#), [Deleting Snapshots by Using the AWS SDK for .NET \(p. 187\)](#), and [Deleting Snapshots by Using the AWS Tools for Windows PowerShell \(p. 192\)](#).

## Deleting Snapshots by Using the AWS SDK for Java

To delete many snapshots associated with a volume, you can use a programmatic approach. The example following demonstrates how to delete snapshots using the AWS SDK for Java. To use the example code, you should be familiar with running a Java console application. For more information, see [Getting Started](#) in the *AWS SDK for Java Developer Guide*. If you need to just delete a few snapshots, use the console as described in [Deleting a Snapshot \(p. 185\)](#).

### Example : Deleting Snapshots by Using the AWS SDK for Java

The following Java code example lists the snapshots for each volume of a gateway and whether the snapshot start time is before or after a specified date. It uses the AWS SDK for Java API for Storage Gateway and Amazon EC2. The Amazon EC2 API includes operations for working with snapshots.

Update the code to provide the service endpoint, your gateway Amazon Resource Name (ARN), and the number of days back you want to save snapshots. Snapshots taken before this cutoff are deleted. You also need to specify the Boolean value `viewOnly`, which indicates whether you want to view the snapshots to be deleted or to actually perform the snapshot deletions. Run the code first with just the `view` option (that is, with `viewOnly` set to `true`) to see what the code deletes. For a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the *AWS General Reference*.

```
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.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    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;
    }
}

```

## Deleting Snapshots by Using the AWS SDK for .NET

To delete many snapshots associated with a volume, you can use a programmatic approach. The following example demonstrates how to delete snapshots using the AWS SDK for .NET version 2 and

3. To use the example code, you should be familiar with running a .NET console application. For more information, see [Getting Started](#) in the *AWS SDK for .NET Developer Guide*. If you need to just delete a few snapshots, use the console as described in [Deleting a Snapshot \(p. 185\)](#).

### Example : Deleting Snapshots by Using the AWS SDK for .NET

In the following C# code example, an AWS Identity and Access Management (IAM) user can list the snapshots for each volume of a gateway. The user can then determine whether the snapshot start time is before or after a specified date (retention period) and delete snapshots that have passed the retention period. The example uses the AWS SDK for .NET API for Storage Gateway and Amazon EC2. The Amazon EC2 API includes operations for working with snapshots.

The following code example uses the AWS SDK for .NET version 2 and 3. You can migrate older versions of .NET to the newer version. For more information, see [Migrating Your Code to the Latest Version of the AWS SDK for .NET](#).

Update the code to provide the service endpoint, your gateway Amazon Resource Name (ARN), and the number of days back you want to save snapshots. Snapshots taken before this cutoff are deleted. You also need to specify the Boolean value `viewOnly`, which indicates whether you want to view the snapshots to be deleted or to actually perform the snapshot deletions. Run the code first with just the `view` option (that is, with `viewOnly` set to `true`) to see what the code deletes. For a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the [AWS General Reference](#).

First, you create an IAM user and attach the minimum IAM policy to the IAM user. Then you schedule automated snapshots for your gateway.

The following code creates the minimum policy that allows an IAM user to delete snapshots. In this example, the policy is named **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": [  
                "*"  
            ]  
        }  
    ]  
}
```

The following C# code finds all snapshots in the specified gateway that match the volumes and the specified cut-off period and then deletes them.

```
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;
    }
}
```

## Deleting Snapshots by Using the AWS Tools for Windows PowerShell

To delete many snapshots associated with a volume, you can use a programmatic approach. The example following demonstrates how to delete snapshots using the AWS Tools for Windows PowerShell. To use the example script, you should be familiar with running a PowerShell script. For more information, see [Getting Started](#) in the *AWS Tools for Windows PowerShell*. If you need to delete just a few snapshots, use the console as described in [Deleting a Snapshot \(p. 185\)](#).

### Example : Deleting Snapshots by Using the AWS Tools for Windows PowerShell

The following PowerShell script example lists the snapshots for each volume of a gateway and whether the snapshot start time is before or after a specified date. It uses the AWS Tools for Windows PowerShell cmdlets for Storage Gateway and Amazon EC2. The Amazon EC2 API includes operations for working with snapshots.

You need to update the script and provide your gateway Amazon Resource Name (ARN) and the number of days back you want to save snapshots. Snapshots taken before this cutoff are deleted. You also need to specify the Boolean value `viewOnly`, which indicates whether you want to view the snapshots to be deleted or to actually perform the snapshot deletions. Run the code first with just the `view` option (that is, with `viewOnly` set to `true`) to see what the code deletes.

```
<#
.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)
    }
}

```

## Understanding Volume Statuses and Transitions

Each volume has an associated status that tells you at a glance what the health of the volume is. Most of the time, the status indicates that the volume is functioning normally and that no action is needed on your part. In some cases, the status indicates a problem with the volume that might or might not require action on your part. You can find information following to help you decide when you need to act. You can see volume status on the Storage Gateway console or by using one of the Storage Gateway API operations, for example [DescribeCachediSCSIVolumes](#) or [DescribeStorediSCSIVolumes](#).

### Topics

- [Understanding Volume Status \(p. 193\)](#)
- [Understanding Attachment Status \(p. 196\)](#)
- [Understanding Cached Volume Status Transitions \(p. 196\)](#)
- [Understanding Stored Volume Status Transitions \(p. 198\)](#)

## Understanding Volume Status

The following table shows volume status on the Storage Gateway console. Volume status appears in the **Status** column for each storage volume on your gateway. A volume that is functioning normally has a status of **Available**.

In the following table, you can find a description of each storage volume status, and if and when you should act based on each status. The **Available** status is the normal status of a volume. A volume should have this status all or most of the time it's in use.

Status	Meaning
<b>Available</b>	<p>The volume is available for use. This status is the normal running status for a volume.</p> <p>When a <b>Bootstrapping</b> phase is completed, the volume returns to <b>Available</b> state. That is, the gateway has synchronized any changes made to the volume since it first entered <b>Pass Through</b> status.</p>
<b>Bootstrapping</b>	<p>The gateway is synchronizing data locally with a copy of the data stored in AWS. You typically don't need to take action for this status, because the storage volume automatically sees the <b>Available</b> status in most cases.</p> <p>The following are scenarios when a volume status is <b>Bootstrapping</b>:</p> <ul style="list-style-type: none"> <li>A gateway has unexpectedly shut down.</li> <li>A gateway's upload buffer has been exceeded. In this scenario, bootstrapping occurs when your volume has the <b>Pass Through</b> status and the amount of free upload buffer increases sufficiently. You can provide additional upload buffer space as one way to increase the percentage of free upload buffer space. In this particular scenario, the storage volume goes from <b>Pass Through</b> to <b>Bootstrapping</b> to <b>Available</b> status. You can continue to use this volume during this bootstrapping period. However, you can't take snapshots of the volume at this point.</li> <li>You are creating a stored volume gateway and preserving existing local disk data. In this scenario, your gateway starts uploading all of the data to AWS. The volume has the <b>Bootstrapping</b> status until all of the data from the local disk is copied to AWS. You can use the volume during this bootstrapping period. However, you can't take snapshots of the volume at this point.</li> </ul>
<b>Creating</b>	<p>The volume is currently being created and is not ready for use. The <b>Creating</b> status is transitional. No action is required.</p>
<b>Deleting</b>	<p>The volume is currently being deleted. The <b>Deleting</b> status is transitional. No action is required.</p>
<b>Irrecoverable</b>	<p>An error occurred from which the volume cannot recover. For information on what to do in this situation, see <a href="#">Troubleshooting volume issues (p. 379)</a>.</p>
<b>Pass Through</b>	<p>Data maintained locally is out of sync with data stored in AWS. Data written to a volume while the volume is in <b>Pass Through</b> status remains in the cache until the volume status is <b>Bootstrapping</b>. This data starts to upload to AWS when <b>Bootstrapping</b> status begins.</p> <p>The <b>Pass Through</b> status can occur for several reasons, listed following:</p> <ul style="list-style-type: none"> <li>The <b>Pass Through</b> status occurs if your gateway has run out of upload buffer space. Your applications can continue to read from and write data to your storage volumes while the volumes have the <b>Pass Through</b> status. However, the gateway isn't writing any of your volume data to its upload buffer or uploading any of this data to AWS.</li> </ul>

Status	Meaning
	<p>The gateway continues to upload any data written to the volume before the volume entered the <b>Pass Through</b> status. Any pending or scheduled snapshots of a storage volume fail while the volume has the <b>Pass Through</b> status. For information about what to do when your storage volume has the <b>Pass Through</b> status because the upload buffer has been exceeded, see <a href="#">Troubleshooting volume issues (p. 379)</a>.</p> <p>To return to ACTIVE status, a volume in <b>Pass Through</b> must complete the <b>Bootstrapping</b> phase. During <b>Bootstrapping</b>, the volume re-establishes synchronization within AWS, so that it can resume the record (log) of changes to the volume, and re-enable <code>CreateSnapshot</code> functionality. During <b>Bootstrapping</b>, writes to the volume are recorded in upload buffer.</p> <ul style="list-style-type: none"> <li>The <b>Pass Through</b> status occurs when there is more than one storage volume bootstrapping at once. Only one gateway storage volume can bootstrap at a time. For example, suppose that you create two storage volumes and choose to preserve existing data on both of them. In this case, the second storage volume has the <b>Pass Through</b> status until the first storage volume finishes bootstrapping. In this scenario, you don't need to act. Each storage volume changes to the <b>Available</b> status automatically when it is finished being created. You can read and write to the storage volume while it has the <b>Pass Through</b> or <b>Bootstrapping</b> status.</li> <li>Infrequently, the <b>Pass Through</b> status can indicate that a disk allocated for upload buffer use has failed. For information about what action to take in this scenario, see <a href="#">Troubleshooting volume issues (p. 379)</a>.</li> <li>The <b>Pass Through</b> status can occur when a volume is in <b>Active</b> or <b>Bootstrapping</b> state. In this case, the volume receives a write, but the upload buffer has insufficient capacity to record (log) that write.</li> <li>The <b>Pass Through</b> status occurs when a volume is in any state and the gateway is not shut down cleanly. This type of shutdown can happen because the software crashed or the VM was powered off. In this case, a volume in any state transitions to <b>Pass Through</b> status.</li> </ul>
<b>Restoring</b>	<p>The volume is being restored from an existing snapshot. This status applies only for stored volumes. For more information, see <a href="#">How Storage Gateway works (architecture) (p. 3)</a>.</p> <p>If you restore two storage volumes at the same time, both storage volumes show <b>Restoring</b> as their status. Each storage volume changes to the <b>Available</b> status automatically when it is finished being created. You can read and write to a storage volume and take a snapshot of it while it has the <b>Restoring</b> status.</p>

Status	Meaning
<b>Restoring Pass Through</b>	<p>The volume is being restored from an existing snapshot and has encountered an upload buffer issue. This status applies only for stored volumes. For more information, see <a href="#">How Storage Gateway works (architecture) (p. 3)</a>.</p> <p>One reason that can cause the <b>Restoring Pass Through</b> status is if your gateway has run out of upload buffer space. Your applications can continue to read from and write data to your storage volumes while they have the <b>Restoring Pass Through</b> status. However, you can't take snapshots of a storage volume during the <b>Restoring Pass Through</b> status period. For information about what action to take when your storage volume has the <b>Restoring Pass Through</b> status because upload buffer capacity has been exceeded, see <a href="#">Troubleshooting volume issues (p. 379)</a>.</p> <p>Infrequently, the <b>Restoring Pass Through</b> status can indicate that a disk allocated for an upload buffer has failed. For information about what action to take in this scenario, see <a href="#">Troubleshooting volume issues (p. 379)</a>.</p>
<b>Upload Buffer Not Configured</b>	You can't create or use the volume because the gateway doesn't have an upload buffer configured. For information on how to add upload buffer capacity for volumes in a cached volume setup, see <a href="#">Determining the size of upload buffer to allocate (p. 255)</a> . For information on how to add upload buffer capacity for volumes in a stored volume setup, see <a href="#">Determining the size of upload buffer to allocate (p. 255)</a> .

## Understanding Attachment Status

You can detach a volume from a gateway or attach it to a gateway by using the Storage Gateway console or API. The following table shows volume attachment status on the Storage Gateway console. Volume attachment status appears in the **Attachment status** column for each storage volume on your gateway. For example, a volume that is detached from a gateway has a status of **Detached**. For information about how to detach and attach a volume, see [Moving Your Volumes to a Different Gateway \(p. 182\)](#).

Status	Meaning
<b>Attached</b>	The volume is attached to a gateway.
<b>Detached</b>	The volume is detached from a gateway.
<b>Detaching</b>	The volume is being detached from a gateway. When you are detaching a volume and the volume doesn't have data on it, you might not see this status.

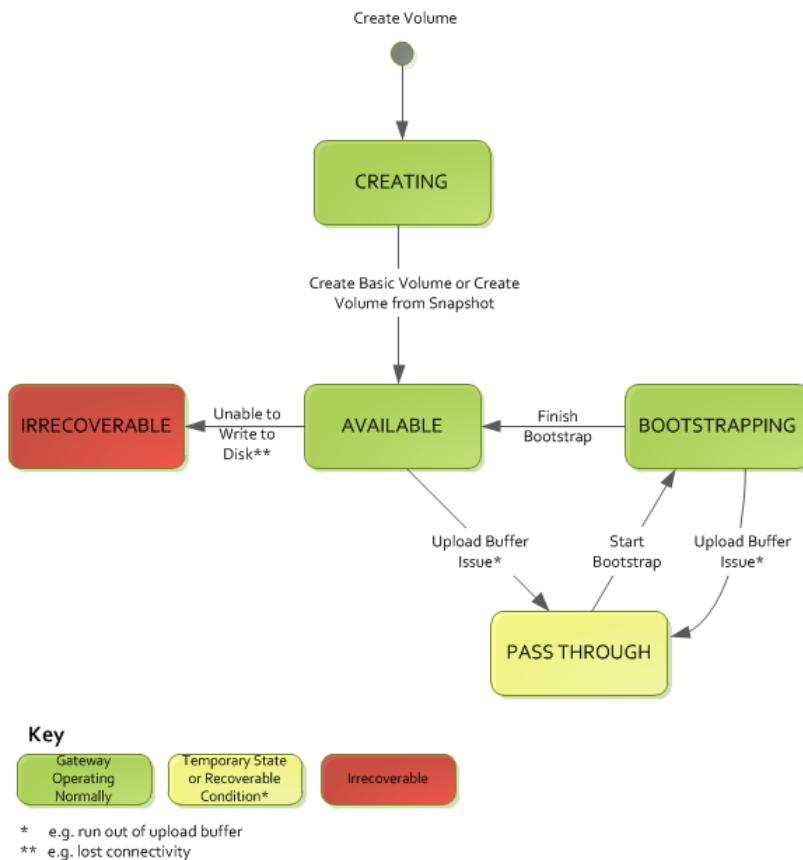
## Understanding Cached Volume Status Transitions

Use the following state diagram to understand the most common transitions between statuses for volumes in cached gateways. You don't need to understand the diagram in detail to use your gateway effectively. Rather, the diagram provides detailed information if you are interested in knowing more about how volume gateways work.

The diagram doesn't show the **Upload Buffer Not Configured** status or the **Deleting** status. Volume states in the diagram appear as green, yellow, and red boxes. You can interpret the colors as described following.

Color	Volume Status
Green	The gateway is operating normally. The volume status is <b>Available</b> or eventually becomes <b>Available</b> .
Yellow	The volume has the <b>Pass Through</b> status, which indicates there is a potential issue with the storage volume. If this status appears because the upload buffer space is filled, then in some cases buffer space becomes available again. At that point, the storage volume self-corrects to the <b>Available</b> status. In other cases, you might have to add more upload buffer space to your gateway to allow the storage volume status to become <b>Available</b> . For information on how to troubleshoot a case when upload buffer capacity has been exceeded, see <a href="#">Troubleshooting volume issues (p. 379)</a> . For information on how to add upload buffer capacity, see <a href="#">Determining the size of upload buffer to allocate (p. 255)</a> .
Red	The storage volume has the <b>Irrecoverable</b> status. In this case, you should delete the volume. For information on how to do this, see <a href="#">To remove a volume (p. 182)</a> .

In the diagram, a transition between two states is depicted with a labeled line. For example, the transition from the **Creating** status to the **Available** status is labeled as *Create Basic Volume or Create Volume from Snapshot*. This transition represents creating a cached volume. For more information about creating storage volumes, see [Adding a Volume \(p. 178\)](#).



#### Note

The volume status of **Pass Through** appears as yellow in this diagram. However, this doesn't match the color of this status icon in the **Status** box of the Storage Gateway console.

## Understanding Stored Volume Status Transitions

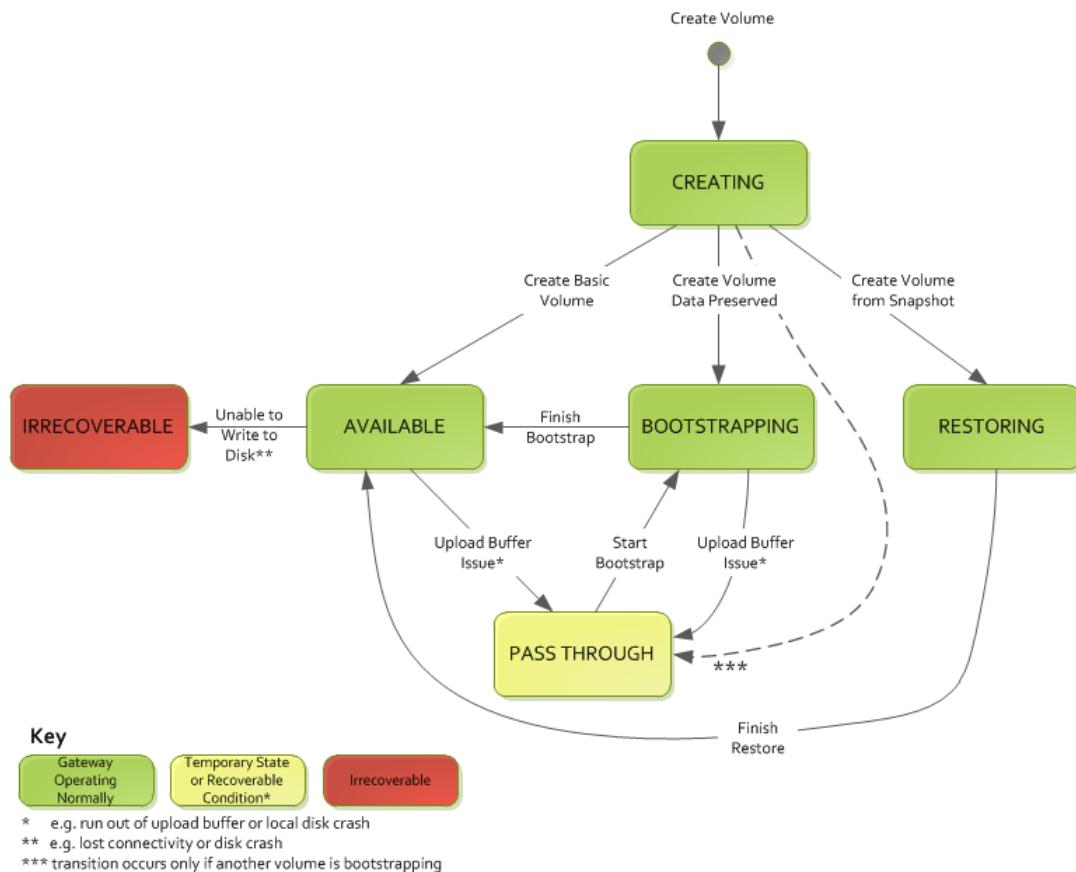
Use the following state diagram to understand the most common transitions between statuses for volumes in stored gateways. You don't need to understand the diagram in detail to use your gateway effectively. Rather, the diagram provides detailed information if you are interested in understanding more about how volume gateways work.

The diagram doesn't show the **Upload Buffer Not Configured** status or the **Deleting** status. Volume states in the diagram appear as green, yellow, and red boxes. You can interpret the colors as described following.

Color	Volume Status
<b>Green</b>	The gateway is operating normally. The volume status is <b>Available</b> or eventually becomes <b>Available</b> .
<b>Yellow</b>	When you are creating a storage volume and preserving data, then the path from the <b>Creating</b> status to the <b>Pass Through</b> status occurs if another volume is bootstrapping. In this case, the volume with the <b>Pass Through</b> status goes to the <b>Bootstrapping</b> status and then to the

Color	Volume Status
	<b>Available</b> status when the first volume is finished bootstrapping. Other than the specific scenario mentioned, yellow ( <b>Pass Through</b> status) indicates that there is a potential issue with the storage volume, the most common one being an upload buffer issue. If upload buffer capacity has been exceeded, then in some cases buffer space becomes available again. At that point, the storage volume self-corrects to the <b>Available</b> status. In other cases, you might have to add more upload buffer capacity to your gateway to return the storage volume to the <b>Available</b> status. For information on how to troubleshoot a case when upload buffer capacity has been exceeded, see <a href="#">Troubleshooting volume issues (p. 379)</a> . For information on how to add upload buffer capacity, see <a href="#">Determining the size of upload buffer to allocate (p. 255)</a> .
Red	The storage volume has the <b>Irrecoverable</b> status. In this case, you should delete the volume. For information on how to do this, see <a href="#">Deleting a Volume (p. 181)</a> .

In the following diagram, a transition between two states is depicted with a labeled line. For example, the transition from the **Creating** status to the **Available** status is labeled as *Create Basic Volume*. This transition represents creating a storage volume without preserving data or creating the volume from a snapshot.



#### Note

The volume status of **Pass Through** appears as yellow in this diagram. However, this doesn't match the color of this status icon in the **Status** box of the Storage Gateway console.

## Managing Your Tape Gateway

Following, you can find information about how to manage your tape gateway resources in AWS Storage Gateway.

### Topics

- [Adding Virtual Tapes \(p. 201\)](#)
- [Managing Automatic Tape Creation \(p. 201\)](#)
- [Archiving Virtual Tapes \(p. 202\)](#)
- [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#)
- [Retrieving Archived Tapes \(p. 203\)](#)
- [Viewing Tape Usage \(p. 204\)](#)
- [Deleting Tapes \(p. 204\)](#)
- [Deleting Custom Tape Pools \(p. 205\)](#)
- [Disabling Your Tape Gateway \(p. 205\)](#)
- [Understanding Tape Status \(p. 206\)](#)

## Adding Virtual Tapes

You can add tapes in your tape gateway when you need them. For information about how to create tapes, see [Creating Tapes \(p. 93\)](#).

After your tape is created, you can find information about it on the **Tapes** page. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties. For information about tape gateway tape quotas, see [AWS Storage Gateway quotas \(p. 444\)](#).

## Managing Automatic Tape Creation

The tape gateway automatically creates new virtual tapes to maintain the minimum number of available tapes that you configure. It then makes these new tapes available for import by the backup application so that your backup jobs can run without interruption. Automatic tape creation removes the need for custom scripting in addition to the manual process for creating new virtual tapes.

### To delete an automatic tape creation policy

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose the **Gateways** tab.
3. Choose the gateway for which you need to manage automatic tape creation.
4. In the **Actions** menu, choose **Configure tape auto-create**.
5. To delete an automatic tape creation policy on a gateway, choose **Remove** to the right of the policy you want to delete.

To stop automatic tape creation on a gateway, delete all of the automatic tape creation policies for that gateway.

Choose **Save changes** to confirm deletion of tape auto-create policies for the selected tape gateway.

**Note**

Deleting a tape auto-creation policy from a gateway cannot be undone.

### To change the automatic tape creation policies for a tape gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose the **Gateways** tab.
3. Choose the gateway for which you need to manage automatic tape creation.
4. In the **Actions** menu, choose **Configure tape auto-create**, and change the settings on the page that appears.
5. For **Minimum number of tapes**, enter the minimum number of virtual tapes that should be available on the tape gateway at all times. The valid range for this value is a minimum of 1 and a maximum of 10.
6. For **Capacity**, enter the size, in bytes of the virtual tape capacity. The valid range for this value is a minimum of 100 GiB and a maximum of 5 TiB.
7. For **Barcode prefix**, enter the prefix that you want to prepend to the barcode of your virtual tapes.

**Note**

Virtual tapes are uniquely identified by a barcode, and you can add a prefix to the barcode. The prefix is optional, but you can use it to help identify your virtual tapes. The prefix must be uppercase letters (A–Z) and must be one to four characters long.

8. For **Pool**, choose **Glacier Pool** or **Deep Archive Pool**. This pool represents the storage class in which your tapes are stored when they are ejected by your backup software.

Choose **Glacier Pool** if you want to archive the tapes in GLACIER. When your backup software ejects the tapes, they are automatically archived in GLACIER. You use S3 Glacier for more active archives where you can retrieve a tape typically within 3-5 hours. For detailed information, see [Storage Classes for Archiving Objects](#) in the *Amazon Simple Storage Service User Guide*.

Choose **Deep Archive Pool** if you want to archive the tapes in DEEP\_ARCHIVE. When your backup software ejects the tape, the tape is automatically archived in DEEP\_ARCHIVE. You use DEEP\_ARCHIVE for long-term data retention and digital preservation where data is accessed once or twice a year. You can retrieve a tape archived in DEEP\_ARCHIVE typically within 12 hours. For detailed information, see [Storage Classes for Archiving Objects](#) in the *Amazon S3 Developer Guide*.

If you archive tapes in GLACIER, you can move them to DEEP\_ARCHIVE later. For more information, see [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#).

9. You can find information about your tapes on the **Tapes** page. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.

The status of available virtual tapes is initially set to **CREATING** when the tapes are being created. After the tapes are created, their status changes to **AVAILABLE**. For more information, see [Managing Your Tape Gateway \(p. 200\)](#).

For more information about enabling automatic tape creation, see [Creating Tapes Automatically \(p. 94\)](#).

## Archiving Virtual Tapes

You can archive your tapes to Amazon S3 Glacier or DEEP\_ARCHIVE. When you create a tape, you choose the archive pool that you want to use to archive your tape.

You choose **Glacier Pool** if you want to archive the tape in S3 Glacier. When your backup software ejects the tape, it is automatically archived in S3 Glacier. You use S3 Glacier for more active archives where the data is regularly retrieved and needed in minutes. For detailed information, see [Storage Classes for Archiving Objects](#)

You choose **Deep Archive Pool** if you want to archive the tape in DEEP\_ARCHIVE. When your backup software ejects the tape, the tape is automatically archived in DEEP\_ARCHIVE. You use DEEP\_ARCHIVE for long-term data retention and digital preservation at a very low cost. Data in S3 Glacier DEEP\_ARCHIVE is not retrieved often or is rarely retrieved. For detailed information, see [Storage Classes for Archiving Objects](#).

### Note

Any tape created before March 27, 2019, are archived directly in S3 Glacier when your backup software ejects it.

When your backup software ejects a tape, it is automatically archived in the pool that you chose when you created the tape. The process for ejecting a tape varies depending on your backup software. Some backup software requires that you export tapes after they are ejected before archiving can begin. For information about supported backup software, see [Using Your Backup Software to Test Your Gateway Setup \(p. 99\)](#).

# Moving Your Tape from Glacier to Deep Archive Storage Class

Move your tapes from GLACIER to DEEP\_ARCHIVE for long-term data retention and digital preservation at a very low cost. You use DEEP\_ARCHIVE for long-term data retention and digital preservation where the data is accessed once or twice a year. For detailed information, see [Storage Classes for Archiving Objects](#).

## To move a tape from GLACIER to DEEP\_ARCHIVE

1. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.
2. Select the check boxes for the tapes you want to move to DEEP\_ARCHIVE. You can see the pool that each tape is associated with in the **Pool** column.
3. Choose **Assign to pool**.
4. In the Assign tape to pool dialog box, verify the barcodes for the tapes you are moving and choose **Assign**.

### Note

If a tape has been ejected by the backup application and archived in DEEP\_ARCHIVE, you can't move it back to GLACIER. There's a charge for moving your tapes from GLACIER to DEEP\_ARCHIVE. In addition, if you move tapes from GLACIER to DEEP\_ARCHIVE prior to 90 days, there is an early deletion fee for GLACIER.

5. After the tape is moved, you can see the updated status in the **Pool** column on the **Tapes** page.

# Retrieving Archived Tapes

To access data stored on an archived virtual tape, you must first retrieve the tape that you want to your tape gateway. Your tape gateway provides one virtual tape library (VTL) for each gateway.

If you have more than one tape gateway in an AWS Region, you can retrieve a tape to only one gateway.

The retrieved tape is write-protected; you can only read the data on the tape.

### Important

If you archive a tape in GLACIER, you can retrieve the tape typically within 3-5 hours. If you archive the tape in DEEP\_ARCHIVE, you can retrieve it typically within 12 hours.

### Note

There is a charge for retrieving tapes from archive. For detailed pricing information, see [Storage Gateway Pricing](#).

## To retrieve an archived tape to your gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.

3. Choose the virtual tape you want to retrieve from the **Virtual Tape Shelf** tab, and choose **Retrieve tape**.

**Note**

The status of the virtual tape that you want to retrieve must be ARCHIVED.

4. In the **Retrieve tape** dialog box, for **Barcode**, verify that the barcode identifies the virtual tape you want to retrieve.
5. For **Gateway**, choose the gateway that you want to retrieve the archived tape to, and then choose **Retrieve tape**.

The status of the tape changes from ARCHIVED to RETRIEVING. At this point, your data is being moved from the virtual tape shelf (backed by GLACIER or DEEP\_ARCHIVE) to the virtual tape library (backed by Amazon S3). After all the data is moved, the status of the virtual tape in the archive changes to RETRIEVED.

**Note**

Retrieved virtual tapes are read-only.

## Viewing Tape Usage

When you write data to a tape, you can view the amount of data stored on the tape in the Storage Gateway console. The **Details** tab for each tape shows the tape usage information.

### To view the amount of data stored on a tape

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.
3. Choose the tape you are interested in.
4. The page that appears provides various details and information about the tape, including the following:
  - **Size:** The total capacity of the selected tape.
  - **Used:** The size of data written to the tape by your backup application.

**Note**

This value is not available for tapes created before May 13, 2015.

## Deleting Tapes

You can delete virtual tapes from your tape gateway by using the Storage Gateway console.

**Note**

If the tape you want to delete from your tape gateway has a status of RETRIEVED, you must first eject the tape using your backup application before deleting the tape. For instructions on how to eject a tape using the Symantec NetBackup software, see [Archiving the Tape \(p. 146\)](#). After the tape is ejected, the tape status changes back to ARCHIVED. You can then delete the tape.

Make copies of your data before you delete your tapes. After you delete a tape, you can't get it back.

### To delete a virtual tape

**Warning**

This procedure permanently deletes the selected virtual tape.

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.
3. Choose the virtual tape that you want to delete.
4. Choose **Delete tape**. A confirmation box appears.
5. Make sure that the tape listed is the tape you intend to delete, type *delete* in the confirmation field, and then choose **Delete**.

After the tape is deleted, it disappears from the tape gateway.

## Deleting Custom Tape Pools

You can delete a custom tape pool only if there are no archived tapes in the pool, and there are no automatic tape creation policies attached to the pool.

### To delete your custom tape pool

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Pools** to see the available pools.
3. Choose the custom tape pools that you want to delete.

If the **Tape Count** for the tape pools that you want to delete is **0**, and if there are no automatic tape creation policies that reference the custom tape pool, you can delete the pools.

4. Choose **Delete**.
5. The **Confirm deletion** dialog box displays the **Name** and **Pool ID** of the pools to be deleted. To delete the pools, enter **delete** in the confirmation field, then choose **Delete**.

#### Warning

This procedure permanently deletes the selected custom tape pools and can't be undone.

After the custom tape pools are deleted, they disappear from the tape library.

## Disabling Your Tape Gateway

You disable a tape gateway if the tape gateway has failed and you want to recover the tapes from the failed gateway to another gateway.

To recover the tapes, you must first disable the failed gateway. Disabling a tape gateway locks down the virtual tapes in that gateway. That is, any data that you might write to these tapes after disabling the gateway isn't sent to AWS. You can only disable a gateway on the Storage Gateway console if the gateway is no longer connected to AWS. If the gateway is connected to AWS, you can't disable the tape gateway.

You disable a tape gateway as part of data recovery. For more information about recovering tapes, see [You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway \(p. 383\)](#).

### To disable your gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the failed gateway.

3. Choose the **Details** tab for the gateway to display the disable gateway message.
4. Choose **Create recovery tapes**.
5. Choose **Disable gateway**.

## Understanding Tape Status

Each tape has an associated status that tells you at a glance what the health of the tape is. Most of the time, the status indicates that the tape is functioning normally and that no action is needed on your part. In some cases, the status indicates a problem with the tape that might require action on your part. You can find information following to help you decide when you need to act.

### Topics

- [Understanding Tape Status Information in a VTL \(p. 206\)](#)
- [Determining Tape Status in an Archive \(p. 207\)](#)

## Understanding Tape Status Information in a VTL

A tape's status must be AVAILABLE for you to read or write to the tape. The following table lists and describes possible status values.

Status	Description	Tape Data Is Stored In
CREATING	The virtual tape is being created. The tape can't be loaded into a tape drive, because the tape is being created.	—
AVAILABLE	The virtual tape is created and ready to be loaded into a tape drive.	Amazon S3
IN TRANSIT TO VTS	The virtual tape has been ejected and is being uploaded for archive. At this point, your tape gateway is uploading data to AWS. If the amount of data being uploaded is small, this status might not appear. When the upload is completed, the status changes to ARCHIVING.	Amazon S3
ARCHIVING	The virtual tape is being moved by your tape gateway to the archive, which is backed by GLACIER or DEEP_ARCHIVE. This process happens after the data upload to AWS is completed.	Data is being moved from Amazon S3 to GLACIER or DEEP_ARCHIVE.
DELETING	The virtual tape is being deleted.	Data is being deleted from Amazon S3
DELETED	The virtual tape has been successfully deleted.	—
RETRIEVING	The virtual tape is being retrieved from the archive to your tape gateway.  <b>Note</b> The virtual tape can be retrieved only to a tape gateway.	Data is being moved from GLACIER or DEEP_ARCHIVE to Amazon S3
RETRIEVED	The virtual tape is retrieved from the archive. The retrieved tape is write-protected.	Amazon S3
RECOVERED	The virtual tape is recovered and is read-only.	Amazon S3

Status	Description	Tape Data Is Stored In
	When your tape gateway is not accessible for any reason, you can recover virtual tapes associated with that tape gateway to another tape gateway. To recover the virtual tapes, first disable the inaccessible tape gateway.	
IRRECOVERABLE	The virtual tape can't be read from or written to. This status indicates an error in your tape gateway.	Amazon S3

## Determining Tape Status in an Archive

You can use the following procedure to determine the status of a virtual tape in an archive.

### To determine the status of a virtual tape

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Tapes**.
3. In the **Status** column of the tape library grid, check the status of the tape.

The tape status also appears in the **Details** tab of each virtual tape.

Following, you can find a description of the possible status values.

Status	Description
ARCHIVED	The virtual tape has been ejected and is uploaded to the archive.
RETRIEVING	The virtual tape is being retrieved from the archive. <b>Note</b> The virtual tape can be retrieved only to a tape gateway.
RETRIEVED	The virtual tape has been retrieved from the archive. The retrieved tape is read-only.

For additional information about how to work with tapes and VTL devices, see [Working With Tapes \(p. 411\)](#).

## Moving your data to a new gateway

You can move data between gateways as your data and performance needs grow, or if you receive an AWS notification to migrate your gateway. The following are some reasons for doing this:

- Move your data to better host platforms or newer Amazon EC2 instances.
- Refresh the underlying hardware for your server.

The steps that you follow to move your data to a new gateway depend on the gateway type that you have.

### Note

Data can only be moved between the same gateway types.

### Topics

- [Migrating your Amazon S3 File Gateway \(p. 208\)](#)
- [Moving stored volumes to a new stored volume gateway \(p. 208\)](#)
- [Moving cached volumes to a new cached volume gateway virtual machine \(p. 209\)](#)
- [Moving virtual tapes to a new tape gateway \(p. 211\)](#)

## Migrating your Amazon S3 File Gateway

If you receive an AWS notification to migrate your file gateway, see [Migrating your Amazon S3 File Gateway](#) in the *User Guide for Amazon S3 File Gateway*.

### Moving stored volumes to a new stored volume gateway

#### To move your stored volume to a new stored volume gateway

1. Stop any applications that are writing to the old stored volume gateway.
2. Use the following steps to create a snapshot of your volume, and then wait for the snapshot to complete.
  - a. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
  - b. In the navigation pane, choose **Volumes**, and then choose the volume that you want to create the snapshot from.
  - c. For **Actions**, choose **Create snapshot**.
  - d. In the **Create snapshot** dialog box, enter a snapshot description, and then choose **Create snapshot**.

You can verify that the snapshot was created using the console. If data is still uploading to the volume, wait until the upload is complete before you go to the next step. To see the snapshot status and validate that none are pending, select the snapshot links on the volumes.

3. Use the following steps to stop the old stored volume gateway:
  - a. In the navigation pane, choose **Gateways**, and then choose the old stored volume gateway that you want to stop. The status of the gateway is **Running**.
  - b. For **Actions**, choose **Stop gateway**. Verify the ID of the gateway from the dialog box, and then choose **Stop gateway**.

While the gateway is stopping, you might see a message that indicates the status of the gateway. When the gateway shuts down, a message and a **Start gateway** button appear in the **Details** tab. When the gateway shuts down, the status of the gateway is **Shutdown**.

- c. Shut down the VM using the hypervisor controls.

For more information about stopping a gateway, see [Starting and Stopping a Volume or Tape Gateway \(p. 253\)](#).

4. Detach the storage disks associated with your stored volumes from the gateway VM. This excludes the root disk of the VM.
5. Activate a new stored volume gateway with a new hypervisor VM image available from the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
6. Attach the physical storage disks that you detached from the old stored volume gateway VM in step 5.
7. To preserve existing data on the disk, use the following steps to create stored volumes.

- a. On the Storage Gateway console, choose **Create volume**.
- b. In the **Create volume** dialog box, select the stored volume gateway that you created in step 5.
- c. Choose a **Disk ID** value from the list.
- d. For **Volume content**, select the **Preserve existing data on the disk** option.

For more information about creating volumes, see [Creating a volume \(p. 72\)](#).

8. (Optional) In the **Configure CHAP authentication** wizard that appears, enter the **Initiator name**, **Initiator secret**, and **Target secret**, and then choose **Save**.

For more information about working with Challenge-Handshake Authentication Protocol (CHAP) authentication, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).

9. Start the application that writes to your stored volume.
10. When you have confirmed that your new stored volume gateway is working correctly, you can delete the old stored volume gateway.

**Important**

Before you delete a gateway, be sure that no applications are currently writing to that gateway's volumes. If you delete a gateway while it is in use, data loss can occur.

Use the following steps to delete the old stored volume gateway:

**Warning**

When a gateway is deleted, there is no way to recover it.

- a. In the navigation pane, choose **Gateways**, and then choose the old stored volume gateway that you want to delete.
- b. For **Actions**, choose **Delete gateway**.
- c. In the confirmation dialog box that appears, select the check box to confirm your deletion. Make sure that the gateway ID listed specifies the old stored volume gateway that you want to delete, and then choose **Delete**.



11. Delete the old gateway VM. For information about deleting a VM, see the documentation for your hypervisor.

## Moving cached volumes to a new cached volume gateway virtual machine

### To move your cached volumes to a new cached volume gateway virtual machine (VM)

1. Stop any applications that are writing to the old cached volume gateway.

2. Unmount or disconnect iSCSI volumes from any clients that are using them. This helps keep data on those volumes consistent by preventing clients from changing or adding data to those volumes.
3. Use the following steps to create a snapshot of your volume, and then wait for the snapshot to complete.
  - a. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
  - b. In the navigation pane, choose **Volumes**, and then choose the volume that you want to create the snapshot from.
  - c. For **Actions**, choose **Create snapshot**.
  - d. In the **Create snapshot** dialog box, enter a snapshot description, and then choose **Create snapshot**.

You can verify that the snapshot was created using the console. If data is still uploading to the volume, wait until the upload is complete before you go to the next step. To see the snapshot status and validate that none are pending, select the snapshot links on the volumes.

For more information about checking volume status in the console, see [Understanding Volume Statuses and Transitions \(p. 193\)](#). For information about cached volume status, see [Understanding Cached Volume Status Transitions \(p. 196\)](#).

4. Use the following steps to stop the old cached volume gateway:
  - a. In the navigation pane, choose **Gateways**, and then choose the old cached volume gateway that you want to stop. The status of the gateway is **Running**.
  - b. For **Actions**, choose **Stop gateway**. Verify the ID of the gateway from the dialog box, and then choose **Stop gateway**. Make a note of the gateway ID, as it is needed in a later step.

While the old gateway is stopping, you might see a message that indicates the status of the gateway. When the old gateway shuts down, a message and a **Start gateway** button appear in the **Details** tab. When the gateway shuts down, the status of the gateway is **Shutdown**.

- c. Shut down the old VM using the hypervisor controls. For more information about shutting down an Amazon EC2 instance, see [Stopping and starting your instances](#) in the *Amazon EC2 User Guide for Windows Instances*. For more information about shutting down a KVM, VMware, or Hyper-V VM, see your hypervisor documentation.

For more information about stopping a gateway, see [Starting and Stopping a Volume or Tape Gateway \(p. 253\)](#).

5. Detach all disks, including the root disk, cache disks, and upload buffer disks, from the old gateway VM.

#### Note

Make a note of the root disk's volume ID, as well as the gateway ID associated with that root disk. You detach this disk from the new storage gateway hypervisor in a later step. (See step 11.)

If you are using an Amazon EC2 instance as the VM for your cached volume gateway, see [Detaching an Amazon EBS volume from a Linux instance](#) in the *Amazon EC2 User Guide for Linux Instances*. For information about detaching disks from a KVM, VMware, or Hyper-V VM, see the documentation for your hypervisor.

6. Create a new storage gateway hypervisor VM instance, but don't activate it as a gateway. For more information about creating a new storage gateway hypervisor VM, see [Choosing a Host Platform and Downloading the VM \(p. 68\)](#). This new gateway will assume the identity of the old gateway.

#### Note

Do not add disks for cache or upload buffer to the new VM. Your new VM will use the same cache disks and upload buffer disks that were used by the old VM.

7. Your new storage gateway hypervisor VM instance should use the same network configuration as the old VM. The default network configuration for the gateway is Dynamic Host Configuration Protocol (DHCP). With DHCP, your gateway is automatically assigned an IP address.

If you need to manually configure a static IP address for your new VM, see [Configuring Your Gateway Network \(p. 293\)](#) for more details. If your gateway must use a Socket Secure version 5 (SOCKS5) proxy to connect to the internet, see [Routing Your On-Premises Gateway Through a Proxy \(p. 290\)](#) for more details.

8. Start the new VM.
9. Attach the disks that you detached from the old cached volume gateway VM in step 5, to the new cached volume gateway. Attach them in the same order to the new gateway VM as they are on the old gateway VM.

All disks must make the transition unchanged. Do not change volume sizes, as that will cause metadata to become inconsistent.

10. Initiate the gateway migration process by connecting to the new VM with a URL that uses the following format.

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

You can re-use the same IP address for the new gateway VM as you used for the old gateway VM. Your URL should look similar to the example following.

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

Use this URL from a browser, or from the command line using `curl`, to initiate the migration process.

When the gateway migration process is successfully initiated, you will see the following message:

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

11. Detach the old gateway's root disk, whose volume ID you noted in step 5.
12. Start the gateway.

Use the following steps to start the new cached volume gateway:

- a. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
- b. In the navigation pane, choose **Gateways** and then choose the new gateway you want to start. The status of the gateway is **Shutdown**.
- c. Choose **Details**, and then choose **Start gateway**.

For more information about starting a gateway, see [Starting and Stopping a Volume or Tape Gateway \(p. 253\)](#).

13. Your volumes should now be available to your applications at the new gateway VM's IP address.
14. Confirm that your volumes are available, and delete the old gateway VM. For information about deleting a VM, see the documentation for your hypervisor.

## Moving virtual tapes to a new tape gateway

## To move your virtual tape to a new tape gateway

1. Use your backup application to back up all your data onto a virtual tape. Wait for the backup to finish successfully.
2. Use your backup application to eject your tape. The tape will be stored in one of the Amazon S3 storage classes. Ejected tapes are archived in S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive, and are read-only.

Before proceeding, confirm that the ejected tapes have been archived:

- a. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
- b. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.
- c. In the **Status** column of the list, check the status of the tape.

The tape status also appears in the **Details** tab of each virtual tape.

For more information about determining tape status in an archive, see [Determining Tape Status in an Archive \(p. 207\)](#).

3. Using your backup application, verify that there are no active backup jobs going to the existing tape gateway before you stop it. If there are any active backup jobs, wait for them to finish and eject your tapes (see previous step) before stopping the gateway.
4. Use the following steps to stop the existing tape gateway:
  - a. In the navigation pane, choose **Gateways**, and then choose the old tape gateway that you want to stop. The status of the gateway is **Running**.
  - b. For **Actions**, choose **Stop gateway**. Verify the ID of the gateway from the dialog box, and then choose **Stop gateway**.

While the old tape gateway is stopping, you might see a message that indicates the status of the gateway. When the gateway shuts down, a message and a **Start gateway** button appear in the **Details** tab.

For more information about stopping a gateway, see [Starting and Stopping a Volume or Tape Gateway \(p. 253\)](#).

5. Create a new tape gateway. For detailed instructions, see [Creating a Gateway \(p. 85\)](#).

6. Use the following steps to create new tapes:

- a. In the navigation pane, choose the **Gateways** tab.
- b. Choose **Create tape** to open the **Create tape** dialog box.
- c. For **Gateway**, choose a gateway. The tape is created for this gateway.
- d. For **Number of tapes**, choose the number of tapes that you want to create. For more information about tape limits, see [AWS Storage Gateway quotas \(p. 444\)](#).

You can also set up automatic tape creation at this point. For more information, see [Creating Tapes Automatically \(p. 94\)](#).

- e. For **Capacity**, enter the size of the virtual tape that you want to create. Tapes must be larger than 100 GiB. For information about capacity limits, see [AWS Storage Gateway quotas \(p. 444\)](#).
- f. For **Barcode prefix**, enter the prefix that you want to prepend to the barcode of your virtual tapes.

### Note

Virtual tapes are uniquely identified by a barcode. You can add a prefix to the barcode. The prefix is optional, but you can use it to help identify your virtual tapes. The prefix must be uppercase letters (A–Z) and must be one to four characters long.

- g. For **Pool**, choose **Glacier Pool** or **Deep Archive Pool**. This pool represents the storage class in which your tape will be stored when it is ejected by your backup software.

Choose **Glacier Pool** if you want to archive the tape in S3 Glacier Flexible Retrieval. When your backup software ejects the tape, it is automatically archived in S3 Glacier Flexible Retrieval. You use S3 Glacier for more active archives where you can retrieve a tape typically within 3–5 hours. For more information, see [Storage classes for archiving objects](#) in the *Amazon Simple Storage Service User Guide*.

Choose **Deep Archive Pool** if you want to archive the tape in S3 Glacier Deep Archive. When your backup software ejects the tape, the tape is automatically archived in S3 Glacier Deep Archive. You use S3 Glacier Deep Archive for long-term data retention and digital preservation where data is accessed once or twice a year. You can retrieve a tape archived in S3 Glacier Deep Archive typically within 12 hours. For more information, see [Storage classes for archiving objects](#) in the *Amazon Simple Storage Service User Guide*.

If you archive a tape in S3 Glacier Flexible Retrieval, you can move it to S3 Glacier Deep Archive later. For more information, see [Moving Your Tape from Glacier to Deep Archive Storage Class \(p. 203\)](#).

### Note

Tapes created before March 27, 2019, are archived directly in Amazon S3 Glacier when your backup software ejects them.

- h. (Optional) For **Tags**, enter a key and value to add tags to your tape. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your tapes.
- i. Choose **Create tapes**.
7. Use your backup application to start a backup job, and back up your data to the new tape.
8. If your tape is archived and you need to restore data from it, retrieve it to the new tape gateway. The tape will be in read-only mode. For more information about retrieving archived tapes, see [Retrieving Archived Tapes \(p. 203\)](#).

### Note

Data egress charges might apply.

- a. In the navigation pane, choose **Tape Library > Tapes** to see your tapes. By default, this list displays up to 1,000 tapes at a time, but the searches that you perform apply to all of your tapes. You can use the search bar to find tapes that match a specific criteria, or to reduce the list to less than 1,000 tapes. When your list contains 1,000 tapes or fewer, you can then sort your tapes in ascending or descending order by various properties.
- b. Choose the virtual tape that you want to retrieve. For **Actions**, choose **Retrieve Tape**.

### Note

The status of the virtual tape that you want to retrieve must be **ARCHIVED**.

- c. In the **Retrieve tape** dialog box, for **Barcode**, verify that the barcode identifies the virtual tape you want to retrieve.
- d. For **Gateway**, choose the new tape gateway that you want to retrieve the archived tape to, and then choose **Retrieve tape**.

When you have confirmed that your new tape gateway is working correctly, you can delete the old tape gateway.

**Important**

Before you delete a gateway, be sure that there are no applications currently writing to that gateway's volumes. If you delete a gateway while it is in use, data loss can occur.

9. Use the following steps to delete the old tape gateway:

**Warning**

When a gateway is deleted, there is no way to recover it.

- a. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to delete.
- b. For **Actions**, choose **Delete gateway**.

In the confirmation dialog box that appears, make sure that the gateway ID listed specifies the old tape gateway that you want to delete, enter **delete** in the confirmation field, and then choose **Delete**.

- c. Delete the VM. For more information about deleting a VM, see the documentation for your hypervisor.

# Monitoring Storage Gateway

In this section, you can find information about how to monitor a gateway, including monitoring resources associated with the gateway, using Amazon CloudWatch. You can monitor the gateway's upload buffer and cache storage. You use the Storage Gateway console to view metrics and alarms for your gateway. For example, you can view the number of bytes used in read and write operations, the time spent in read and write operations, and the time taken to retrieve data from the Amazon Web Services Cloud. With metrics, you can track the health of your gateway and set up alarms to notify you when one or more metrics fall outside a defined threshold.

Storage Gateway provides CloudWatch metrics at no additional charge. Storage Gateway metrics are recorded for a period of two weeks. By using these metrics, you can access historical information and get a better perspective on how your gateway and volumes are performing. Storage Gateway also provides CloudWatch alarms, except high-resolution alarms, at no additional charge. For more information about CloudWatch pricing, see [Amazon CloudWatch pricing](#). For more information about CloudWatch, see [Amazon CloudWatch User Guide](#).

## Topics

- [Understanding gateway metrics \(p. 215\)](#)
- [Dimensions for Storage Gateway metrics \(p. 219\)](#)
- [Monitoring the upload buffer \(p. 220\)](#)
- [Monitoring cache storage \(p. 222\)](#)
- [Understanding CloudWatch alarms \(p. 223\)](#)
- [Monitoring your file gateway \(p. 225\)](#)
- [Monitoring Your Volume Gateway \(p. 237\)](#)
- [Monitoring Your Tape Gateway \(p. 247\)](#)

## Understanding gateway metrics

For the discussion in this topic, we define *gateway* metrics as metrics that are scoped to the gateway—that is, they measure something about the gateway. Because a gateway contains one or more volumes, a gateway-specific metric is representative of all volumes on the gateway. For example, the `CloudBytesUploaded` metric is the total number of bytes that the gateway sent to the cloud during the reporting period. This metric includes the activity of all the volumes on the gateway.

When working with gateway metric data, you specify the unique identification of the gateway that you are interested in viewing metrics for. To do this, you specify both the `GatewayId` and the `GatewayName` values. When you want to work with metric for a gateway, you specify the gateway *dimension* in the metrics namespace, which distinguishes a gateway-specific metric from a volume-specific metric. For more information, see [Using Amazon CloudWatch Metrics \(p. 238\)](#).

Metric	Description	Applies To
<code>AvailabilityNotifications</code>	Number of availability-related health notifications generated by the gateway.  Use this metric with the <code>Sum</code> statistic to observe whether the gateway is experiencing any availability-related events. For	All gateways.

Metric	Description	Applies To
	<p>details about the events, check your configured CloudWatch log group.</p> <p>Unit: Number</p>	
CacheHitPercent	<p>Percent of application reads served from the cache. The sample is taken at the end of the reporting period.</p> <p>Unit: Percent</p>	File, cached-volume, and tape gateways.
CacheUsed	<p>The total number of bytes being used in the gateway's cache storage. The sample is taken at the end of the reporting period.</p> <p>Unit: Bytes</p>	File, cached-volume, and tape gateways.
IndexEvictions	<p>The number of files whose metadata was evicted from the cached index of file metadata to make room for new entries. The gateway maintains this metadata index, which is populated from the Amazon Web Services Cloud on demand.</p> <p>Statistics: SampleCount for number of directories, SUM for total number of files, Average for average number of files per directory.</p> <p>Unit: Number</p>	File gateways only.
IndexFetches	<p>The number of files for which metadata was fetched. The gateway maintains a cached index of file metadata, which is populated from the Amazon Web Services Cloud on demand.</p> <p>Statistics: SampleCount for number of directories, SUM for total number of files, Average for average number of files per directory.</p> <p>Unit: Number</p>	File gateways only.
IoWaitPercent	<p>Percent of time that the gateway is waiting on a response from the local disk.</p> <p>Unit: Percent</p>	All gateways.

Metric	Description	Applies To
MemTotalBytes	Amount of RAM provisioned to the gateway VM, in bytes.  Unit: Bytes	All gateways.
MemUsedBytes	Amount of RAM currently in use by the gateway VM, in bytes.  Unit: Bytes	All gateways.
NfsSessions	The number of active sessions for NFS clients.  Unit: Number	S3 File Gateways only.
QueuedWrites	The number of bytes waiting to be written to AWS, sampled at the end of the reporting period for all volumes in the gateway. These bytes are kept in your gateway's working storage.  Unit: Bytes	All gateways.
ReadBytes	The total number of bytes read from your on-premises applications in the reporting period for all volumes in the gateway.  Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.  Unit: Bytes	File, cached-volume, and stored-volume gateways.
ReadTime	The total number of milliseconds spent to do read operations from your on-premises applications in the reporting period for all volumes in the gateway.  Use this metric with the <code>Average</code> statistic to measure latency.  Unit: Milliseconds	File, cached-volume, and stored-volume gateways.
SmbV1Sessions	The number of Server Message Block (SMB) version 1 sessions that are active on the gateway.  Unit: Number	File gateways only.

Metric	Description	Applies To
SmbV2Sessions	The number of SMB version 2 sessions that are active on the gateway.  Unit: Number	File gateways only.
SmbV3Sessions	The number of SMB version 3 sessions that are active on the gateway.  Unit: Number	File gateways only.
TimeSinceLastRecoveryPoint	The time since the last available recovery point. For more information, see <a href="#">Your Cached Gateway is Unreachable And You Want to Recover Your Data (p. 380)</a> .  Unit: Seconds	Cached volumes and stored volumes.
TotalCacheSize	The total size of the cache in bytes. The sample is taken at the end of the reporting period.  Unit: Bytes	File, cached-volume, and tape gateways.
UploadBufferPercentUsed	Percent use of the gateway's upload buffer. The sample is taken at the end of the reporting period.  Unit: Percent	Cached-volume and tape gateways.
UploadBufferUsed	The total number of bytes being used in the gateway's upload buffer. The sample is taken at the end of the reporting period.  Unit: Bytes	Cached-volume and tape gateways.
UserCpuPercent	Percent of CPU time spent on gateway processing, averaged across all cores.  Unit: Percent	All gateways.
WorkingStorageFree	The total amount of unused space in the gateway's working storage. The sample is taken at the end of the reporting period.  Unit: Bytes	Stored volumes only.

Metric	Description	Applies To
WorkingStoragePercentUsed	Percent use of the gateway's upload buffer. The sample is taken at the end of the reporting period.  Unit: Percent	Stored volumes only.
WorkingStorageUsed	The total number of bytes being used in the gateway's upload buffer. The sample is taken at the end of the reporting period.  Unit: Bytes	Stored volumes only.
WriteBytes	The total number of bytes written to your on-premises applications in the reporting period for all volumes in the gateway.  Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.  Unit: Bytes	File, cached-volume, and stored-volume gateways.
WriteTime	The total number of milliseconds spent to do write operations from your on-premises applications in the reporting period for all volumes in the gateway.  Use this metric with the <code>Average</code> statistic to measure latency.  Unit: Milliseconds	File, cached-volume, and stored-volume gateways.

## Dimensions for Storage Gateway metrics

The CloudWatch namespace for the Storage Gateway service is `AWS/StorageGateway`. Data is available automatically in 5-minute periods at no charge.

Dimension	Description
GatewayId, GatewayName	These dimensions filter the data that you request to gateway-specific metrics. You can identify a gateway to work by the value for <code>GatewayId</code> or <code>GatewayName</code> . If the name of your gateway was different for the time range that you are interested in viewing metrics, use the <code>GatewayId</code> .

Dimension	Description
	Throughput and latency data of a gateway is based on all the volumes for the gateway. For information about working with gateway metrics, see <a href="#">Measuring Performance Between Your Gateway and AWS</a> .
VolumeId	This dimension filters the data you request to volume-specific metrics. Identify a storage volume to work with by its VolumeId value. For information about working with volume metrics, see <a href="#">Measuring Performance Between Your Application and Gateway</a> .

## Monitoring the upload buffer

You can find information following about how to monitor a gateway's upload buffer and how to create an alarm so that you get a notification when the buffer exceeds a specified threshold. By using this approach, you can add buffer storage to a gateway before it fills completely and your storage application stops backing up to AWS.

You monitor the upload buffer in the same way in both the cached-volume and tape gateway architectures. For more information, see [How Storage Gateway works \(architecture\) \(p. 3\)](#).

**Note**

The WorkingStoragePercentUsed, WorkingStorageUsed, and WorkingStorageFree metrics represent the upload buffer for stored volumes only before the release of the cached-volume feature in Storage Gateway. Now, use the equivalent upload buffer metrics UploadBufferPercentUsed, UploadBufferUsed, and UploadBufferFree. These metrics apply to both gateway architectures.

Item of Interest	How to Measure
Upload buffer usage	Use the UploadBufferPercentUsed, UploadBufferUsed, and UploadBufferFree metrics with the Average statistic. For example, use the UploadBufferUsed with the Average statistic to analyze the storage usage over a time period.

### To measure the percent of the upload buffer that is used

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose the **StorageGateway: Gateway Metrics** dimension, and find the gateway that you want to work with.
3. Choose the UploadBufferPercentUsed metric.
4. For **Time Range**, choose a value.
5. Choose the **Average** statistic.
6. For **Period**, choose a value of 5 minutes to match the default reporting time.

The resulting time-ordered set of data points contains the percent used of the upload buffer.

Using the following procedure, you can create an alarm using the CloudWatch console. To learn more about alarms and thresholds, see [Creating CloudWatch Alarms](#) in the *Amazon CloudWatch User Guide*.

### To set an upper threshold alarm for a gateway's upload buffer

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. Choose **Create Alarm** to start the Create Alarm wizard.
3. Specify a metric for your alarm:
  - a. On the **Select Metric** page of the Create Alarm wizard, choose the **AWS/StorageGateway:GatewayId,GatewayName** dimension, and then find the gateway that you want to work with.
  - b. Choose the **UploadBufferPercentUsed** metric. Use the **Average** statistic and a period of 5 minutes.
  - c. Choose **Continue**.
4. Define the alarm name, description, and threshold:
  - a. On the **Define Alarm** page of the Create Alarm wizard, identify your alarm by giving it a name and description in the **Name** and **Description** boxes.
  - b. Define the alarm threshold.
  - c. Choose **Continue**.
5. Configure an email action for the alarm:
  - a. On the **Configure Actions** page of the Create Alarm wizard, choose **Alarm for Alarm State**.
  - b. Choose **Choose or create email topic for Topic**.

To create an email topic means that you set up an Amazon SNS topic. For more information about Amazon SNS, see [Set Up Amazon SNS](#) in the *Amazon CloudWatch User Guide*.
  - c. For **Topic**, enter a descriptive name for the topic.
  - d. Choose **Add Action**.
  - e. Choose **Continue**.
6. Review the alarm settings, and then create the alarm:
  - a. On the **Review** page of the Create Alarm wizard, review the alarm definition, metric, and associated actions to take (for example, sending an email notification).
  - b. After reviewing the alarm summary, choose **Save Alarm**.
7. Confirm your subscription to the alarm topic:
  - a. Open the Amazon SNS email that was sent to the email address that you specified when creating the topic.

The following image shows a typical email notification.



- b. Confirm your subscription by clicking the link in the email.

A subscription confirmation appears.

# Monitoring cache storage

You can find information following about how to monitor a gateway's cache storage and how to create an alarm so that you get a notification when parameters of the cache pass specified thresholds. Using this alarm, you know when to add cache storage to a gateway.

You only monitor cache storage in the cached volumes architecture. For more information, see [How Storage Gateway works \(architecture\) \(p. 3\)](#).

Item of Interest	How to Measure
Total usage of cache	<p>Use the <code>CachePercentUsed</code> and <code>TotalCacheSize</code> metrics with the <code>Average</code> statistic. For example, use the <code>CachePercentUsed</code> with the <code>Average</code> statistic to analyze the cache usage over a period of time.</p> <p>The <code>TotalCacheSize</code> metric changes only when you add cache to the gateway.</p>
Percent of read requests that are served from the cache	<p>Use the <code>CacheHitPercent</code> metric with the <code>Average</code> statistic.</p> <p>Typically, you want <code>CacheHitPercent</code> to remain high.</p>
Percent of the cache that is dirty—that is, it contains content that has not been uploaded to AWS	<p>Use the <code>CachePercentDirty</code> metrics with the <code>Average</code> statistic.</p> <p>Typically, you want <code>CachePercentDirty</code> to remain low.</p>

## To measure the percent of a cache that is dirty for a gateway and all its volumes

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose the **StorageGateway: Gateway Metrics** dimension, and find the gateway that you want to work with.
3. Choose the `CachePercentDirty` metric.
4. For **Time Range**, choose a value.
5. Choose the `Average` statistic.
6. For **Period**, choose a value of 5 minutes to match the default reporting time.

The resulting time-ordered set of data points contains the percentage of the cache that is dirty over the 5 minutes.

## To measure the percent of the cache that is dirty for a volume

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose the **StorageGateway: Volume Metrics** dimension, and find the volume that you want to work with.
3. Choose the `CachePercentDirty` metric.
4. For **Time Range**, choose a value.
5. Choose the `Average` statistic.
6. For **Period**, choose a value of 5 minutes to match the default reporting time.

The resulting time-ordered set of data points contains the percentage of the cache that is dirty over the 5 minutes.

## Understanding CloudWatch alarms

You can add CloudWatch alarms to your Storage Gateway console and monitor them visually. When an alarm is present, it turns red when it is in the ALARM state, making it easier for you to monitor its status proactively. Alarms invoke actions for sustained state changes only. Alarms don't invoke actions simply because they are in a particular state. The state must have changed and been maintained for a specified number of periods. For more information about CloudWatch alarms, see [Using Amazon CloudWatch alarms](#).

**Note**

If you don't have permission to view CloudWatch, you can't view the alarms.

For each activated gateway, we recommend that you create the following CloudWatch alarms:

- High IO wait: `IoWaitpercent >= 20` for 3 datapoints in 15 minutes
- Cache percent dirty: `CachePercentDirty > 80` for 4 datapoints within 20 minutes
- Availability notifications: `AvailabilityNotifications >= 1` for 1 datapoints within 5 minutes
- Health notifications: `HealthNotifications >= 1` for 1 datapoints within 5 minutes

**Note**

You can set a health notification alarm only if the gateway had a previous health notification in CloudWatch.

The following table describes the state of an alarm.

State	Description
OK	The metric or expression is within the defined threshold.
Alarm	The metric or expression is outside of the defined threshold.
Insufficient data	The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.
None	No alarms are created for the gateway. To create a new alarm, see <a href="#">Creating an CloudWatch alarm for Storage Gateway (p. 223)</a> .
Unavailable	The state of the alarm is unknown. Choose <b>Unavailable</b> to view error information in the <b>Monitoring</b> tab.

## Creating an CloudWatch alarm for Storage Gateway

CloudWatch uses Amazon Simple Notification Service (Amazon SNS) to send alarm notifications when an alarm changes state. An alarm watches a single metric over a time period you specify, and performs

one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic. You can create an Amazon SNS topic when you create a CloudWatch alarm. For more information about Amazon SNS, see [What is Amazon SNS?](#) in the *Amazon Simple Notification Service Developer Guide*.

### To create a CloudWatch alarm in the Storage Gateway console

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home/>.
2. In the navigation pane, choose **Gateways**.
3. Choose a gateway, and then choose the alarm state or the **Monitoring** tab.
4. Do one of the following:
  - If there are no alarms, choose **CloudWatch Alarms**.
  - If there is an existing alarm, choose **Create alarm**.

The CloudWatch console opens.

5. Create an alarm. The following are the types of CloudWatch alarms:
  - Static threshold alarm: An alarm based on a set threshold for a chosen metric. The alarm goes to ALARM state when the metric breaches the threshold for a specified number of evaluation periods.

To create a static threshold alarm, see [Creating a CloudWatch alarm based on a static threshold](#) in the *Amazon CloudWatch User Guide*.
  - Anomaly detection alarm: Anomaly detection mines past metric data and creates a model of expected values. You set a value for the anomaly detection threshold, and CloudWatch uses this threshold with the model to determine the "normal" range of values for the metric. A higher value for the threshold produces a thicker band of "normal" values. You can choose whether the alarm is triggered when the metric value is above the band of expected values, below the band, or either above or below the band.

To create an anomaly detection alarm, see [Creating a CloudWatch alarm based on anomaly detection](#) in the *Amazon CloudWatch User Guide*.
  - Metric math expression alarm: An alarm based one or more metrics used in a math expression. You specify the expression, threshold, and evaluation periods.

To create a metric math expression alarm, see [Creating a CloudWatch alarm based on a metric math expression](#) in the *Amazon CloudWatch User Guide*.
  - Composite alarm: An alarm that determines its alarm state by watching the alarm states of other alarms. A composite alarm can help you reduce alarm noise.

To create a composite alarm, see [Creating a composite alarm](#) in the *Amazon CloudWatch User Guide*.
6. After you create the alarm in the CloudWatch console, return to the Storage Gateway console. You can view the alarm by doing one of the following:
  - In the navigation pane, choose **Gateways**, and then choose a gateway. On the **Details** tab, for **Alarms**, choose **CloudWatch Alarms**.
  - In the navigation pane, choose **Gateways**, then choose a gateway, and then choose the **Monitoring** tab.
  - In the navigation pane, choose **Gateways**, and then choose the alarm state of a gateway.

To edit or delete an alarm, see [Editing or deleting a CloudWatch alarm](#).

# Monitoring your file gateway

You can monitor your file gateway and associated resources by using Amazon CloudWatch metrics and file share audit logs, and use Amazon CloudWatch Events to get notified when your file operations are done. For information about file gateway type metrics, see [Understanding gateway metrics \(p. 215\)](#).

## Topics

- [Getting file gateway health logs with CloudWatch Log Groups \(p. 225\)](#)
- [Using Amazon CloudWatch metrics \(p. 226\)](#)
- [Getting notified about file operations \(p. 227\)](#)
- [Understanding file share metrics \(p. 233\)](#)
- [Understanding file gateway audit logs \(p. 234\)](#)

## Getting file gateway health logs with CloudWatch Log Groups

You can use Amazon CloudWatch Logs to get information about the health of your file gateway and related resources. You can use the logs to monitor your gateway for errors that it encounters. In addition, you can use Amazon CloudWatch subscription filters to automate processing of the log information in real-time. For more information see, [Real-time Processing of Log Data with Subscriptions](#) in the *Amazon CloudWatch User Guide*.

For example, you can configure a CloudWatch Log Group to monitor your gateway and get notified when your file gateway fails to upload files to an S3 bucket. You can either configure the group when you are activating the gateway or after your gateway is activated and up and running. For information about how to configure a CloudWatch Log Group when activating a gateway, see [Configuring Amazon CloudWatch logging \(p. 45\)](#). For general information about CloudWatch Log Groups, see [Working with Log Groups and Log Streams](#) in the *Amazon CloudWatch User Guide*.

The following is an example of an error reported by file gateway.

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

This error means that file gateway is unable to upload the object `myFolder/myFile.text` to S3 because it has transitioned out of the Amazon S3 Standard storage class to either Amazon S3 Glacier or S3 Glacier Deep Archive storage class.

In the preceding gateway health log, these items specify the given information:

- `source: share-E1A2B34C` indicates the file share that encountered this error.
- `"type": "InaccessibleStorageClass"` indicates the type of error that occurred. In this case, this error was encountered when the gateway was trying to upload the specified object to Amazon S3 or read from Amazon S3. However, in this case the object has transitioned to Amazon S3 Glacier. The

value of "type" can be any error that the file gateway encounters. For a list of possible errors, see [Troubleshooting file gateway issues \(p. 371\)](#).

- "operation": "S3Upload" indicates that this error occurred when the gateway was trying to upload this object to S3.
- "key": "myFolder/myFile.text" indicates the object that caused the failure.
- "gateway": "sgw-B1D123D4" indicates the file gateway that encountered this error.
- "timestamp": "1565740862516" indicate the time that the error occurred.

For information about how to troubleshoot and fix these types of errors, see [Troubleshooting file gateway issues \(p. 371\)](#).

## Configuring a CloudWatch Log Group after your gateway is activated

The following procedure shows you how to configure a CloudWatch Log Group after your gateway is activated.

### To configure a CloudWatch Log Group to work with your file gateway

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to configure the CloudWatch Log Group for.
3. For **Actions**, choose **Edit gateway information** or on the **Details** tab, under **Health logs and Not Enabled**, choose **Configure log group** to open the **Edit CustomerGatewayName** dialog box.
4. For **Gateway health log group**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.
  - **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.  
Choose a log group from the **Existing log group list**.
5. Choose **Save changes**.
6. To see the health logs for your gateway, do the following:
  1. In the navigation pane, choose **Gateways**, and then choose the gateway that you configured the CloudWatch Log Group for.
  2. Choose the **Details** tab, and under **Health logs**, choose **CloudWatch Logs**. The **Log group details** page opens in the CloudWatch console.

For information about how to troubleshoot errors, see [Troubleshooting file gateway issues \(p. 371\)](#).

## Using Amazon CloudWatch metrics

You can get monitoring data for your file gateway by using either the AWS Management Console or the CloudWatch API. The console displays a series of graphs based on the raw data from the CloudWatch API. The CloudWatch API can also be used through one of the [AWS Software Development Kits \(SDKs\)](#) or the [Amazon CloudWatch API](#) tools. Depending on your needs, you might prefer to use either the graphs displayed in the console or retrieved from the API.

Regardless of which method you choose to use to work with metrics, you must specify the following information:

- The metric dimension to work with. A *dimension* is a name-value pair that helps you to uniquely identify a metric. The dimensions for Storage Gateway are `GatewayId` and `GatewayName`. In the CloudWatch console, you can use the `Gateway Metrics` view to easily select gateway-specific dimensions. For more information about dimensions, see [Dimensions](#) in the *Amazon CloudWatch User Guide*.
- The metric name, such as `ReadBytes`.

The following table summarizes the types of Storage Gateway metric data that are available to you.

Amazon CloudWatch namespace	Dimension	Description
AWS / StorageGateway	GatewayId, GatewayName	<p>These dimensions filter for metric data that describes aspects of the gateway. You can identify a file gateway to work with by specifying both the <code>GatewayId</code> and the <code>GatewayName</code> dimensions.</p> <p>Throughput and latency data of a gateway are based on all the file shares in the gateway.</p> <p>Data is available automatically in 5-minute periods at no charge.</p>

Working with gateway and file metrics is similar to working with other service metrics. You can find a discussion of some of the most common metrics tasks in the CloudWatch documentation listed following:

- [Viewing available metrics](#)
- [Getting statistics for a metric](#)
- [Creating CloudWatch alarms](#)

## Getting notified about file operations

Storage Gateway can trigger CloudWatch Events when your file operations are done:

- You can get notified when the gateway finishes the asynchronous uploading of your files from the file share to Amazon S3. Use the `NotificationPolicy` parameter to request a file upload notification. This sends a notification for each completed file upload to Amazon S3. For more information, see [Getting file upload notification \(p. 228\)](#).
- You can get notified when the gateway finishes the asynchronous uploading of your working file set from the file share to Amazon S3. Use the `NotifyWhenUploaded` API operation to request a working file set upload notification. This sends a notification when all files in the working file set have been uploaded to Amazon S3. For more information, see [Getting working file set upload notification \(p. 230\)](#).
- You can get notified when the gateway finishes refreshing the cache for your S3 bucket. When you invoke the `RefreshCache` operation through the Storage Gateway console or Storage Gateway API, subscribe to the notification when the operation is complete. For more information, see [Getting refresh cache notification \(p. 231\)](#).

When the file operation you requested is done, Storage Gateway sends you a notification through CloudWatch Events. You can configure CloudWatch Events to send the notification through event targets

such as Amazon SNS, Amazon SQS, or an AWS Lambda function. For example, you can configure an Amazon SNS target to send the notification to Amazon SNS consumers such as an email or text message. For information about CloudWatch Events, see [What is CloudWatch Events?](#)

### To set up CloudWatch Events notification

1. Create a target, such as an Amazon SNS topic or Lambda function, to invoke when the event you requested in Storage Gateway is triggered.
2. Create a rule in the CloudWatch Events console to invoke targets based on an event in Storage Gateway.
3. In the rule, create an event pattern for the event type. The notification is triggered when the event matches this rule pattern.
4. Select the target and configure the settings.

The following example shows a rule that triggers the specified event type in the specified gateway and in the specified AWS Region. For example, you could specify the `Storage Gateway File Upload Event` as the event type.

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

For information about how to use CloudWatch Events to trigger rules, see [Creating a CloudWatch Events rule that triggers on an event](#) in the *Amazon CloudWatch Events User Guide*.

## Getting file upload notification

There are two use cases in which you can use file upload notification:

- For automating in-cloud processing of files that are uploaded, you can call the `NotificationPolicy` parameter and get back a notification ID. The notification that is triggered when the files have been uploaded has the same notification ID as the one that was returned by the API. If you map this notification ID to track the list of files that you are uploading, you can trigger processing of the file that is uploaded in AWS when the event with the same ID is generated.
- For content distribution use cases, you can have two file gateways that map to the same Amazon S3 bucket. The file share client for Gateway1 could upload new files to Amazon S3, and the files are read by file share clients on Gateway2. The files upload to Amazon S3, but they are not visible to Gateway2 because it uses a locally cached version of files in S3. To make the files visible in Gateway2, you can use the `NotificationPolicy` parameter to request file upload notification from Gateway1 to notify you when the upload file is done. You can then use the CloudWatch Events to automatically issue a `RefreshCache` request for the file share on Gateway2. When the `RefreshCache` request is complete, the new file is visible in Gateway2.

### Example Example—File upload notification

The following example shows a file upload notification that is sent to you through CloudWatch when the event matches the rule you created. This notification is in JSON format. You can configure this

notification to be delivered to the target as a text message. The detail-type is Storage Gateway Object Upload Event.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/ggw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "my-bucket",
    }
}
```

Field names	Description
version	The current version of the IAM policy.
id	The ID that identifies the IAM policy.
detail-type	A description of the event that triggered the notification that was sent.
source	The AWS service that is the source of the request and notification.
account	The ID of the Amazon Web Services account where the request and notification were generated from.
time	When the request to upload files to Amazon S3 was made.
region	The AWS Region where the request and notification was sent from.
resources	The storage gateway resources that the policy applies to.
object-size	The size of the object in bytes.
modification-time	The time the client modified the file.
object-key	The path to the file.
event-type	The CloudWatch Events that triggered the notification.
prefix	The prefix name of the S3 bucket.

Field names	Description
bucket-name	The name of the S3 bucket.

## Getting working file set upload notification

There are two use cases in which you can use the working file set upload notification:

- For automating in-cloud processing of files that are uploaded, you can call the [NotifyWhenUploaded](#) API and get back a notification ID. The notification that is triggered when the working set of files have been uploaded has the same notification ID as the one that was returned by the API. If you map this notification ID to track the list of files that you are uploading, you can trigger processing of the working set of files that are uploaded in AWS when the event with the same ID is generated.
- For content distribution use cases, you can have two file gateways that map to the same Amazon S3 bucket. The file share client for Gateway1 can upload new files to Amazon S3, and the files are read by file share clients on Gateway2. The files upload to Amazon S3, but they aren't visible to Gateway2 because it uses a locally cached version of files in S3. To make the files visible in Gateway2, use the [NotifyWhenUploaded](#) API operation to request file upload notification from Gateway1, to notify you when the upload of the working set of files is done. You can then use the CloudWatch Events to automatically issue a [RefreshCache](#) request for the file share on Gateway2. When the [RefreshCache](#) request is complete, the new files are visible in Gateway2. This operation does not import files into the file gateway cache storage. It only updates the cached inventory to reflect changes in the inventory of the objects in the S3 bucket.

### Example Example—Working file set upload notification

The following example shows a working file set upload notification that is sent to you through CloudWatch when the event matches the rule you created. This notification is in JSON format. You can configure this notification to be delivered to the target as a text message. The detail-type is `Storage Gateway File Upload Event`.

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

Field names	Description
version	The current version of the IAM policy.
id	The ID that identifies the IAM policy.

Field names	Description
detail-type	A description of the event that triggered the notification that was sent.
source	The AWS service that is the source of the request and notification.
account	The ID of the Amazon Web Services account where the request and notification were generated from.
time	When the request to upload files to Amazon S3 was made.
region	The AWS Region where the request and notification was sent from.
resources	The storage gateway resources that the policy applies to.
event-type	The CloudWatch Events that triggered the notification.
notification-id	The randomly generated ID of the notification that was sent. This ID is in UUID format. This is the notification ID that is returned when <code>NotifyWhenUploaded</code> is called.
request-received	When the gateway received the <code>NotifyWhenUploaded</code> request.
completed	When all the files in the working-set were uploaded to Amazon S3.

## Getting refresh cache notification

For refresh cache notification use case, you can have two file gateways that map to the same Amazon S3 bucket and the NFS client for Gateway1 uploads new files to the S3 bucket. The files upload to Amazon S3, but they don't appear in Gateway2 until you refresh the cache. This is because Gateway2 uses a locally cached version of the files in S3. You might want to do something with the files in Gateway2 when the refresh cache is done. Large files could take a while to show up in Gateway2, so you might want to be notified when the cache refresh is done. You can request refresh cache notification from Gateway2 to notify you when all the files are visible in Gateway2.

### Example Example—Refresh cache notification

The following example shows a refresh cache notification that is sent to you through CloudWatch when the event matches the rule you created. This notification is in JSON format. You can configure this notification to be delivered to the target as a text message. The `detail-type` is `Storage Gateway Refresh Cache Event`.

```
{
  "version": "2012-10-17",
  "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
  "detail-type": "Storage Gateway Refresh Cache Event",
  "source": "aws.storagegateway",
  "account": "209870788375",
```

```

"time": "2017-11-06T21:34:42Z",
"region": "us-east-2",
"resources": [
    "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
    "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
],
"detail": {
    "event-type": "refresh-complete",
    "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
    "started": "2018-02-06T21:34:42Z",
    "completed": "2018-02-06T21:34:53Z",
    "folderList": [
        "/"
    ]
}
}

```

Field names	Description
version	The current version of the IAM policy.
id	The ID that identifies the IAM policy.
detail-type	A description of the type of the event that triggered notification that was sent.
source	The AWS service that is the source of the request and notification.
account	The ID of the Amazon Web Services account where the request and notification were generated from.
time	When the request to refresh the files in working-set was made.
region	The AWS Region where the request and notification was sent from.
resources	The storage gateway resources that the policy applies to.
event-type	The CloudWatch Events that triggered the notification.
notification-id	The randomly generated ID of the notification that was sent. This ID is in UUID format. This is the notification ID that is returned when you call RefreshCache.
started	when the gateway received the RefreshCache request and the refresh was started.
completed	When the refresh of the working-set was completed.
folderList	A comma-separated list of the paths of folders that were refreshed in the cache. The default is ["/"].

## Understanding file share metrics

You can find information following about the Storage Gateway metrics that cover file shares. Each file share has a set of metrics associated with it. Some file share-specific metrics have the same name as certain gateway-specific metrics. These metrics represent the same kinds of measurements, but are scoped to the file share instead. Always specify whether you want to work with either a gateway or a file share metric before working with a metric. Specifically, when working with file share metrics, you must specify the `File share ID` that identifies the file share for which you are interested in viewing metrics. For more information, see [Using Amazon CloudWatch metrics \(p. 226\)](#).

The following table describes the Storage Gateway metrics that you can use to get information about your file shares.

Metric	Description
<code>CacheHitPercent</code>	<p>Percent of application read operations from the file shares that are served from cache. The sample is taken at the end of the reporting period.</p> <p>When there are no application read operations from the file share, this metric reports 100 percent.</p> <p>Units: Percent</p>
<code>CachePercentDirty</code>	<p>The file share's contribution to the overall percentage of the gateway's cache that has not been persisted to AWS. The sample is taken at the end of the reporting period.</p> <p>Use the <code>CachePercentDirty</code> metric of the gateway to view the overall percentage of the gateway's cache that has not been persisted to AWS. For more information, see <a href="#">Understanding gateway metrics (p. 215)</a>.</p> <p>Units: Percent</p>
<code>CachePercentUsed</code>	<p>The file share's contribution to the overall percent use of the gateway's cache storage. The sample is taken at the end of the reporting period.</p> <p>Use the <code>CachePercentUsed</code> metric of the gateway to view overall percent use of the gateway's cache storage. For more information, see <a href="#">Understanding gateway metrics (p. 215)</a>.</p> <p>Units: Percent</p>
<code>CloudBytesUploaded</code>	<p>The total number of bytes that the gateway uploaded to AWS during the reporting period.</p> <p>Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.</p> <p>Units: Bytes</p>

Metric	Description
CloudBytesDownloaded	<p>The total number of bytes that the gateway downloaded from AWS during the reporting period.</p> <p>Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure input/output operations per second (IOPS).</p> <p>Units: Bytes</p>
ReadBytes	<p>The total number of bytes read from your on-premises applications in the reporting period for a file share.</p> <p>Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.</p> <p>Units: Bytes</p>
WriteBytes	<p>The total number of bytes written to your on-premises applications in the reporting period.</p> <p>Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.</p> <p>Units: Bytes</p>

## Understanding file gateway audit logs

File gateway audit logs provide you with details about user access to files and folders within a file share. You can use them to monitor user activities and take action if inappropriate activity patterns are identified.

The following table describes the file gateway audit log file access operations.

Operation name	Definition
Read Data	Read the content of a file.
Write Data	Change the content of a file.
Create	Create a new file or folder.
Rename	Rename an existing file or folder.
Delete	Delete a file or folder.
Write Attributes	Update file or folder metadata (ACLs, owner, group, permissions).

The following table describes the S3 File Gateway audit log file access attributes.

Attribute	Definition
accessMode	The permission setting for the object.
accountDomain ( <b>SMB only</b> )	The Active Directory (AD) domain that the client's account belongs to.
accountName ( <b>SMB only</b> )	The Active Directory user name of the client.
bucket	The S3 bucket name.
clientGid ( <b>NFS only</b> )	The identifier of the group of the user accessing the object.
clientUid ( <b>NFS only</b> )	The identifier of the user accessing the object.
ctime	The time that the object's content or metadata was modified, set by the client.
groupId	The identifier for group owner of the object.
fileSizeInBytes	The size of the file in bytes, set by the client at file creation time.
gateway	The Storage Gateway ID.
mtime	This time that the object's content was modified, set by the client.
newObjectName	The full path to the new object after it has been renamed.
objectName	The full path to the object.
objectType	Defines whether the object is a file or folder.
operation	The name of the object access operation.
ownerId	The identifier for the owner of the object.
securityDescriptor ( <b>SMB only</b> )	Shows the discretionary access control list (DACL) set on an object, in SDDL format.
shareName	The name of the share that is being accessed.
source	The ID of the file share being audited.
sourceAddress	The IP address of file share client machine.
status	The status of the operation. Only success is logged (failures are logged with the exception of failures arising from permissions denied).
timestamp	The time that the operation occurred based on the OS timestamp of the gateway.
version	The version of the audit log format.

The following table describes the S3 File Gateway audit log attributes logged in each file access operation.

Attribute	Read data	Write data	Create folder	Create file	Rename file/folder	Delete file/folder	Write attribute (change ACL - SMB only)	attribute (chown)	attribute (chmod)	attribute (chgrp)
accessMode			X	X					X	
accountDomain <b>(SMB only)</b>	X	X	X	X	X	X	X	X	X	X
accountName <b>(SMB only)</b>	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
clientGid <b>(NFS only)</b>	X	X	X	X	X	X		X	X	X
clientUid <b>(NFS only)</b>	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupId			X	X						
fileSizeInBytes				X						
gateway	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObjectName					X					
objectName	X	X	X	X	X	X	X	X	X	X
objectType	X	X	X	X	X	X	X	X	X	X
operation	X	X	X	X	X	X	X	X	X	X
ownerId			X	X				X		
securityDescriptor <b>(SMB only)</b>							X	X		
shareName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
sourceAddress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timestamp	X	X	X	X	X	X	X	X	X	X

Attribute	Read data	Write data	Create folder	Create file	Rename file/folder	Delete file/folder	Write attributes (change ACL - SMB only)	Write attributes (chown)	Write attributes (chmod)	Write attributes (chgrp)
version	X	X	X	X	X	X	X	X	X	X

## Monitoring Your Volume Gateway

In this section, you can find information about how to monitor a gateway in a cached volumes or stored volumes setup, including monitoring the volumes associated with the gateway and monitoring the upload buffer. You use the AWS Management Console to view metrics for your gateway. For example, you can view the number of bytes used in read and write operations, the time spent in read and write operations, and the time taken to retrieve data from the Amazon Web Services cloud. With metrics, you can track the health of your gateway and set up alarms to notify you when one or more metrics fall outside a defined threshold.

Storage Gateway provides CloudWatch metrics at no additional charge. Storage Gateway metrics are recorded for a period of two weeks. By using these metrics, you can access historical information and get a better perspective on how your gateway and volumes are performing. For detailed information about CloudWatch, see the [Amazon CloudWatch User Guide](#).

### Topics

- [Getting Volume Gateway Health Logs with CloudWatch Log Groups \(p. 237\)](#)
- [Using Amazon CloudWatch Metrics \(p. 238\)](#)
- [Measuring Performance Between Your Application and Gateway \(p. 239\)](#)
- [Measuring Performance Between Your Gateway and AWS \(p. 241\)](#)
- [Understanding Volume Metrics \(p. 243\)](#)

## Getting Volume Gateway Health Logs with CloudWatch Log Groups

You can use Amazon CloudWatch Logs to get information about the health of your volume gateway and related resources. You can use the logs to monitor your gateway for errors that it encounters. In addition, you can use Amazon CloudWatch subscription filters to automate processing of the log information in real time. For more information, see [Real-time Processing of Log Data with Subscriptions](#) in the *Amazon CloudWatch User Guide*.

For example, suppose that your gateway is deployed in a cluster enabled with VMware HA and you need to know about any errors. You can configure a CloudWatch log group to monitor your gateway and get notified when your gateway encounters an error. You can either configure the group when you are activating the gateway or after your gateway is activated and up and running. For information about how to configure a CloudWatch log group when activating a gateway, see [Configuring Amazon CloudWatch Logging \(p. 72\)](#). For general information about CloudWatch log groups, see [Working with Log Groups and Log Streams](#) in the *Amazon CloudWatch User Guide*.

For information about how to troubleshoot and fix these types of errors, see [Troubleshooting volume issues \(p. 379\)](#).

The following procedure shows you how to configure a CloudWatch log group after your gateway is activated.

## To configure a CloudWatch Log Group to work with your file gateway

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to configure the CloudWatch Log Group for.
3. For **Actions**, choose **Edit gateway information** or on the **Details** tab, under **Health logs and Not Enabled**, choose **Configure log group** to open the **Edit CustomerGatewayName** dialog box.
4. For **Gateway health log group**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.
  - **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.Choose a log group from the **Existing log group list**.
5. Choose **Save changes**.
6. To see the health logs for your gateway, do the following:
  1. In the navigation pane, choose **Gateways**, and then choose the gateway that you configured the CloudWatch Log Group for.
  2. Choose the **Details** tab, and under **Health logs**, choose **CloudWatch Logs**. The **Log group details** page opens in the CloudWatch console.

## Using Amazon CloudWatch Metrics

You can get monitoring data for your gateway using either the AWS Management Console or the CloudWatch API. The console displays a series of graphs based on the raw data from the CloudWatch API. You can also use the CloudWatch API through one of the [AWS Software Development Kits \(SDKs\)](#) or the [Amazon CloudWatch API](#) tools. Depending on your needs, you might prefer to use either the graphs displayed in the console or retrieved from the API.

Regardless of which method you choose to use to work with metrics, you must specify the following information:

- The metric dimension to work with. A *dimension* is a name-value pair that helps you to uniquely identify a metric. The dimensions for Storage Gateway are `GatewayId`, `GatewayName`, and `VolumeId`. In the CloudWatch console, you can use the `Gateway Metrics` and `Volume Metrics` views to easily select gateway-specific and volume-specific dimensions. For more information about dimensions, see [Dimensions in the Amazon CloudWatch User Guide](#).
- The metric name, such as `ReadBytes`.

The following table summarizes the types of Storage Gateway metric data that you can use.

CloudWatch Namespace	Dimension	Description
AWS / StorageGateway	GatewayId, GatewayName	<p>These dimensions filter for metric data that describes aspects of the gateway. You can identify a gateway to work with by specifying both the <code>GatewayId</code> and the <code>GatewayName</code> dimensions.</p> <p>Throughput and latency data of a gateway are based on all the volumes in the gateway.</p>

CloudWatch Namespace	Dimension	Description
		Data is available automatically in 5-minute periods at no charge.
	VolumeId	This dimension filters for metric data that is specific to a volume. Identify a volume to work with by its VolumeId dimension.  Data is available automatically in 5-minute periods at no charge.

Working with gateway and volume metrics is similar to working with other service metrics. You can find a discussion of some of the most common metrics tasks in the CloudWatch documentation listed following:

- [Viewing Available Metrics](#)
- [Getting Statistics for a Metric](#)
- [Creating CloudWatch Alarms](#)

## Measuring Performance Between Your Application and Gateway

Data throughput, data latency, and operations per second are three measures that you can use to understand how your application storage that is using your gateway is performing. When you use the correct aggregation statistic, you can use Storage Gateway metrics to measure these values.

A *statistic* is an aggregation of a metric over a specified period of time. When you view the values of a metric in CloudWatch, use the *Average* statistic for data latency (milliseconds), use the *Sum* statistic for data throughput (bytes per second), and use the *Samples* statistic for input/output operations per second (IOPS). For more information, see [Statistics](#) in the *Amazon CloudWatch User Guide*.

The following table summarizes the metrics and corresponding statistic you can use to measure the throughput, latency, and IOPS between your applications and gateways.

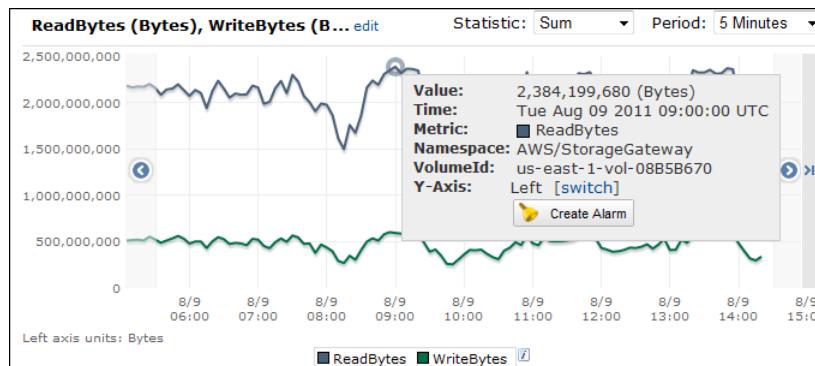
Item of Interest	How to Measure
Throughput	Use the <code>ReadBytes</code> and <code>WriteBytes</code> metrics with the <code>Sum</code> CloudWatch statistic. For example, the <code>Sum</code> value of the <code>ReadBytes</code> metric over a sample period of 5 minutes divided by 300 seconds gives you the throughput as a rate in bytes per second.
Latency	Use the <code>ReadTime</code> and <code>WriteTime</code> metrics with the <code>Average</code> CloudWatch statistic. For example, the <code>Average</code> value of the <code>ReadTime</code> metric gives you the latency per operation over the sample period of time.
IOPS	Use the <code>ReadBytes</code> and <code>WriteBytes</code> metrics with the <code>Samples</code> CloudWatch statistic. For example, the <code>Samples</code> value of the <code>ReadBytes</code> metric over a sample period of 5 minutes divided by 300 seconds gives you IOPS.

For the average latency graphs and average size graphs, the average is calculated over the total number of operations (read or write, whichever is applicable to the graph) that completed during the period.

### To measure the data throughput from an application to a volume

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Metrics**, then choose the **All metrics** tab and then choose **Storage Gateway**.
3. Choose the **Volume metrics** dimension, and find the volume that you want to work with.
4. Choose the **ReadBytes** and **WriteBytes** metrics.
5. For **Time Range**, choose a value.
6. Choose the **Sum** statistic.
7. For **Period**, choose a value of 5 minutes or greater.
8. In the resulting time-ordered sets of data points (one for **ReadBytes** and one for **WriteBytes**), divide each data point by the period (in seconds) to get the throughput at the sample point. The total throughput is the sum of the throughputs.

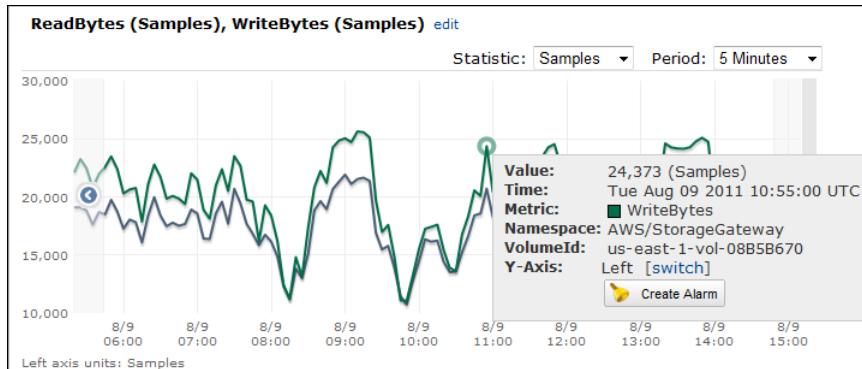
The following image shows the **ReadBytes** and **WriteBytes** metrics for a volume with the **Sum** statistic. In the image, the cursor over a data point displays information about the data point including its value and the number of bytes. Divide the bytes value by the **Period** value (5 minutes) to get the data throughput at that sample point. For the point highlighted, the read throughput is 2,384,199,680 bytes divided by 300 seconds, which is 7.6 megabytes per second.



### To measure the data input/output operations per second from an application to a volume

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Metrics**, then choose the **All metrics** tab and then choose **Storage Gateway**.
3. Choose the **Volume metrics** dimension, and find the volume that you want to work with.
4. Choose the **ReadBytes** and **WriteBytes** metrics.
5. For **Time Range**, choose a value.
6. Choose the **Samples** statistic.
7. For **Period**, choose a value of 5 minutes or greater.
8. In the resulting time-ordered sets of data points (one for **ReadBytes** and one for **WriteBytes**), divide each data point by the period (in seconds) to get IOPS.

The following image shows the **ReadBytes** and **WriteBytes** metrics for a storage volume with the **Samples** statistic. In the image, the cursor over a data point displays information about the data point, including its value and the number of samples. Divide the samples value by the **Period** value (5 minutes) to get the operations per second at that sample point. For the point highlighted, the number of write operations is 24,373 bytes divided by 300 seconds, which is 81 write operations per second.



## Measuring Performance Between Your Gateway and AWS

Data throughput, data latency, and operations per second are three measures that you can use to understand how your application storage using the Storage Gateway is performing. These three values can be measured using the Storage Gateway metrics provided for you when you use the correct aggregation statistic. The following table summarizes the metrics and corresponding statistic to use to measure the throughput, latency, and input/output operations per second (IOPS) between your gateway and AWS.

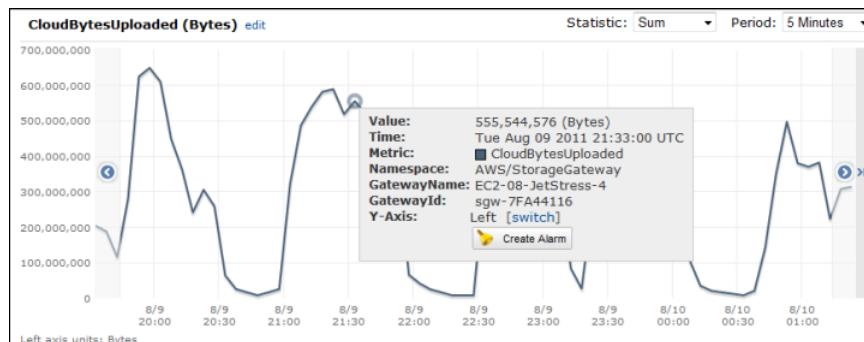
Item of Interest	How to Measure
Throughput	Use the <code>ReadBytes</code> and <code>WriteBytes</code> metrics with the <code>Sum</code> CloudWatch statistic. For example, the <code>Sum</code> value of the <code>ReadBytes</code> metric over a sample period of 5 minutes divided by 300 seconds gives you the throughput as a rate in bytes per second.
Latency	Use the <code>ReadTime</code> and <code>WriteTime</code> metrics with the <code>Average</code> CloudWatch statistic. For example, the <code>Average</code> value of the <code>ReadTime</code> metric gives you the latency per operation over the sample period of time.
IOPS	Use the <code>ReadBytes</code> and <code>WriteBytes</code> metrics with the <code>Samples</code> CloudWatch statistic. For example, the <code>Samples</code> value of the <code>ReadBytes</code> metric over a sample period of 5 minutes divided by 300 seconds gives you IOPS.
Throughput to AWS	Use the <code>CloudBytesDownloaded</code> and <code>CloudBytesUploaded</code> metrics with the <code>Sum</code> CloudWatch statistic. For example, the <code>Sum</code> value of the <code>CloudBytesDownloaded</code> metric over a sample period of 5 minutes divided by 300 seconds gives you the throughput from AWS to the gateway as bytes per second.
Latency of data to AWS	Use the <code>CloudDownloadLatency</code> metric with the <code>Average</code> statistic. For example, the <code>Average</code> statistic of the <code>CloudDownloadLatency</code> metric gives you the latency per operation.

### To measure the upload data throughput from a gateway to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Metrics**, then choose the **All metrics** tab and then choose **Storage Gateway**.
3. Choose the **Gateway metrics** dimension, and find the volume that you want to work with.
4. Choose the `CloudBytesUploaded` metric.

5. For **Time Range**, choose a value.
6. Choose the **Sum** statistic.
7. For **Period**, choose a value of 5 minutes or greater.
8. In the resulting time-ordered set of data points, divide each data point by the period (in seconds) to get the throughput at that sample period.

The following image shows the **CloudBytesUploaded** metric for a gateway volume with the **Sum** statistic. In the image, the cursor over a data point displays information about the data point, including its value and bytes uploaded. Divide this value by the **Period** value (5 minutes) to get the throughput at that sample point. For the point highlighted, the throughput from the gateway to AWS is 555,544,576 bytes divided by 300 seconds, which is 1.7 megabytes per second.



#### To measure the latency per operation of a gateway

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Metrics**, then choose the **All metrics** tab and then choose **Storage Gateway**.
3. Choose the **Gateway metrics** dimension, and find the volume that you want to work with.
4. Choose the **ReadTime** and **WriteTime** metrics.
5. For **Time Range**, choose a value.
6. Choose the **Average** statistic.
7. For **Period**, choose a value of 5 minutes to match the default reporting time.
8. In the resulting time-ordered set of points (one for **ReadTime** and one for **WriteTime**), add data points at the same time sample to get to the total latency in milliseconds.

#### To measure the data latency from a gateway to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Metrics**, then choose the **All metrics** tab and then choose **Storage Gateway**.
3. Choose the **Gateway metrics** dimension, and find the volume that you want to work with.
4. Choose the **CloudDownloadLatency** metric.
5. For **Time Range**, choose a value.
6. Choose the **Average** statistic.
7. For **Period**, choose a value of 5 minutes to match the default reporting time.

The resulting time-ordered set of data points contains the latency in milliseconds.

#### To set an upper threshold alarm for a gateway's throughput to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. Choose **Alarms**.
3. Choose **Create Alarm** to start the Create Alarm wizard.
4. Choose the **Storage Gateway** dimension, and find the gateway that you want to work with.
5. Choose the `CloudBytesUploaded` metric.
6. To define the alarm, define the alarm state when the `CloudBytesUploaded` metric is greater than or equal to a specified value for a specified time. For example, you can define an alarm state when the `CloudBytesUploaded` metric is greater than 10 MB for 60 minutes.
7. Configure the actions to take for the alarm state. For example, you can have an email notification sent to you.
8. Choose **Create Alarm**.

#### To set an upper threshold alarm for reading data from AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Create Alarm** to start the Create Alarm wizard.
3. Choose the **StorageGateway: Gateway Metrics** dimension, and find the gateway that you want to work with.
4. Choose the `CloudDownloadLatency` metric.
5. Define the alarm by defining the alarm state when the `CloudDownloadLatency` metric is greater than or equal to a specified value for a specified time. For example, you can define an alarm state when the `CloudDownloadLatency` is greater than 60,000 milliseconds for greater than 2 hours.
6. Configure the actions to take for the alarm state. For example, you can have an email notification sent to you.
7. Choose **Create Alarm**.

## Understanding Volume Metrics

You can find information following about the Storage Gateway metrics that cover a volume of a gateway. Each volume of a gateway has a set of metrics associated with it.

Some volume-specific metrics have the same name as certain gateway-specific metrics. These metrics represent the same kinds of measurements but are scoped to the volume instead of the gateway. Before starting work, specify whether you want to work with a gateway metric or a volume metric. Specifically, when working with volume metrics, specify the volume ID for the storage volume that you want to view metrics for. For more information, see [Using Amazon CloudWatch Metrics \(p. 238\)](#).

The following table describes the Storage Gateway metrics that you can use to get information about your storage volumes.

Metric	Description	Cached Volumes	Stored Volumes
AvailabilityNotifications	The number of availability notifications sent by the volume.  Units: count	Yes	Yes
CacheHitPercent	Percent of application read operations from the volume that are served from cache. The sample is taken at the	Yes	No

Metric	Description	Cached Volumes	Stored Volumes
	<p>end of the reporting period.</p> <p>When there are no application read operations from the volume, this metric reports 100 percent.</p> <p>Units: Percent</p>		
CachePercentDirty	<p>The volume's contribution to the overall percentage of the gateway's cache that isn't persisted to AWS. The sample is taken at the end of the reporting period.</p> <p>Use the CachePercentDirty metric of the gateway to view the overall percentage of the gateway's cache that isn't persisted to AWS. For more information, see <a href="#">Understanding gateway metrics (p. 215)</a>.</p> <p>Units: Percent</p>	Yes	Yes
CachePercentUsed	<p>The volume's contribution to the overall percent use of the gateway's cache storage. The sample is taken at the end of the reporting period.</p> <p>Use the CachePercentUsed metric of the gateway to view overall percent use of the gateway's cache storage. For more information, see <a href="#">Understanding gateway metrics (p. 215)</a>.</p> <p>Units: Percent</p>	Yes	No

Metric	Description	Cached Volumes	Stored Volumes
CloudBytesDownloaded	The number of bytes downloaded from the cloud to the volume.  Units: Bytes	Yes	Yes
CloudBytesUploaded	The number of bytes uploaded from the cloud to the volume.  Units: Bytes	Yes	Yes
HealthNotification	The number of health notifications sent by the volume.  Units: count	Yes	Yes
IoWaitPercent	The percentage of IoWaitPercent units that are currently used by the volume.  Units: Percent	Yes	Yes
MemTotalBytes	The percentage of total memory that is currently used by the volume.  Units: Percent	Yes	No
MemoryUsage	The percentage of memory that is currently used by the volume.  Units: Percent	Yes	No
ReadBytes	The total number of bytes read from your on-premises applications in the reporting period.  Use this metric with the Sum statistic to measure throughput and with the Samplesstatistic to measure IOPS.  Units: Bytes	Yes	Yes

Metric	Description	Cached Volumes	Stored Volumes
ReadTime	<p>The total number of milliseconds spent on read operations from your on-premises applications in the reporting period.</p> <p>Use this metric with the Average statistic to measure latency.</p> <p>Units: Milliseconds</p>	Yes	Yes
UserCpuPercent	<p>The percentage of allocated CPU compute units that are currently used by the volume.</p> <p>Units: Percent</p>	Yes	Yes
WriteBytes	<p>The total number of bytes written to your on-premises applications in the reporting period.</p> <p>Use this metric with the Sum statistic to measure throughput and with the Samples statistic to measure IOPS.</p> <p>Units: Bytes</p>	Yes	Yes
WriteTime	<p>The total number of milliseconds spent on write operations from your on-premises applications in the reporting period.</p> <p>Use this metric with the Average statistic to measure latency.</p> <p>Units: Milliseconds</p>	Yes	Yes
QueuedWrites	<p>The number of bytes waiting to be written to AWS, sampled at the end of the reporting period.</p> <p>Units: Bytes</p>	Yes	Yes

# Monitoring Your Tape Gateway

In this section, you can find information about how to monitor your tape gateway, virtual tapes associated with your tape gateway, cache storage, and the upload buffer. You use the AWS Management Console to view metrics for your tape gateway. With metrics, you can track the health of your tape gateway and set up alarms to notify you when one or more metrics are outside a defined threshold.

Storage Gateway provides CloudWatch metrics at no additional charge. Storage Gateway metrics are recorded for a period of two weeks. By using these metrics, you can access historical information and get a better perspective of how your tape gateway and virtual tapes are performing. For detailed information about CloudWatch, see the [Amazon CloudWatch User Guide](#).

## Topics

- [Getting Tape Gateway Health Logs with CloudWatch Log Groups \(p. 247\)](#)
- [Using Amazon CloudWatch Metrics \(p. 248\)](#)
- [Understanding Virtual Tape Metrics \(p. 249\)](#)
- [Measuring Performance Between Your Tape Gateway and AWS \(p. 250\)](#)

## Getting Tape Gateway Health Logs with CloudWatch Log Groups

You can use Amazon CloudWatch Logs to get information about the health of your tape gateway and related resources. You can use the logs to monitor your gateway for errors that it encounters. In addition, you can use Amazon CloudWatch subscription filters to automate processing of the log information in real time. For more information, see [Real-time Processing of Log Data with Subscriptions](#) in the *Amazon CloudWatch User Guide*.

For example, suppose that your gateway is deployed in a cluster enabled with VMware HA and you need to know about any errors. You can configure a CloudWatch log group to monitor your gateway and get notified when your gateway encounters an error. You can either configure the group when you are activating the gateway or after your gateway is activated and up and running. For information about how to configure a CloudWatch log group when activating a gateway, see [Configuring Amazon CloudWatch Logging \(p. 90\)](#). For general information about CloudWatch log groups, see [Working with Log Groups and Log Streams](#) in the *Amazon CloudWatch User Guide*.

For information about how to troubleshoot and fix these types of errors, see [Troubleshooting virtual tape issues \(p. 383\)](#).

The following procedure shows you how to configure a CloudWatch log group after your gateway is activated.

### To configure a CloudWatch Log Group to work with your file gateway

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to configure the CloudWatch Log Group for.
3. For **Actions**, choose **Edit gateway information** or on the **Details** tab, under **Health logs and Not Enabled**, choose **Configure log group** to open the **Edit CustomerGatewayName** dialog box.
4. For **Gateway health log group**, choose one of the following:
  - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.

- **Create a new log group** to create a new CloudWatch log group.
  - **Use an existing log group** to use a CloudWatch log group that already exists.
- Choose a log group from the **Existing log group list**.
5. Choose **Save changes**.
  6. To see the health logs for your gateway, do the following:
    1. In the navigation pane, choose **Gateways**, and then choose the gateway that you configured the CloudWatch Log Group for.
    2. Choose the **Details** tab, and under **Health logs**, choose **CloudWatch Logs**. The **Log group details** page opens in the CloudWatch console.

Following is an example of a tape gateway event message that is sent to CloudWatch. This example shows a `TapeStatusTransition` message.

```
{  
  "severity": "INFO",  
  "source": "FZTT16FCF5",  
  "type": "TapeStatusTransition",  
  "gateway": "sgw-C51DFEAC",  
  "timestamp": "1581553463831",  
  "newStatus": "RETRIEVED"  
}
```

## Using Amazon CloudWatch Metrics

You can get monitoring data for your tape gateway by using either the AWS Management Console or the CloudWatch API. The console displays a series of graphs based on the raw data from the CloudWatch API. The CloudWatch API can also be used through one of the [Amazon AWS Software Development Kits \(SDKs\)](#) or the [Amazon CloudWatch API](#) tools. Depending on your needs, you might prefer to use either the graphs displayed in the console or retrieved from the API.

Regardless of which method you choose to use to work with metrics, you must specify the following information:

- The metric dimension to work with. A *dimension* is a name-value pair that helps you to uniquely identify a metric. The dimensions for Storage Gateway are `GatewayId` and `GatewayName`. In the CloudWatch console, you can use the `Gateway Metrics` view to easily select gateway-specific and tape-specific dimensions. For more information about dimensions, see [Dimensions](#) in the [Amazon CloudWatch User Guide](#).
- The metric name, such as `ReadBytes`.

The following table summarizes the types of Storage Gateway metric data that are available to you.

Amazon CloudWatch Namespace	Dimension	Description
AWS / StorageGateway	GatewayId, GatewayName	These dimensions filter for metric data that describes aspects of the tape gateway. You can identify a tape gateway to work with by specifying both the <code>GatewayId</code> and the <code>GatewayName</code> dimensions.

Amazon CloudWatch Namespace	Dimension	Description
		<p>Throughput and latency data of a tape gateway is based on all the virtual tapes in the tape gateway.</p> <p>Data is available automatically in 5-minute periods at no charge.</p>

Working with gateway and tape metrics is similar to working with other service metrics. You can find a discussion of some of the most common metrics tasks in the CloudWatch documentation listed following:

- [Viewing Available Metrics](#)
- [Getting Statistics for a Metric](#)
- [Creating CloudWatch Alarms](#)

## Understanding Virtual Tape Metrics

You can find information following about the Storage Gateway metrics that cover virtual tapes. Each tape has a set of metrics associated with it.

Some tape-specific metrics might have the same name as certain gateway-specific metrics. These metrics represent the same kinds of measurements but are scoped to a tape instead of a gateway. Before starting work, specify whether you want to work with a gateway metric or a tape metric. When working with tape metrics, specify the tape ID for the tape that you want to view metrics for. For more information, see [Using Amazon CloudWatch Metrics \(p. 238\)](#).

The following table describes the Storage Gateway metrics that you can use to get information about your tapes.

Metric	Description
CachePercentDirty	<p>The tape's contribution to the overall percentage of the gateway's cache that isn't persisted to AWS. The sample is taken at the end of the reporting period.</p> <p>Use the CachePercentDirty metric of the gateway to view the overall percentage of the gateway's cache that isn't persisted to AWS. For more information, see <a href="#">Understanding gateway metrics (p. 215)</a>.</p> <p>Units: Percent</p>
CloudTraffic	<p>The amount of bytes uploaded and downloaded from the cloud to the tape.</p> <p>Units: bytes</p>
IoWaitPercent	<p>The percentage of allocated IoWait units that are currently used by the tape.</p> <p>Units: Percent</p>

Metric	Description
HealthNotification	The number of health notifications sent by the tape.  Units: count
MemUsedBytes	The percentage of allocated memory that is currently used by the tape.  Units: Percent
MemTotalBytes	The percentage of total memory that is currently used by the tape.  Units: Percent
ReadBytes	The total number of bytes read from your on-premises applications in the reporting period for a file share.  Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.  Units: Bytes
UserCpuPercent	The percentage of allocated CPU compute units for the user that are currently used by the tape.  Units: Percent
WriteBytes	The total number of bytes written to your on-premises applications in the reporting period.  Use this metric with the <code>Sum</code> statistic to measure throughput and with the <code>Samples</code> statistic to measure IOPS.  Units: Bytes

## Measuring Performance Between Your Tape Gateway and AWS

Data throughput, data latency, and operations per second are measures that you can use to understand how your application storage that is using your tape gateway is performing. When you use the correct aggregation statistic, these values can be measured by using the Storage Gateway metrics that are provided for you.

A *statistic* is an aggregation of a metric over a specified period of time. When you view the values of a metric in CloudWatch, use the `Average` statistic for data latency (milliseconds), and use the `Samples` statistic for input/output operations per second (IOPS). For more information, see [Statistics](#) in the [Amazon CloudWatch User Guide](#).

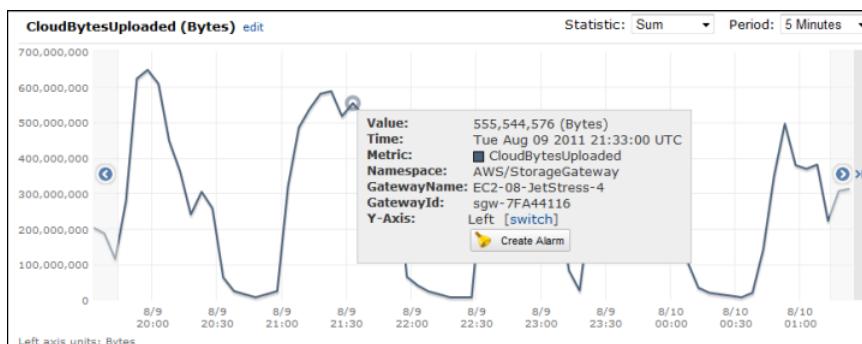
The following table summarizes the metrics and the corresponding statistic you can use to measure the throughput, latency, and IOPS between your tape gateway and AWS.

Item of Interest	How to Measure
Latency	Use the <code>ReadTime</code> and <code>WriteTime</code> metrics with the <code>Average</code> CloudWatch statistic. For example, the <code>Average</code> value of the <code>ReadTime</code> metric gives you the latency per operation over the sample period of time.
Throughput to AWS	Use the <code>CloudBytesDownloaded</code> and <code>CloudBytesUploaded</code> metrics with the <code>Sum</code> CloudWatch statistic. For example, the <code>Sum</code> value of the <code>CloudBytesDownloaded</code> metric over a sample period of 5 minutes divided by 300 seconds gives you the throughput from AWS to the tape gateway as a rate in bytes per second.
Latency of data to AWS	Use the <code>CloudDownloadLatency</code> metric with the <code>Average</code> statistic. For example, the <code>Average</code> statistic of the <code>CloudDownloadLatency</code> metric gives you the latency per operation.

### To measure the upload data throughput from a tape gateway to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose the **Metrics** tab.
3. Choose the **StorageGateway: Gateway Metrics** dimension, and find the tape gateway that you want to work with.
4. Choose the `CloudBytesUploaded` metric.
5. For **Time Range**, choose a value.
6. Choose the `Sum` statistic.
7. For **Period**, choose a value of 5 minutes or greater.
8. In the resulting time-ordered set of data points, divide each data point by the period (in seconds) to get the throughput at that sample period.

The following image shows the `CloudBytesUploaded` metric for a gateway tape with the `Sum` statistic. In the image, placing the cursor over a data point displays information about the data point, including its value and the number of bytes uploaded. Divide this value by the **Period** value (5 minutes) to get the throughput at that sample point. For the point highlighted, the throughput from the tape gateway to AWS is 555,544,576 bytes divided by 300 seconds, which is 1.7 megabytes per second.



### To measure the data latency from a tape gateway to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose the **Metrics** tab.
3. Choose the **StorageGateway: GatewayMetrics** dimension, and find the tape gateway that you want to work with.

4. Choose the `CloudDownloadLatency` metric.
5. For **Time Range**, choose a value.
6. Choose the **Average** statistic.
7. For **Period**, choose a value of 5 minutes to match the default reporting time.

The resulting time-ordered set of data points contains the latency in milliseconds.

#### To set an upper threshold alarm for a tape gateway's throughput to AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Create Alarm** to start the Create Alarm wizard.
3. Choose the **StorageGateway: Gateway Metrics** dimension, and find the tape gateway that you want to work with.
4. Choose the `CloudBytesUploaded` metric.
5. Define the alarm by defining the alarm state when the `CloudBytesUploaded` metric is greater than or equal to a specified value for a specified time. For example, you can define an alarm state when the `CloudBytesUploaded` metric is greater than 10 megabytes for 60 minutes.
6. Configure the actions to take for the alarm state. For example, you can have an email notification sent to you.
7. Choose **Create Alarm**.

#### To set an upper threshold alarm for reading data from AWS

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Choose **Create Alarm** to start the Create Alarm wizard.
3. Choose the **StorageGateway: Gateway Metrics** dimension, and find the tape gateway that you want to work with.
4. Choose the `CloudDownloadLatency` metric.
5. Define the alarm by defining the alarm state when the `CloudDownloadLatency` metric is greater than or equal to a specified value for a specified time. For example, you can define an alarm state when the `CloudDownloadLatency` is greater than 60,000 milliseconds for greater than 2 hours.
6. Configure the actions to take for the alarm state. For example, you can have an email notification sent to you.
7. Choose **Create Alarm**.

# Maintaining Your Gateway

Maintaining your gateway includes tasks such as configuring cache storage and upload buffer space, and doing general maintenance your gateway's performance. These tasks are common to all gateway types. If you haven't created a gateway, see [Creating Your Gateway \(p. 40\)](#).

## Topics

- [Shutting Down Your Gateway VM \(p. 253\)](#)
- [Managing local disks for your Storage Gateway \(p. 254\)](#)
- [Managing Bandwidth for Your Gateway \(p. 258\)](#)
- [Managing Gateway Updates Using the AWS Storage Gateway Console \(p. 263\)](#)
- [Performing Maintenance Tasks on the Local Console \(p. 264\)](#)
- [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#)

## Shutting Down Your Gateway VM

You might need to shutdown or reboot your VM for maintenance, such as when applying a patch to your hypervisor. Before you shutdown the VM, you must first stop the gateway. For file gateway, you just shutdown your VM. Although this section focuses on starting and stopping your gateway using the Storage Gateway Management Console, you can also start and stop your gateway by using your VM local console or Storage Gateway API. When you power on your VM, remember to restart your gateway.

- Gateway VM local console—see [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).
- Storage Gateway API—see [ShutdownGateway](#)

### Note

If you stop your gateway while your backup software is writing or reading from a tape, the write or read task might not succeed. Before you stop your gateway, you should check your backup software and the backup schedule for any tasks in progress.

For file gateway, you simply shutdown your VM. You don't shutdown the gateway.

## Starting and Stopping a Volume or Tape Gateway

The following instructions apply to volume and tape gateways only.

### To stop a volume or tape gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway to stop. The status of the gateway is **Running**.
3. For **Actions**, choose **Stop gateway** and verify the id of the gateway from the dialog box, and then choose **Stop gateway**.

While the gateway is stopping, you might see a message that indicates the status of the gateway. When the gateway shuts down, a message and a **Start gateway** button appears in the **Details** tab.

When you stop your gateway, the storage resources will not be accessible until you start your storage. If the gateway was uploading data when it was stopped, the upload will resume when you start the gateway.

### To start a volume or tape gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways** and then choose the gateway to start. The status of the gateway is **Shutdown**.
3. Choose **Details**, and then choose **Start gateway**.

## Managing local disks for your Storage Gateway

The gateway virtual machine (VM) uses the local disks that you allocate on-premises for buffering and storage. Gateways created on Amazon EC2 instances use Amazon EBS volumes as local disks.

### Topics

- [Deciding the amount of local disk storage \(p. 254\)](#)
- [Determining the size of upload buffer to allocate \(p. 255\)](#)
- [Determining the size of cache storage to allocate \(p. 256\)](#)
- [Adding an upload buffer or cache storage \(p. 256\)](#)
- [Using ephemeral storage with EC2 gateways \(p. 257\)](#)

## Deciding the amount of local disk storage

The number and size of disks that you want to allocate for your gateway is up to you. Depending on the storage solution you deploy (see [Plan your Storage Gateway deployment \(p. 9\)](#)), the gateway requires the following additional storage:

- File gateways require at least one disk to use as a cache.
- Volume gateways:
  - Stored gateways require at least one disk to use as an upload buffer.
  - Cached gateways require at least two disks. One to use as a cache, and one to use as an upload buffer.
- Tape gateways require at least two disks. One to use as a cache, and one to use as an upload buffer.

The following table recommends sizes for local disk storage for your deployed gateway. You can add more local storage later after you set up the gateway, and as your workload demands increase.

Local storage	Description	Gateway type
Upload buffer	The upload buffer provides a staging area for the data before the gateway uploads the data to Amazon S3. Your gateway uploads this buffer data over an encrypted Secure Sockets Layer (SSL) connection to AWS.	<ul style="list-style-type: none"><li>• Cached volumes</li><li>• Stored volumes</li><li>• Tape gateways</li></ul>
Cache storage	The cache storage acts as the on-premises durable store for data that is pending upload to Amazon S3 from the upload buffer. When your application	<ul style="list-style-type: none"><li>• Cached volumes</li><li>• Tape gateways</li><li>• File gateways</li></ul>

Local storage	Description	Gateway type
	performs I/O on a volume or tape, the gateway saves the data to the cache storage for low-latency access. When your application requests data from a volume or tape, the gateway first checks the cache storage for the data before downloading the data from AWS.	

**Note**

When you provision disks, we strongly recommend that you do not provision local disks for the upload buffer and cache storage if they use the same physical resource (the same disk). Underlying physical storage resources are represented as a data store in VMware. When you deploy the gateway VM, you choose a data store on which to store the VM files. When you provision a local disk (for example, to use as cache storage or upload buffer), you have the option to store the virtual disk in the same data store as the VM or a different data store. If you have more than one data store, we strongly recommend that you choose one data store for the cache storage and another for the upload buffer. A data store that is backed by only one underlying physical disk can lead to poor performance in some situations when it is used to back both the cache storage and upload buffer. This is also true if the backup is a less-performant RAID configuration such as RAID1.

After the initial configuration and deployment of your gateway, you can adjust the local storage by adding or removing disks for an upload buffer. You can also add disks for cache storage.

## Determining the size of upload buffer to allocate

You can determine the size of your upload buffer to allocate by using an upload buffer formula. We strongly recommend that you allocate at least 150 GiB of upload buffer. If the formula returns a value less than 150 GiB, use 150 GiB as the amount you allocate to the upload buffer. You can configure up to 2 TiB of upload buffer capacity for each gateway.

**Note**

For volume gateways, when the upload buffer reaches its capacity, your volume goes to PASS THROUGH status. In this status, new data that your application writes is persisted locally but not uploaded to AWS immediately. Thus, you cannot take new snapshots. When the upload buffer capacity frees up, the volume goes through BOOTSTRAPPING status. In this status, any new data that was persisted locally is uploaded to AWS. Finally, the volume returns to ACTIVE status. Storage Gateway then resumes normal synchronization of the data stored locally with the copy stored in AWS, and you can start taking new snapshots. For more information about volume status, see [Understanding Volume Statuses and Transitions \(p. 193\)](#).

For tape gateways, when the upload buffer reaches its capacity, your applications can continue to read from and write data to your storage volumes. However, the tape gateway does not write any of your volume data to its upload buffer and does not upload any of this data to AWS until Storage Gateway synchronizes the data stored locally with the copy of the data stored in AWS. This synchronization occurs when the volumes are in BOOTSTRAPPING status.

To estimate the amount of upload buffer to allocate, you can determine the expected incoming and outgoing data rates and plug them into the following formula.

### Rate of incoming data

This rate refers to the application throughput, the rate at which your on-premises applications write data to your gateway over some period of time.

### Rate of outgoing data

This rate refers to the network throughput, the rate at which your gateway is able to upload data to AWS. This rate depends on your network speed, utilization, and whether you've enabled bandwidth throttling. This rate should be adjusted for compression. When uploading data to AWS, the gateway applies data compression where possible. For example, if your application data is text-only, you might get an effective compression ratio of about 2:1. However, if you are writing videos, the gateway might not be able to achieve any data compression and might require more upload buffer for the gateway.

We strongly recommend that you allocate at least 150 GiB of upload buffer space if either of the following is true:

- Your incoming rate is higher than the outgoing rate.
- The formula returns a value less than 150 GiB.

$$\left( \frac{\text{Application Throughput (MB/s)}}{\text{Network Throughput to AWS (MB/s)}} - \frac{\text{Compression Factor}}{2} \right) \times \frac{\text{Duration of writes (s)}}{3600} = \text{Upload Buffer (MB)}$$

For example, assume that your business applications write text data to your gateway at a rate of 40 MB per second for 12 hours per day and your network throughput is 12 MB per second. Assuming a compression factor of 2:1 for the text data, you would allocate approximately 690 GiB of space for the upload buffer.

#### Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

You can initially use this approximation to determine the disk size that you want to allocate to the gateway as upload buffer space. Add more upload buffer space as needed using the Storage Gateway console. Also, you can use the Amazon CloudWatch operational metrics to monitor upload buffer usage and determine additional storage requirements. For information on metrics and setting the alarms, see [Monitoring the upload buffer \(p. 220\)](#).

## Determining the size of cache storage to allocate

Your gateway uses its cache storage to provide low-latency access to your recently accessed data. The cache storage acts as the on-premises durable store for data that is pending upload to Amazon S3 from the upload buffer. Generally speaking, you size the cache storage at 1.1 times the upload buffer size. For more information about how to estimate your cache storage size, see [Determining the size of upload buffer to allocate \(p. 255\)](#).

You can initially use this approximation to provision disks for the cache storage. You can then use Amazon CloudWatch operational metrics to monitor the cache storage usage and provision more storage as needed using the console. For information on using the metrics and setting up alarms, see [Monitoring cache storage \(p. 222\)](#).

## Adding an upload buffer or cache storage

As your application needs change, you can increase the gateway's upload buffer or cache storage capacity. You can add more buffer capacity to your gateway without interrupting existing gateway functions. When you add more upload buffer capacity, you do so with the gateway VM turned on.

### Important

When adding cache or upload buffer to an existing gateway, it is important to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer. Do not remove cache disks that have been allocated as cache storage.

The following procedure shows you how to configure an upload buffer or cache storage for your gateway.

#### To add and configure upload buffer or cache storage

1. Provision a new disk in your host (hypervisor or Amazon EC2 instance). For information about how to provision a disk in a hypervisor, see your hypervisor's user manual. For information about how to add Amazon EBS volumes for your Amazon EC2 instance, see [Adding and Removing Amazon EBS Volumes for Your Gateway Hosted on Amazon EC2 \(p. 406\)](#). You configure this disk as an upload buffer or cache storage.
2. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
3. In the navigation pane, choose **Gateways**.
4. In the **Actions** menu, choose **Edit local disks**.
5. In the Edit local disks dialog box, identify the disks you provisioned and decide which one you want to use for an upload buffer or cached storage.

#### Note

For stored volumes, only the upload buffer is displayed because stored volumes have no cache disks.

6. In the drop-down list box, in the **Allocated to** column, choose **Upload Buffer** for the disk to use as an upload buffer.
7. For gateways created with cached volumes and tape gateway, choose **Cache** for the disk you want to use as a cache storage.

If you don't see your disks, choose the **Refresh** button.

8. Choose **Save** to save your configuration settings.

## Using ephemeral storage with EC2 gateways

This section describes steps you need to take to prevent data loss when you select an ephemeral disk as storage for your gateway's cache.

Ephemeral disks provide temporary block-level storage for your Amazon EC2 instance. Ephemeral disks are ideal for temporary storage of data that changes frequently, such as data in a gateway's upload buffer or cache storage. When you launch your gateway with an Amazon EC2 Amazon Machine Image, and the instance type you select supports ephemeral storage, the disks are listed automatically and you can select one of the disks to store data in your gateway's cache. For more information, see [Amazon EC2 instance store](#) in the *Amazon EC2 User Guide for Linux Instances*.

Application writes to the disks are stored in the cache synchronously, and asynchronously uploaded to durable storage in Amazon S3. If the data stored in the ephemeral storage is lost because an Amazon EC2 instance stopped before data upload was completed, the data that is still in the cache and has not been uploaded to Amazon S3 can be lost. You can prevent such data loss by following the steps before you restart or stop the EC2 instance that hosts your gateway.

#### Note

If you are using ephemeral storage and you stop and start your gateway, the gateway will be permanently offline. This happens because the physical storage disk is replaced. There is no work around for this issue so you'd have to delete the gateway and activate a new one on a new EC2 instance.

These steps in this following procedure are specific for file gateways.

#### To prevent data loss in file gateways that use ephemeral disks

1. Stop all the processes that are writing to the file share.
2. Subscribe to receive notification from CloudWatch Events. For information, see [Getting notified about file operations \(p. 227\)](#).
3. Call the [NotifyWhenUploaded API](#) to get notified when data that is written, up until the ephemeral storage was lost, has been durably stored in Amazon S3.
4. Wait for the API to complete and you receive a notification id.

You receive a CloudWatch event with the same notification id.

5. Verify that the [CachePercentDirty metric](#) for your file share is 0. This confirms that all your data has been written to Amazon S3. For information about file share metrics, see [Understanding file share metrics \(p. 233\)](#).
6. You can now restart or stop the file gateway without risk of losing any data.

## Managing Bandwidth for Your Gateway

You can limit (or throttle) the upload throughput from the gateway to AWS or the download throughput from your AWS to your gateway. Using bandwidth throttling helps you to control the amount of network bandwidth used by your gateway. By default, an activated gateway has no rate limits on upload or download.

You can specify the rate limit by using the AWS Management Console, or programmatically by using either the Storage Gateway API (see [UpdateBandwidthRateLimit](#)) or an AWS Software Development Kit (SDK). By throttling bandwidth programmatically, you can change limits automatically throughout the day—for example, by scheduling tasks to change the bandwidth.

You can also define schedule-based bandwidth throttling for your gateway. You schedule bandwidth throttling by defining one or more bandwidth rate limit intervals. For more information, see [Schedule-Based Bandwidth Throttling Using the Storage Gateway Console \(p. 259\)](#).

The schedule-based bandwidth throttling function is a superset of the changing bandwidth throttling function. Configuring a single setting for gateway bandwidth throttling is the functional equivalent of defining a schedule with a single bandwidth rate interval set for **Everyday**, with a **Start time** of 00:00 and an **End time** of 23:59.

#### Note

Configuring bandwidth rate limit is currently not supported in the file gateway type.

#### Topics

- [Changing Bandwidth Throttling Using the Storage Gateway Console \(p. 258\)](#)
- [Schedule-Based Bandwidth Throttling Using the Storage Gateway Console \(p. 259\)](#)
- [Updating Gateway Bandwidth Rate Limits Using the AWS SDK for Java \(p. 260\)](#)
- [Updating Gateway Bandwidth Rate Limits Using the AWS SDK for .NET \(p. 261\)](#)
- [Updating Gateway Bandwidth Rate Limits Using the AWS Tools for Windows PowerShell \(p. 262\)](#)

## Changing Bandwidth Throttling Using the Storage Gateway Console

The following procedure shows you how to change a gateway's bandwidth throttling from the Storage Gateway console.

### To change a gateway's bandwidth throttling using the console

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to manage.
3. For **Actions**, choose **Edit Bandwidth Limit**.
4. In the **Edit Rate Limits** dialog box, enter new limit values, and then choose **Save**. Your changes appear in the **Details** tab for your gateway.

## Schedule-Based Bandwidth Throttling Using the Storage Gateway Console

The following procedure shows you how to schedule changes to a gateway's bandwidth throttling using the Storage Gateway console.

### To add or modify a schedule for gateway bandwidth throttling

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway that you want to manage.
3. For **Actions**, choose **Edit bandwidth rate limit schedule**.

The gateway's bandwidth rate limit schedule is displayed in the **Edit bandwidth rate limit schedule** dialog box. By default, a new gateway bandwidth rate limit schedule is empty.

4. In the **Edit bandwidth rate limit schedule** dialog box, choose **Add new entry** to add a new bandwidth rate limit interval. Enter the following information for each bandwidth rate limit interval:
  - **Days of week** – You can create the bandwidth rate limit interval for weekdays (Monday through Friday), for weekends (Saturday and Sunday), for every day of the week, or for one or more specific days of the week.
  - **Start time** – Enter the start time for the bandwidth interval, using the HH:MM format and the timezone offset from GMT for your gateway.

#### Note

Your bandwidth rate limit interval begins at the start of the minute that you specify here.

- **End time** – Enter the end time for the bandwidth interval, using the HH:MM format and the timezone offset from GMT for your gateway.

#### Important

The bandwidth rate limit interval ends at the end of the minute specified here. To schedule an interval that ends at the end of an hour, enter **59**.

To schedule consecutive continuous intervals, transitioning at the start of the hour, with no interruption between the intervals, enter **59** for the end minute of the first interval. Enter **00** for the start minute of the succeeding interval.

- **Download rate** – Enter the download rate limit, in kilobits/second, or select **No limit** to disable bandwidth throttling for downloading. The minimum value for download rate is 100 kilobits/second.
- **Upload rate** – Enter the upload rate limit, in kilobits/second, or select **No limit** to disable bandwidth throttling for uploading. The minimum value for upload rate is 50 kilobits/second.
- To modify bandwidth rate limit intervals, you can enter revised values for the interval parameters.

To remove bandwidth rate limit intervals, you can choose the **cancel** icon ("x") to the right of the interval to be deleted.

---

When changes are complete, choose **Save**.

5. Continue adding bandwidth rate limit intervals by choosing **Add new entry** and entering the day, start and end times, and download and upload rate limits.

**Important**

Bandwidth rate limit intervals cannot overlap. The start time of an interval must occur after the end time of a preceding interval, and before the start time of a following interval.

6. After entering all bandwidth rate limiting intervals, choose **Save** to save your bandwidth rate limit schedule.

When the bandwidth rate limit schedule is successfully updated, you can see the current download and upload rate limits in the **Details** panel for the gateway.

## Updating Gateway Bandwidth Rate Limits Using the AWS SDK for Java

By updating bandwidth rate limits programmatically, you can adjust limits automatically over a period of time—for example, by using scheduled tasks. The following example demonstrates how to update a gateway's bandwidth rate limits using the AWS SDK for Java. To use the example code, you should be familiar with running a Java console application. For more information, see [Getting Started](#) in the *AWS SDK for Java Developer Guide*.

### Example : Updating Gateway Bandwidth Limits Using the AWS SDK for Java

The following Java code example updates a gateway's bandwidth rate limits. You need to update the code and provide the service endpoint, your gateway Amazon Resource Name (ARN), and the upload and download limits. For a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the *AWS General Reference*.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;

public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

    // Rates
    static long uploadRate = 51200; // Bits per second, minimum 51200
    static long downloadRate = 102400; // Bits per second, minimum 102400

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

        // Create a storage gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
            UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);
```

```
        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
        long downloadRate2) {
        try
    {
        UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
            new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

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

## Updating Gateway Bandwidth Rate Limits Using the AWS SDK for .NET

By updating bandwidth rate limits programmatically, you can adjust limits automatically over a period of time—for example, by using scheduled tasks. The following example demonstrates how to update a gateway's bandwidth rate limits by using the AWS SDK for .NET. To use the example code, you should be familiar with running a .NET console application. For more information, see [Getting Started](#) in the [AWS SDK for .NET Developer Guide](#).

### Example : Updating Gateway Bandwidth Limits by Using the AWS SDK for .NET

The following C# code example updates a gateway's bandwidth rate limits. You need to update the code and provide the service endpoint, your gateway Amazon Resource Name (ARN), and the upload and download limits. For a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the [AWS General Reference](#).

```
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());
    }
}
```

## Updating Gateway Bandwidth Rate Limits Using the AWS Tools for Windows PowerShell

By updating bandwidth rate limits programmatically, you can adjust limits automatically over a period of time—for example, by using scheduled tasks. The following example demonstrates how to update a gateway's bandwidth rate limits using the AWS Tools for Windows PowerShell. To use the example code, you should be familiar with running a PowerShell script. For more information, see [Getting Started](#) in the *AWS Tools for Windows PowerShell User Guide*.

### Example : Updating Gateway Bandwidth Limits by Using the AWS Tools for Windows PowerShell

The following PowerShell script example updates a gateway's bandwidth rate limits. You need to update the script and provide your gateway Amazon Resource Name (ARN), and the upload and download limits.

```
<#
.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)
```

## Managing Gateway Updates Using the AWS Storage Gateway Console

Storage Gateway periodically releases important software updates for your gateway. You can manually apply updates on the Storage Gateway Management Console, or wait until the updates are automatically applied during the configured maintenance schedule. Although Storage Gateway checks for updates every minute, it only goes through maintenance and restarts if there are updates.

Gateway software releases regularly include operating system updates and security patches that have been validated by AWS. These updates are typically released every six months, and are applied as part of the normal gateway update process during scheduled maintenance windows.

#### Note

You should treat the Storage Gateway appliance as a managed embedded device, and should not attempt to access or modify its installation in any way. Attempting to install or update any software packages using methods other than the normal gateway update mechanism (for example, SSM or hypervisor tools) may cause the gateway to malfunction.

To modify the email address that software update notifications are sent, go to the [Managing an AWS account](#) page and update the alternate contact for "operations".

Before any update is applied to your gateway, AWS notifies you with a message on the Storage Gateway console and your AWS Personal Health Dashboard. For more information, see [AWS Personal Health](#)

[Dashboard](#). The VM doesn't reboot, but the gateway is unavailable for a short period while it's being updated and restarted.

When you deploy and activate your gateway, a default weekly maintenance schedule is set. You can modify the maintenance schedule at any time. When updates are available, the **Details** tab displays a maintenance message. You can see the date and time that the last successful update was applied to your gateway on the **Details** tab.

**Important**

You can minimize the chance of any disruption to your applications due to the gateway restart by increasing the timeouts of your iSCSI initiator. For more information about increasing iSCSI initiator timeouts for Windows and Linux, see [Customizing Your Windows iSCSI Settings \(p. 424\)](#) and [Customizing Your Linux iSCSI Settings \(p. 428\)](#).

**To modify the maintenance schedule**

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the navigation pane, choose **Gateways**, and choose the gateway that you want to modify the update schedule for.
3. For **Actions**, choose **Edit maintenance window** to open the Edit maintenance start time dialog box.
4. For **Schedule**, choose **Weekly** or **Monthly** to schedule updates.
5. If you choose **Weekly**, modify the values for **Day of the week** and **Time**.

If you choose **Monthly**, modify the values for **Day of the month** and **Time**. If you choose this option and you get an error, it means your gateway is an older version and has not been upgraded to a newer version yet.

**Note**

The maximum value that can be set for day of the month is 28. If 28 is selected, the maintenance start time will be on the 28th day of every month.

Your maintenance start time appears on the **Details** tab for the gateway next time that you open the **Details** tab.

## Performing Maintenance Tasks on the Local Console

You can perform the following maintenance tasks using the host's local console. Local console tasks can be performed on the VM host or the Amazon EC2 instance. Many of the tasks are common among the different hosts, but there are also some differences.

For instructions to access the gateway local console for Tape Gateway on Snowball Edge, see [Troubleshooting and best practices for Tape Gateway on Snowball Edge](#).

**Topics**

- [Performing tasks on the VM local console \(file gateway\) \(p. 265\)](#)
- [Performing tasks on the Amazon EC2 local console \(file gateway\) \(p. 280\)](#)
- [Performing Tasks on the VM Local Console \(Volume and Tape Gateways\) \(p. 287\)](#)
- [Performing Tasks on the Amazon EC2 Local Console \(Volume and Tape Gateways\) \(p. 304\)](#)
- [Accessing the Gateway Local Console \(p. 310\)](#)
- [Configuring Network Adapters for Your Gateway \(p. 315\)](#)

# Performing tasks on the VM local console (file gateway)

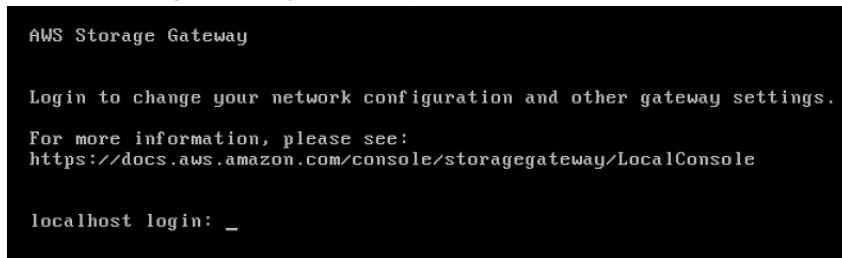
For a file gateway deployed on-premises, you can perform the following maintenance tasks using the VM host's local console. These tasks are common to VMware, Microsoft Hyper-V, and Linux Kernel-based Virtual Machine (KVM) hypervisors.

## Topics

- [Logging in to the file gateway local console \(p. 265\)](#)
- [Configuring an HTTP proxy \(p. 266\)](#)
- [Configuring your gateway network settings \(p. 268\)](#)
- [Testing your gateway connection to the internet \(p. 271\)](#)
- [Viewing your gateway system resource status \(p. 272\)](#)
- [Configuring a Network Time Protocol \(NTP\) server for your gateway \(p. 274\)](#)
- [Running storage gateway commands on the local console \(p. 275\)](#)
- [Configuring network adapters for your gateway \(p. 276\)](#)

## Logging in to the file gateway local console

When the VM is ready for you to log in, the login screen is displayed. If this is your first time logging in to the local console, you use the default user name and password to log in. These default login credentials give you access to menus where you can configure gateway network settings and change the password from the local console. AWS Storage Gateway enables you to set your own password from the Storage Gateway console instead of changing the password from the local console. You don't need to know the default password to set a new password. For more information, see [Setting the Local Console Password from the Storage Gateway Console \(p. 289\)](#).



### To log in to the gateway's local console

- If this is your first time logging in to the local console, log in to the VM with the default credentials. The default user name is `admin` and the password is `password`. Otherwise, use your credentials to log in.

#### Note

We recommend changing the default password. You do this by running the `passwd` command from the local console menu (item 6 on the main menu). For information about how to run the command, see [Running storage gateway commands on the local console \(p. 275\)](#). You can also set the password from the Storage Gateway console. For more information, see [Setting the Local Console Password from the Storage Gateway Console \(p. 289\)](#).

## Setting the local console password from the Storage Gateway console

When you log in to the local console for the first time, you log in to the VM with the default credentials. For all types of gateways, you use default credentials. The user name is `admin` and the password is `password`.

We recommend that you always set a new password immediately after you create your new gateway. You can set this password from the AWS Storage Gateway console rather than the local console if you want. You don't need to know the default password to set a new password.

### To set the local console password on the Storage Gateway console

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. On the navigation pane, choose **Gateways**, and then choose the gateway for which you want to set a new password.
3. For **Actions**, choose **Set Local Console Password**.
4. In the **Set Local Console Password** dialog box, enter a new password, confirm the password, and then choose **Save**.

Your new password replaces the default password. Storage Gateway doesn't save the password but rather safely transmits it to the VM.

#### Note

The password can consist of any character on the keyboard and can be 1–512 characters long.

## Configuring an HTTP proxy

File gateways support configuration of an HTTP proxy.

#### Note

The only proxy configuration that file gateways support is HTTP.

If your gateway must use a proxy server to communicate to the internet, then you need to configure the HTTP proxy settings for your gateway. You do this by specifying an IP address and port number for the host running your proxy. After you do so, Storage Gateway routes all AWS endpoint traffic through your proxy server. Communications between the gateway and endpoints is encrypted, even when using the HTTP proxy. For information about network requirements for your gateway, see [Network and firewall requirements \(p. 13\)](#).

### To configure an HTTP proxy for a file gateway

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - For more information on logging in to the local console for the Linux Kernel-Based Virtual Machine (KVM), see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **1** to begin configuring the HTTP proxy.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

3. On the **HTTP Proxy Configuration menu**, enter **1** and provide the host name for the HTTP proxy server.

```
AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: _
```

You can configure other HTTP settings from this menu as shown following.

To	Do this
Configure an HTTP proxy	Enter <b>1</b> .  You need to supply a host name and port to complete configuration.
View the current HTTP proxy configuration	Enter <b>2</b> .  If an HTTP proxy isn't configured, the message <b>HTTP Proxy not configured</b> is displayed. If an HTTP proxy is configured, the host name and port of the proxy are displayed.
Remove an HTTP proxy configuration	Enter <b>3</b> .  The message <b>HTTP Proxy Configuration Removed</b> is displayed.

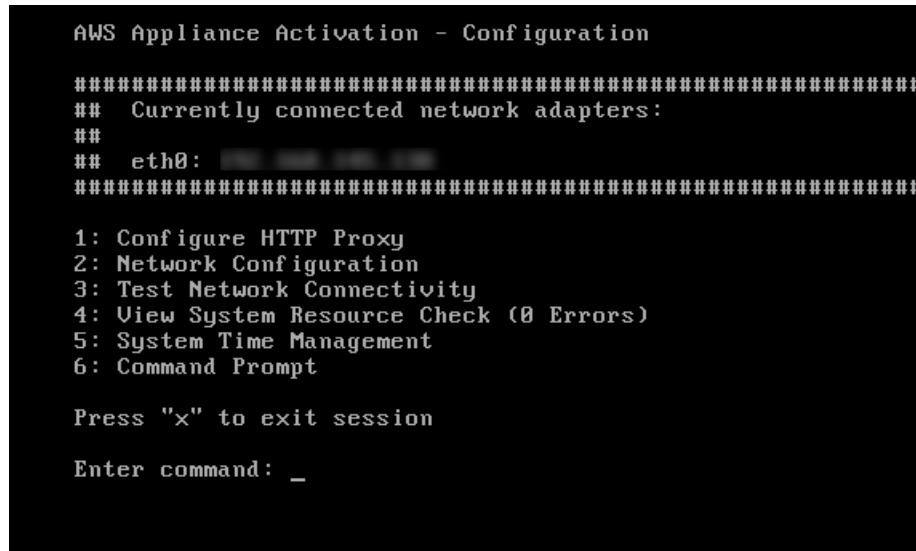
4. Restart your VM to apply your HTTP configuration settings.

## Configuring your gateway network settings

The default network configuration for the gateway is Dynamic Host Configuration Protocol (DHCP). With DHCP, your gateway is automatically assigned an IP address. In some cases, you might need to manually assign your gateway's IP as a static IP address, as described following.

### To configure your gateway to use static IP addresses

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - For more information on logging in to the KVM local console, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **2** to begin configuring your network.



AWS Appliance Activation - Configuration

```
#####
## Currently connected network adapters:
## 
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

3. On the **Network Configuration** menu, choose one of the following options.

```
AWS Appliance Activation - Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: Edit DNS Configuration
7: View DNS Configuration
8: View Routes

Press "x" to exit

Enter command: _
```

To	Do this
Get information about your network adapter	<p>Enter <b>1</b>.</p> <p>A list of adapter names appears, and you are prompted to enter an adapter name—for example, <b>eth0</b>. If the adapter you specify is in use, the following information about the adapter is displayed:</p> <ul style="list-style-type: none"><li>• Media access control (MAC) address</li><li>• IP address</li><li>• Netmask</li><li>• Gateway IP address</li><li>• DHCP enabled status</li></ul> <p>You use the same adapter name when you configure a static IP address (option <b>3</b>) as when you set your gateway's default route adapter (option <b>5</b>).</p>

To	Do this
Configure DHCP	<p>Enter <b>2</b>.</p> <p>You are prompted to configure the network interface to use DHCP.</p> <pre>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: 2  Available adapters: eth0 Enter Network Adapter: eth0  Reset to DHCP [y/n]: y  Adapter eth0 set to use DHCP  You must exit Network Configuration to complete this configuration.  Press Return to Continue...</pre>
Configure a static IP address for your gateway	<p>Enter <b>3</b>.</p> <p>You are prompted to enter the following information to configure a static IP:</p> <ul style="list-style-type: none"> <li>• Network adapter name</li> <li>• IP address</li> <li>• Netmask</li> <li>• Default gateway address</li> <li>• Primary Domain Name Service (DNS) address</li> <li>• Secondary DNS address</li> </ul> <p><b>Important</b>  If your gateway has already been activated, you must shut it down and restart it from the Storage Gateway console for the settings to take effect. For more information, see <a href="#">Shutting Down Your Gateway VM (p. 253)</a>.</p> <p>If your gateway uses more than one network interface, you must set all enabled interfaces to use DHCP or static IP addresses.</p> <p>For example, suppose that your gateway VM uses two interfaces configured as DHCP. If you later set one interface to a static IP, the other interface is disabled. To enable the interface in this case, you must set it to a static IP.</p> <p>If both interfaces are initially set to use static IP addresses and you then set the gateway to use DHCP, both interfaces use DHCP.</p>

To	Do this
Reset all your gateway's network configuration to DHCP	<p>Enter <b>4</b>.</p> <p>All network interfaces are set to use DHCP.</p> <p><b>Important</b> If your gateway has already been activated, you must shut down and restart your gateway from the Storage Gateway console for the settings to take effect. For more information, see <a href="#">Shutting Down Your Gateway VM (p. 253)</a>.</p>
Set your gateway's default route adapter	<p>Enter <b>5</b>.</p> <p>The available adapters for your gateway are shown, and you are prompted to choose one of the adapters—for example, <code>eth0</code>.</p>
Edit your gateway's DNS configuration	<p>Enter <b>6</b>.</p> <p>The available adapters of the primary and secondary DNS servers are displayed. You are prompted to provide the new IP address.</p>
View your gateway's DNS configuration	<p>Enter <b>7</b>.</p> <p>The available adapters of the primary and secondary DNS servers are displayed.</p> <p><b>Note</b> For some versions of the VMware hypervisor, you can edit the adapter configuration in this menu.</p>
View routing tables	<p>Enter <b>8</b>.</p> <p>The default route of your gateway is displayed.</p>

## Testing your gateway connection to the internet

You can use your gateway's local console to test your internet connection. This test can be useful when you are troubleshooting network issues with your gateway.

### To test your gateway's connection to the internet

1. Log in to your gateway's local console:

- For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
- For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
- For more information on logging in to the KVM local console, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).

2. On the **AWS Appliance Activation - Configuration** main menu, enter **3** to begin testing network connectivity.

```
AWS Appliance Activation - Configuration
#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

3. Choose option **1** for Storage Gateway.

4. For **Select endpoint type** type one of the following options:

1. **Public** if you want to test a public endpoint.

2. **VPC (PrivateLink)** if you want to test a VPC endpoint.

- If you selected **Public**, the console displays the available AWS Regions for Storage Gateway.

Choose the AWS Region that you want to test. For example, us-east-2. For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.

Each endpoint in the selected AWS Region displays either a **PASSED** or **FAILED** message, as shown following.

- If you selected **VPC (PrivateLink)**, each VPC endpoint (DNS/IP) in the AWS Region displays either a **PASSED** or **FAILED** message, as shown following.

- 5.

Message	Description
[ PASSED ]	Storage Gateway has internet connectivity.
[ FAILED ]	Storage Gateway doesn't have internet connectivity.

For information about network and firewall requirements, see [Network and firewall requirements \(p. 13\)](#).

## Viewing your gateway system resource status

When your gateway starts, it checks its virtual CPU cores, root volume size, and RAM. It then determines whether these system resources are sufficient for your gateway to function properly. You can view the results of this check on the gateway's local console.

### To view the status of a system resource check

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - For more information on logging in to the KVM local console, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. In the **AWS Appliance Activation - Configuration** main menu, enter **4** to view the results of a system resource check.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

The console displays an **[OK]**, **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
<b>[OK]</b>	The resource has passed the system resource check.
<b>[WARNING]</b>	The resource doesn't meet the recommended requirements, but your gateway can continue to function. Storage Gateway displays a message that describes the results of the resource check.
<b>[FAIL]</b>	The resource doesn't meet the minimum requirements. Your gateway might not function properly. Storage Gateway displays a message that describes the results of the resource check.

The console also displays the number of errors and warnings next to the resource check menu option.

## Configuring a Network Time Protocol (NTP) server for your gateway

You can view and edit Network Time Protocol (NTP) server configurations and synchronize the VM time on your gateway with your hypervisor host.

### To manage system time

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - For more information on logging in to the KVM local console, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. In the **AWS Appliance Activation - Configuration** main menu, enter **5** to manage your system's time.

```
AWS Appliance Activation - Configuration
#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

3. In the **System Time Management** menu, choose one of the following options.

```
System Time Management
1: View and Synchronize System Time
2: Edit NTP Configuration
3: View NTP Configuration

Press "x" to exit
Enter command: _
```

To	Do this
View and synchronize your VM time with NTP server time.	Enter <b>1</b> .

To	Do this
	<p>The current time of your VM is displayed. Your file gateway determines the time difference from your gateway VM, and your NTP server time prompts you to synchronize the VM time with NTP time.</p> <p>After your gateway is deployed and running, in some scenarios the gateway VM's time can drift. For example, suppose that there is a prolonged network outage and your hypervisor host and gateway don't get time updates. In this case, the gateway VM's time is different from the true time. When there is a time drift, a discrepancy occurs between the stated times when operations such as snapshots occur and the actual times that the operations occur.</p> <p>For a gateway deployed on VMware ESXi, setting the hypervisor host time and synchronizing the VM time to the host is sufficient to avoid time drift. For more information, see <a href="#">Synchronizing VM Time with Host Time (p. 392)</a>.</p> <p>For a gateway deployed on Microsoft Hyper-V, you should periodically check your VM's time. For more information, see <a href="#">Synchronizing Your Gateway VM Time (p. 397)</a>.</p> <p>For a gateway deployed on KVM, you can check and synchronize the VM time using <code>virsh</code> command line interface for KVM.</p>
Edit your NTP server configuration	<p>Enter <b>2</b>.</p> <p>You are prompted to provide a preferred and a secondary NTP server.</p>
View your NTP server configuration	<p>Enter <b>3</b>.</p> <p>Your NTP server configuration is displayed.</p>

## Running storage gateway commands on the local console

The VM local console in Storage Gateway helps provide a secure environment for configuring and diagnosing issues with your gateway. Using the local console commands, you can perform maintenance tasks such as saving routing tables, connecting to AWS Support, and so on.

### To run a configuration or diagnostic command

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).

- For more information on logging in to the KVM local console, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **6** for **Command Prompt**.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

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

Press "x" to exit session

Enter command: _
```

3. On the **AWS Appliance Activation - Command Prompt** console, enter **h**, and then press the **Return** key.

The console displays the **AVAILABLE COMMANDS** menu with what the commands do, as shown in the following screenshot.

```
AVAILABLE COMMANDS
ip Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig View or configure network interfaces
iptables Administration tool for IPv4 packet filtering and NAT
save-iptables Persist IP tables
passwd Update authentication tokens
open-support-channel Connect to AWS Support
h Display available command list
exit Return to Configuration menu

Command: _
```

4. At the command prompt, enter the command that you want to use and follow the instructions.

To learn about a command, enter the command name at the command prompt.

## Configuring network adapters for your gateway

By default, Storage Gateway is configured to use the E1000 network adapter type, but you can reconfigure your gateway to use the VMXNET3 (10 GbE) network adapter. You can also configure Storage Gateway so it can be accessed by more than one IP address. You do this by configuring your gateway to use more than one network adapter.

### Topics

- [Configuring your gateway to use the VMXNET3 network adapter \(p. 277\)](#)
- [Configuring your gateway for multiple NICs \(p. 279\)](#)

## Configuring your gateway to use the VMXNET3 network adapter

Storage Gateway supports the E1000 network adapter type in both VMware ESXi and Microsoft Hyper-V hypervisor hosts. However, the VMXNET3 (10 GbE) network adapter type is supported in VMware ESXi hypervisor only. If your gateway is hosted on a VMware ESXi hypervisor, you can reconfigure your gateway to use the VMXNET3 (10 GbE) adapter enter. For more information on this adapter, see the [VMware website](#).

For KVM hypervisor hosts, Storage Gateway supports the use of `virtio` network device drivers. Use of the E1000 network adapter type for KVM hosts isn't supported.

**Important**

To select VMXNET3, your guest operating system enter must be **Other Linux64**.

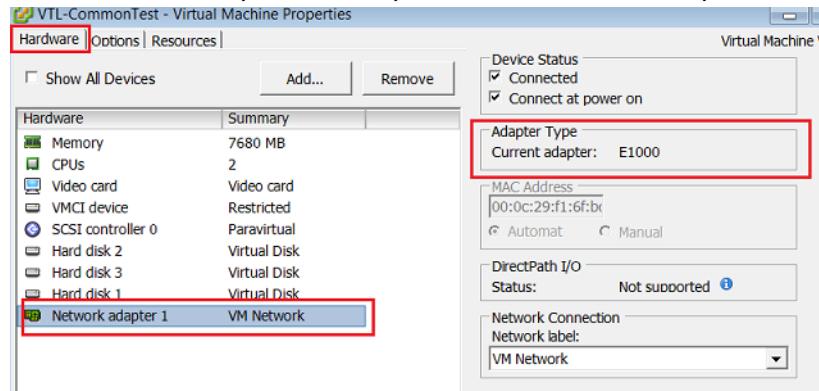
Following are the steps you take to configure your gateway to use the VMXNET3 adapter:

1. Remove the default E1000 adapter.
2. Add the VMXNET3 adapter.
3. Restart your gateway.
4. Configure the adapter for the network.

Details on how to perform each step follow.

### To remove the default E1000 adapter and configure your gateway to use the VMXNET3 adapter

1. In VMware, open the context (right-click) menu for your gateway and choose **Edit Settings**.
2. In the **Virtual Machine Properties** window, choose the **Hardware** tab.
3. For **Hardware**, choose **Network adapter**. Notice that the current adapter is E1000 in the **Adapter Enter** section. You replace this adapter with the VMXNET3 adapter.



4. Choose the E1000 network adapter, and then choose **Remove**. In this example, the E1000 network adapter is **Network adapter 1**.

**Note**

Although you can run the E1000 and VMXNET3 network adapters in your gateway at the same time, we don't recommend doing so because it can cause network problems.

5. Choose **Add** to open the Add Hardware wizard.
6. Choose **Ethernet Adapter**, and then choose **Next**.
7. In the Network Enter wizard, select **VMXNET3** for **Adapter Enter**, and then choose **Next**.
8. In the Virtual Machine properties wizard, verify in the **Adapter Enter** section that **Current Adapter** is set to **VMXNET3**, and then choose **OK**.

9. In the VMware VSphere client, shut down your gateway.
10. In the VMware VSphere client, restart your gateway.

After your gateway restarts, reconfigure the adapter you just added to make sure that network connectivity to the internet is established.

### To configure the adapter for the network

1. In the VSphere client, choose the **Console** tab to start the local console. Use the default login credentials to log in to the gateway's local console for this configuration task. For information about how to log in using the default credentials, see [Logging in to the file gateway local console \(p. 265\)](#).



The screenshot shows two terminal windows from the AWS Storage Gateway Local Console. The top window displays a login prompt:

```
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: _
```

The bottom window shows the "AWS Appliance Activation - Configuration" menu:

```
AWS Appliance Activation - Configuration
#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####
1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _
```

2. At the prompt, enter **2** to select **Network Configuration**, and then press **Enter** to open the network configuration menu.
3. At the prompt, enter **4** to select **Reset all to DHCP**, and then enter **y** (for yes) at the prompt to set all adapters to use Dynamic Host Configuration Protocol (DHCP). All available adapters are set to use DHCP.

```
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: 2

Available adapters: eth0
Enter Network Adapter: eth0

Reset to DHCP [y/n]: y

Adapter eth0 set to use DHCP

You must exit Network Configuration to complete this configuration.

Press Return to Continue_
```

If your gateway is already activated, you must shut it down and restart it from the Storage Gateway Management Console. After the gateway restarts, you must test network connectivity to the internet. For information about how to test network connectivity, see [Testing your gateway connection to the internet \(p. 271\)](#).

## Configuring your gateway for multiple NICs

If you configure your gateway to use multiple network adapters (NICs), it can be accessed by more than one IP address. You might want to do this in the following situations:

- **Maximizing throughput** – You might want to maximize throughput to a gateway when network adapters are a bottleneck.
- **Application separation** – You might need to separate how your applications write to a gateway's volumes. For example, you might choose to have a critical storage application exclusively use one particular adapter defined for your gateway.
- **Network constraints** – Your application environment might require that you keep your iSCSI targets and the initiators that connect to them in an isolated network. This network is different from the network by which the gateway communicates with AWS.

In a typical multiple-adapter use case, one adapter is configured as the route by which the gateway communicates with AWS (that is, as the default gateway). Except for this one adapter, initiators must be in the same subnet as the adapter that contains the iSCSI targets to which they connect. Otherwise, communication with the intended targets might not be possible. If a target is configured on the same adapter that is used for communication with AWS, then iSCSI traffic for that target and AWS traffic flows through the same adapter.

In some cases, you might configure one adapter to connect to the Storage Gateway console and then add a second adapter. In such a case, Storage Gateway automatically configures the route table to use the second adapter as the preferred route. For instructions on how to configure multiple adapters, see the following sections:

- [Configuring Your Gateway for Multiple NICs in a VMware ESXi Host \(p. 315\)](#)
- [Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host \(p. 317\)](#)

# Performing tasks on the Amazon EC2 local console (file gateway)

Some maintenance tasks require that you log in to the local console when running a gateway deployed on an Amazon EC2 instance. In this section, you can find information about how to log in to the local console and perform maintenance tasks.

## Topics

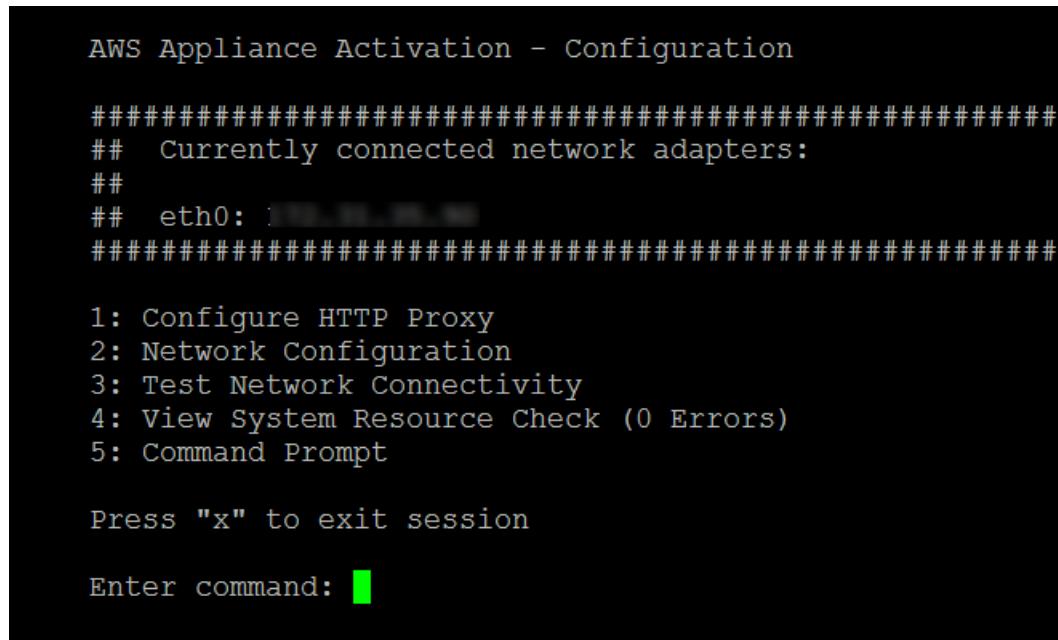
- [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#)
- [Routing your gateway deployed on EC2 through an HTTP proxy \(p. 281\)](#)
- [Configuring your gateway network settings \(p. 283\)](#)
- [Testing your gateway connectivity to the internet \(p. 284\)](#)
- [Viewing your gateway system resource status \(p. 285\)](#)
- [Running Storage Gateway commands on the local console \(p. 286\)](#)

## Logging in to your Amazon EC2 gateway local console

You can connect to your Amazon EC2 instance by using a Secure Shell (SSH) client. For detailed information, see [Connect to your instance](#) in the *Amazon EC2 User Guide*. To connect this way, you need the SSH key pair that you specified when you launched your instance. For information about Amazon EC2 key pairs, see [Amazon EC2 key pairs](#) in the *Amazon EC2 User Guide*.

### To log in to the gateway local console

1. Log in to your local console. If you are connecting to your EC2 instance from a Windows computer, log in as *admin*.
2. After you log in, you see the **AWS Appliance Activation - Configuration** main menu, as shown in the following screenshot.



The screenshot shows a terminal window with the following text:

```
AWS Appliance Activation - Configuration

#####
##  Currently connected network adapters:
##
##  eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

To Learn About This	See This Topic
Configure an HTTP proxy for your gateway	<a href="#">Routing your gateway deployed on EC2 through an HTTP proxy (p. 281)</a>
Configure network settings for your gateway	<a href="#">Testing your gateway connectivity to the internet (p. 284)</a>
Test network connectivity	<a href="#">Testing your gateway connectivity to the internet (p. 284)</a>
View a system resource check	<a href="#">Logging in to your Amazon EC2 gateway local console (p. 280)</a> .
Run Storage Gateway console commands	<a href="#">Running Storage Gateway commands on the local console (p. 286)</a>

To shut down the gateway, enter **0**.

To exit the configuration session, enter **x** to exit the menu.

## Routing your gateway deployed on EC2 through an HTTP proxy

Storage Gateway supports the configuration of a Socket Secure version 5 (SOCKS5) proxy between your gateway deployed on Amazon EC2 and AWS.

If your gateway must use a proxy server to communicate to the internet, then you need to configure the HTTP proxy settings for your gateway. You do this by specifying an IP address and port number for the host running your proxy. After you do so, Storage Gateway routes all AWS endpoint traffic through your proxy server. Communications between the gateway and endpoints is encrypted, even when using the HTTP proxy.

### To route your gateway internet traffic through a local proxy server

1. Log in to your gateway's local console. For instructions, see [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **1** to begin configuring the HTTP proxy.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

3. Choose one of the following options in the **AWS Appliance Activation - Configuration HTTP Proxy Configuration** menu.

```
AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: █
```

To	Do This
Configure an HTTP proxy	Enter 1.  You need to supply a host name and port to complete configuration.
View the current HTTP proxy configuration	Enter 2.  If an HTTP proxy is not configured, the message <code>HTTP Proxy not configured</code> is displayed. If an HTTP proxy is configured, the host name and port of the proxy are displayed.
Remove an HTTP proxy configuration	Enter 3.

To	Do This
	The message <b>HTTP Proxy Configuration Removed</b> is displayed.

## Configuring your gateway network settings

You can view and configure your Domain Name Server (DNS) settings through the local console.

### To configure your gateway to use static IP addresses

1. Log in to your gateway's local console. For instructions, see [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **2** to begin configuring your DNS server.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

3. On the **Network Configuration** menu, choose one of the following options.

```
AWS Appliance Activation - Network Configuration

1: Edit DNS Configuration
2: View DNS Configuration

Press "x" to exit

Enter command: █
```

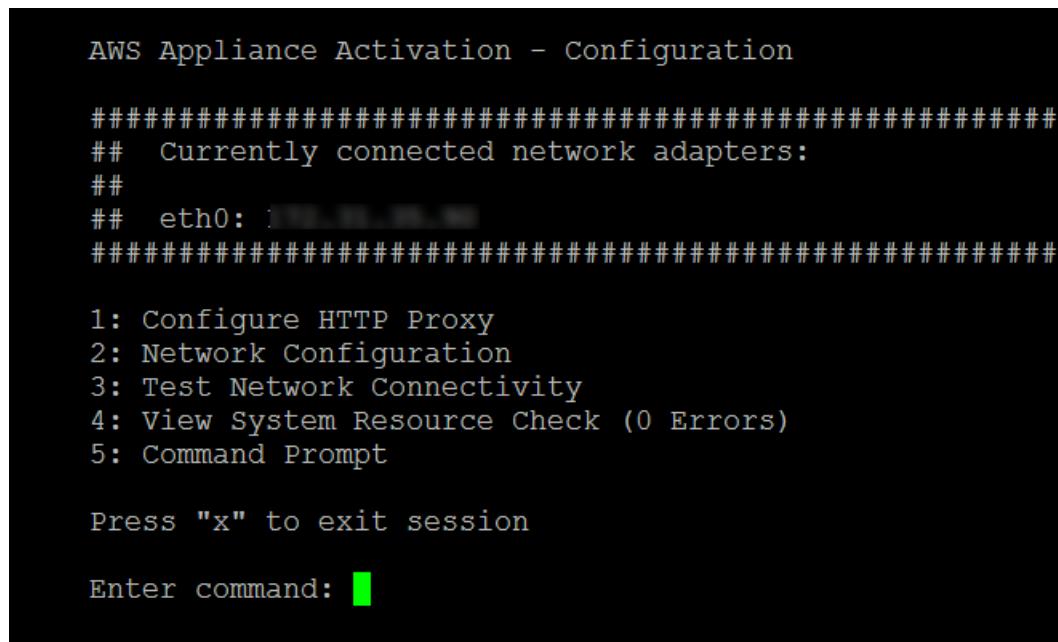
To	Do This
Edit your gateway's DNS configuration	Enter <b>1</b> .  The available adapters of the primary and secondary DNS servers are displayed. You are prompted to provide the new IP address.
View your gateway's DNS configuration	Enter <b>2</b> .  The available adapters of the primary and secondary DNS servers are displayed.

## Testing your gateway connectivity to the internet

You can use your gateway's local console to test your internet connection. This test can be useful when you are troubleshooting network issues with your gateway.

### To test your gateway's connection to the internet

1. Log in to your gateway's local console. For instructions, see [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#).
2. In the **Storage Gateway Configuration** main menu, enter **3** to begin testing network connectivity.



The screenshot shows a terminal window titled "AWS Appliance Activation - Configuration". It displays a menu with the following options:

```
#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

The console displays the available AWS Regions.

3. Choose option **1** for Storage Gateway.



The screenshot shows a terminal window with the following text:

```
Testing network connection

Select gateway family:
 1: Storage Gateway
 2: EFS File Sync

Press "x" to exit

Please select a gateway family or exit: _
```

The console displays the available AWS Regions for Storage Gateway.

4. Choose the AWS Region that you want to test. For example, us-east-2. For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway endpoints and quotas](#) in the *AWS General Reference*.

Each endpoint in the AWS Region that you choose displays either a **[PASSED]** or **[FAILED]** message, as shown following.

Message	Description
<b>[PASSED]</b>	Storage Gateway has internet connectivity.
<b>[FAILED]</b>	Storage Gateway does not have internet connectivity.

## Viewing your gateway system resource status

When your gateway starts, it checks its virtual CPU cores, root volume size, and RAM. It then determines whether these system resources are sufficient for your gateway to function properly. You can view the results of this check on the gateway's local console.

### To view the status of a system resource check

1. Log in to your gateway's local console. For instructions, see [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#).
2. In the **Storage Gateway Configuration** main menu, enter **4** to view the results of a system resource check.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

The console displays an **[OK]**, **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
<b>[OK]</b>	The resource has passed the system resource check.
<b>[WARNING]</b>	The resource doesn't meet the recommended requirements, but your gateway can continue to function. Storage Gateway displays a message that describes the results of the resource check.
<b>[FAIL]</b>	The resource doesn't meet the minimum requirements. Your gateway might not function properly. Storage Gateway displays a message that describes the results of the resource check.

The console also displays the number of errors and warnings next to the resource check menu option.

## Running Storage Gateway commands on the local console

The AWS Storage Gateway console helps provide a secure environment for configuring and diagnosing issues with your gateway. Using the console commands, you can perform maintenance tasks such as saving routing tables or connecting to AWS Support.

### To run a configuration or diagnostic command

1. Log in to your gateway's local console. For instructions, see [Logging in to your Amazon EC2 gateway local console \(p. 280\)](#).
2. In the **AWS Appliance Activation Configuration** main menu, enter **5** for **Gateway Console**.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

3. In the command prompt, enter **h**, and then press the **Return** key.

The console displays the **AVAILABLE COMMANDS** menu with the available commands. After the menu, a gateway console prompt appears, as shown in the following screenshot.

```
AVAILABLE COMMANDS
ip                      Show / manipulate routing, devices, and tunnels
save-routing-table      Save newly added routing table entry
ifconfig                View or configure network interfaces
iptables               Administration tool for IPv4 packet filtering and
save-iptables          Persist IP tables
open-support-channel   Connect to AWS Support
h                      Display available command list
exit                   Return to Configuration menu

Command: █
```

4. At the command prompt, enter the command that you want to use and follow the instructions.

To learn about a command, enter the command name at the command prompt.

## Performing Tasks on the VM Local Console (Volume and Tape Gateways)

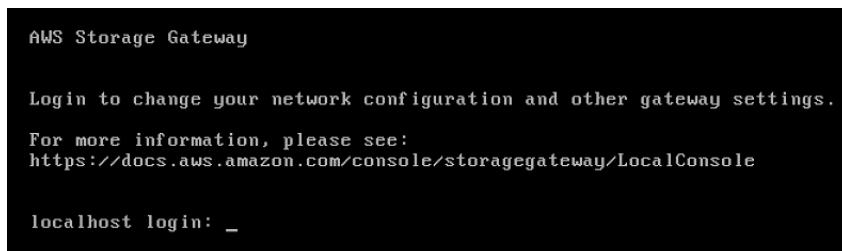
For a gateway deployed on-premises, you can perform the following maintenance tasks using the VM host's local console. These tasks are common to VMware, Hyper-V, and Linux Kernel-based Virtual Machine (KVM) hosts.

## Topics

- [Logging in to the Local Console Using Default Credentials \(p. 288\)](#)
- [Setting the Local Console Password from the Storage Gateway Console \(p. 289\)](#)
- [Routing Your On-Premises Gateway Through a Proxy \(p. 290\)](#)
- [Configuring Your Gateway Network \(p. 293\)](#)
- [Testing Your Gateway Connection to the Internet \(p. 296\)](#)
- [Synchronizing Your Gateway VM Time \(p. 297\)](#)
- [Running Storage Gateway Commands on the Local Console \(p. 298\)](#)
- [Viewing Your Gateway System Resource Status \(p. 299\)](#)
- [Configuring Network Adapters for Your Gateway \(p. 300\)](#)

## Logging in to the Local Console Using Default Credentials

When the VM is ready for you to log in, the login screen is displayed. If this is your first time logging in to the local console, you use the default user name and password to log in. These default login credentials give you access to menus where you can configure gateway network settings and change the password from the local console. Storage Gateway enables you to set your own password from the AWS Storage Gateway console instead of changing the password from the local console. You don't need to know the default password to set a new password. For more information, see [Setting the Local Console Password from the Storage Gateway Console \(p. 289\)](#).



### To log in to the gateway's local console

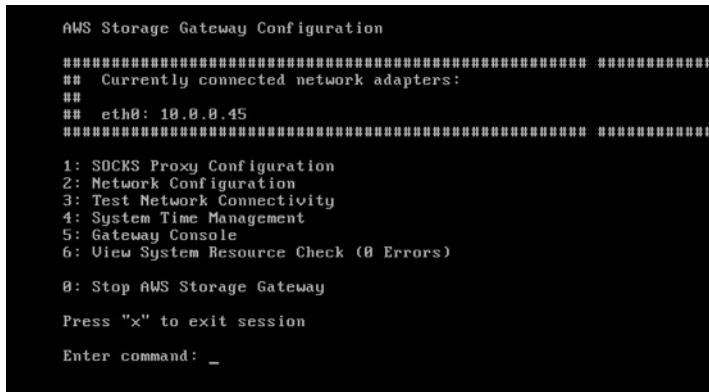
- If this is your first time logging in to the local console, log in to the VM with the default credentials. The default user name is `admin` and the password is `password`.

Otherwise, use your credentials to log in.

#### Note

If your volume or tape gateway has not been updated to a newer version yet, the user name is `sguser` and the password is `sgpassword`. If you reset your password and your gateway is updated to a newer version, your the user name will change to `admin` but the password will be maintained.

After you log in, you see the **Storage Gateway Configuration** main menu, as shown in the following screenshot.



```
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: _
```

### Note

We recommend changing the default password. You do this by running the `passwd` command from the local console menu (item 5 on the main menu). For information about how to run the command, see [Running Storage Gateway Commands on the Local Console \(p. 298\)](#). You can also set your own password from the AWS Storage Gateway console. For more information, see [Setting the Local Console Password from the Storage Gateway Console \(p. 289\)](#).

To	See
Configure a SOCKS proxy for your gateway	<a href="#">Routing Your On-Premises Gateway Through a Proxy (p. 290)</a> .
Configure your network	<a href="#">Configuring Your Gateway Network (p. 293)</a> .
Test network connectivity	<a href="#">Testing Your Gateway Connection to the Internet (p. 296)</a> .
Manage VM time	<a href="#">Synchronizing Your Gateway VM Time (p. 297)</a> .
Run Storage Gateway console commands	<a href="#">Running Storage Gateway Commands on the Local Console (p. 298)</a> .
View system resource check	<a href="#">Viewing Your Gateway System Resource Status (p. 299)</a> .

To shut down the gateway, type **0**.

To exit the configuration session, type **x** to exit the menu.

## Setting the Local Console Password from the Storage Gateway Console

When you log in to the local console for the first time, you log in to the VM with the default credentials — The user name is `admin` and the password is `password`. We recommend that you always set a new password immediately after you create your new gateway. You can set this password from the AWS Storage Gateway console rather than the local console if you want. You don't need to know the default password to set a new password.

### To set the local console password on the Storage Gateway console

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.

2. On the navigation pane, choose **Gateways** then choose the gateway for which you want to set a new password.
3. For **Actions**, choose **Set Local Console Password**.
4. In the **Set Local Console Password** dialog box, type a new password, confirm the password and then choose **Save**. Your new password replaces the default password. Storage Gateway does not save the password but rather safely transmits it to the VM.

**Note**

The password can consist of any character on the keyboard and can be 1 to 512 characters long.

## Routing Your On-Premises Gateway Through a Proxy

Volume gateways and tape gateways support configuration of a Socket Secure version 5 (SOCKS5) proxy between your on-premises gateway and AWS. File gateways support configuration of an HyperText Transfer Protocol (HTTP) proxy.

**Note**

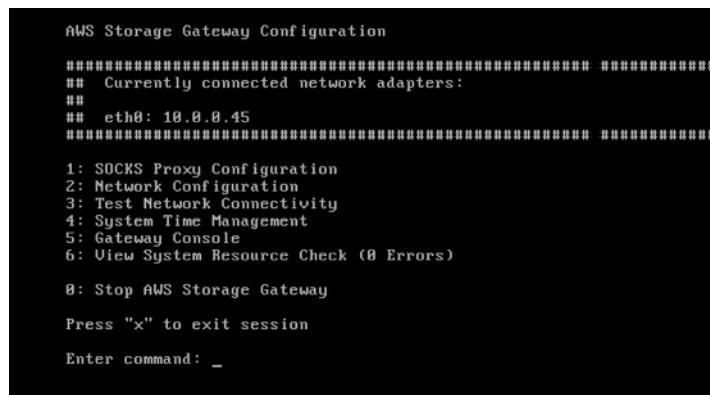
The only proxy configurations Storage Gateway supports are SOCKS5 and HTTP.

If your gateway must use a proxy server to communicate to the internet, then you need to configure the SOCKS or HTTP proxy settings for your gateway. You do this by specifying an IP address and port number for the host running your proxy. After you do so, Storage Gateway routes all HTTP traffic through your proxy server. For information about network requirements for your gateway, see [Network and firewall requirements \(p. 13\)](#).

The following procedure shows you how to configure SOCKS proxy for volume gateway and tape gateway. For instructions on how to configure HTTP proxy for file gateway, see [To configure an HTTP proxy for a file gateway \(p. 291\)](#).

### To configure a SOCKS5 proxy for volume and tape gateways

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, type 1 to begin configuring the SOCKS proxy.



AWS Storage Gateway Configuration  
#####  
## Currently connected network adapters:  
##  
## eth0: 10.0.8.45  
#####  
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. Choose one of the following options on the **Storage Gateway SOCKS Proxy Configuration** menu.

```
AWS Storage Gateway SOCKS Proxy Configuration
1: Configure SOCKS Proxy
2: View Current SOCKS Proxy Configuration
3: Remove SOCKS Proxy Configuration

Press "x" to exit

Enter command: _
```

To	Do This
Configure a SOCKS proxy	Type option <b>1</b> .  You will need to supply a host name and port to complete configuration.
View the current SOCKS proxy configuration	Type option <b>2</b> .  If a SOCKS proxy is not configured, the message <code>SOCKS Proxy not configured</code> is displayed. If a SOCKS proxy is configured, the host name and port of the proxy are displayed.
Remove a SOCKS proxy configuration	Type option <b>3</b> .  The message <code>SOCKS Proxy Configuration Removed</code> is displayed.

The following procedure shows you how to configure an HTTP proxy for a file gateway. For instructions on how to configure SOCKS proxy for a volume gateway or tape gateway, see [To configure a SOCKS5 proxy for volume and tape gateways \(p. 290\)](#).

### To configure an HTTP proxy for a file gateway

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, type **1** to begin configuring the HTTP proxy.

```
AWS Storage Gateway Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.0.252
#####

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

Press "x" to exit session

Enter command: █
```

3. Choose one of the following options on the **Storage Gateway HTTP Proxy Configuration** menu:

```
AWS Storage Gateway HTTP Proxy Configuration

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: █
```

To	Do This
Configure a HTTP proxy	Type option 1.  You will need to supply a host name and port to complete configuration.
View the current HTTP proxy configuration	Type option 2.  If a HTTP proxy is not configured, the message <b>HTTP Proxy not configured</b> is displayed. If a HTTP proxy is configured, the host name and port of the proxy are displayed.
Remove a HTTP proxy configuration	Type option 3.  The message <b>HTTP Proxy Configuration Removed</b> is displayed.

4. Restart your VM to apply your HTTP configuration.

## Configuring Your Gateway Network

The default network configuration for the gateway is Dynamic Host Configuration Protocol (DHCP). With DHCP, your gateway is automatically assigned an IP address. In some cases, you might need to manually assign your gateway's IP as a static IP address, as described following.

### To configure your gateway to use static IP addresses

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, type option **2** to begin configuring a static IP address.

```
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)

8: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. Choose one of the following options on the **Storage Gateway Network Configuration** menu:

```
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: _
```

To	Do This
Describe network adapter	<p>Type option <b>1</b>.</p> <p>A list of adapter names appears, and you are prompted to type an adapter name—for example, <b>eth0</b>. If the adapter you specify is in use, the following information about the adapter is displayed:</p> <ul style="list-style-type: none"><li>• Media access control (MAC) address</li></ul>

To	Do This
	<ul style="list-style-type: none"><li>• IP address</li><li>• Netmask</li><li>• Gateway IP address</li><li>• DHCP enabled status</li></ul> <p>You use the same adapter name when you configure a static IP address (option 3) as when you set your gateway's default route adapter (option 5).</p>
Configure DHCP	<p>Type option 2.</p> <p>You are prompted to configure network interface to use DHCP.</p> <div style="background-color: black; color: white; padding: 10px;"><pre>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: 2  Available adapters: eth0 Enter Network Adapter: eth0  Reset to DHCP [y/n]: y Adapter eth0 set to use DHCP  You must exit Network Configuration to complete this configuration.  Press Return to Continue...</pre></div>

To	Do This
Configure a static IP address for your gateway	<p>Type option <b>3</b>.</p> <p>You are prompted to type the following information to configure a static IP:</p> <ul style="list-style-type: none"><li>• Network adapter name</li><li>• IP address</li><li>• Netmask</li><li>• Default gateway address</li><li>• Primary Domain Name Service (DNS) address</li><li>• Secondary DNS address</li></ul> <p><b>Important</b> If your gateway has already been activated, you must shut it down and restart it from the Storage Gateway console for the settings to take effect. For more information, see <a href="#">Shutting Down Your Gateway VM (p. 253)</a>.</p> <p>If your gateway uses more than one network interface, you must set all enabled interfaces to use DHCP or static IP addresses.</p> <p>For example, suppose your gateway VM uses two interfaces configured as DHCP. If you later set one interface to a static IP, the other interface is disabled. To enable the interface in this case, you must set it to a static IP.</p> <p>If both interfaces are initially set to use static IP addresses and you then set the gateway to use DHCP, both interfaces will use DHCP.</p>

To	Do This
Reset all your gateway's network configuration to DHCP	<p>Type option 4.</p> <pre>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: 4  All adapters will be reset to use DHCP. Continue [y/n]: y Adapter eth0 set to use DHCP You must exit Network Configuration to complete this configuration.  Press Return to Continue_</pre> <p>All network interfaces are set to use DHCP.</p> <p><b>Important</b>  If your gateway has already been activated, you must shut down and restart your gateway from the Storage Gateway console for the settings to take effect. For more information, see <a href="#">Shutting Down Your Gateway VM (p. 253)</a>.</p>
Set your gateway's default route adapter	<p>Type option 5.</p> <p>The available adapters for your gateway are shown, and you are prompted to select one of the adapters—for example, <b>eth0</b>.</p>
View your gateway's DNS configuration	<p>Type option 6.</p> <p>The IP addresses of the primary and secondary DNS name servers are displayed.</p>
View routing tables	<p>Type option 7.</p> <p>The default route of your gateway is displayed.</p>

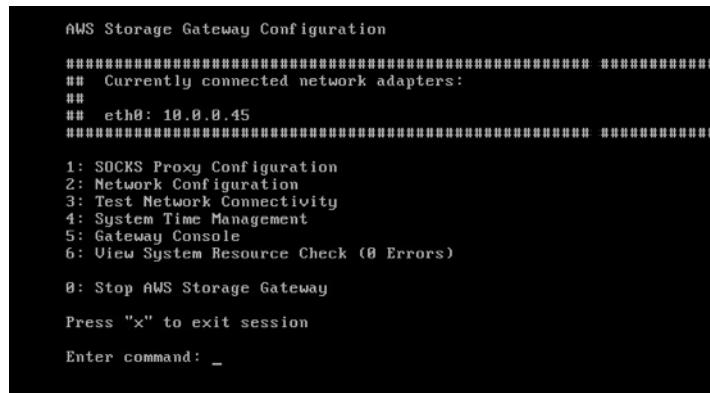
## Testing Your Gateway Connection to the Internet

You can use your gateway's local console to test your internet connection. This test can be useful when you are troubleshooting network issues with your gateway.

### To test your gateway's connection to the internet

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).

- Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, type option **3** to begin testing network connectivity.



The screenshot shows a terminal window titled "AWS Storage Gateway Configuration". It displays a menu with the following options:

- ## 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 (8 Errors)
- 0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: \_

The console displays the available regions.

3. Select the region you want to test. For example, us-east-2. For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas in the AWS General Reference](#).

Each endpoint in the selected region displays either a PASSED or FAILED message, as shown following.

Message	Description
[ PASSED ]	Storage Gateway has internet connectivity.
[ FAILED ]	Storage Gateway does not have internet connectivity.

For information about network and firewall requirements, see [Network and firewall requirements \(p. 13\)](#).

## Synchronizing Your Gateway VM Time

After your gateway is deployed and running, in some scenarios the gateway VM's time can drift. For example, if there is a prolonged network outage and your hypervisor host and gateway do not get time updates, then the gateway VM's time will be different from the true time. When there is a time drift, a discrepancy occurs between the stated times when operations such as snapshots occur and the actual times that the operations occur.

For a gateway deployed on VMware ESXi, setting the hypervisor host time and synchronizing the VM time to the host is sufficient to avoid time drift. For more information, see [Synchronizing VM Time with Host Time \(p. 392\)](#).

For a gateway deployed on Microsoft Hyper-V, you should periodically check your VM's time. For more information, see [Synchronizing Your Gateway VM Time \(p. 397\)](#).

## Running Storage Gateway Commands on the Local Console

The AWS Storage Gateway console helps provide a secure environment for configuring and diagnosing issues with your gateway. Using the console commands, you can perform maintenance tasks such as saving routing tables or connecting to AWS Support.

### To run a configuration or diagnostic command

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, type option **5** for **Gateway Console**.

```
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 (8 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

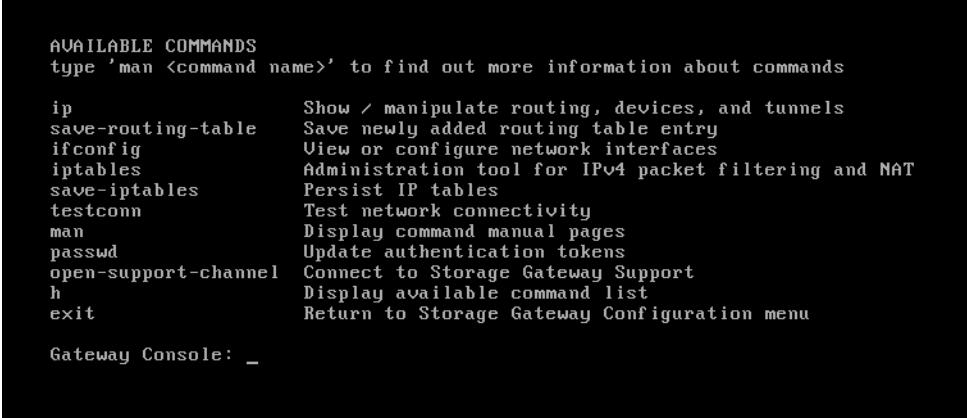
3. On the AWS Storage Gateway console, type **h**, and then press the **Return** key.

```

type 'h <ENTER>' to get help

Gateway Console: _
```

The console displays the **Available Commands** menu with the available commands and after the menu a **Gateway Console** prompt, as shown in the following screenshot.



```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands

ip Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig View or configure network interfaces
iptables Administration tool for IPv4 packet filtering and NAT
save-iptables Persist IP tables
testconn Test network connectivity
man Display command manual pages
passwd Update authentication tokens
open-support-channel Connect to Storage Gateway Support
h Display available command list
exit Return to Storage Gateway Configuration menu

Gateway Console: _
```

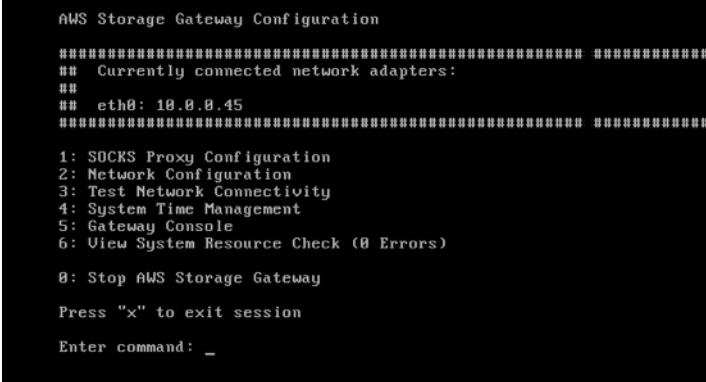
4. To learn about a command, type **man** + **command name** at the **Gateway Console** prompt.

## Viewing Your Gateway System Resource Status

When your gateway starts, it checks its virtual CPU cores, root volume size, and RAM and determines whether these system resources are sufficient for your gateway to function properly. You can view the results of this check on the gateway's local console.

### To view the status of a system resource check

1. Log in to your gateway's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - Linux KVM – for more information, see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. In the **Storage Gateway Configuration** main menu, type **6** to view the results of a system resource check.



```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.8.8.45
#####

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

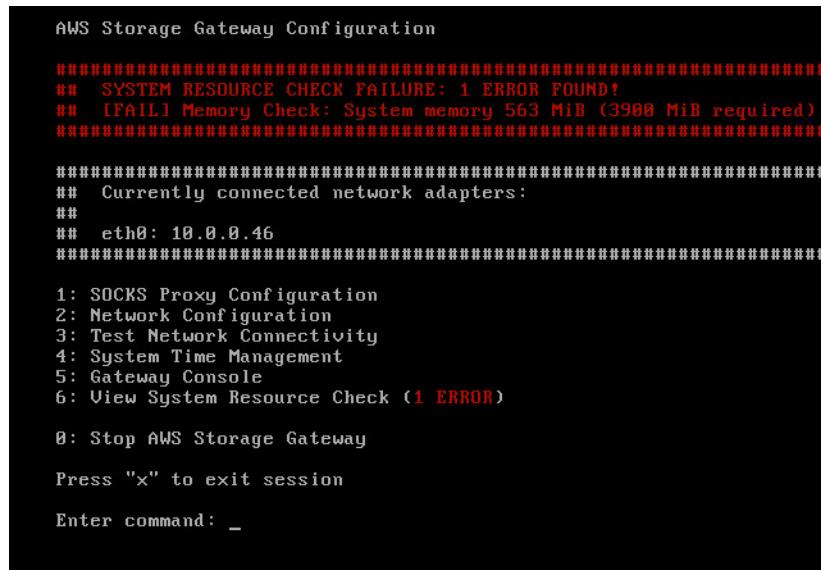
Enter command: _
```

The console displays an **[OK]**, **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
[OK]	The resource has passed the system resource check.
[WARNING]	The resource does not meet the recommended requirements, but your gateway will continue to function. Storage Gateway displays a message that describes the results of the resource check.
[FAIL]	The resource does not meet the minimum requirements. Your gateway might not function properly. Storage Gateway displays a message that describes the results of the resource check.

The console also displays the number of errors and warnings next to the resource check menu option.

The following screenshot shows a [FAIL] message and the accompanying error message.



AWS Storage Gateway Configuration

```
#####
## SYSTEM RESOURCE CHECK FAILURE: 1 ERROR FOUND!
## [FAIL] Memory Check: System memory 563 MiB (3900 MiB required)
#####

#####
## Currently connected network adapters:
##
## eth0: 10.0.0.46
#####

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

## Configuring Network Adapters for Your Gateway

By default, Storage Gateway is configured to use the E1000 network adapter type, but you can reconfigure your gateway to use the VMXNET3 (10 GbE) network adapter. You can also configure Storage Gateway so it can be accessed by more than one IP address. You do this by configuring your gateway to use more than one network adapter.

### Topics

- [Configuring Your Gateway to Use the VMXNET3 Network Adapter \(p. 301\)](#)
- [Configuring Your Gateway for Multiple NICs \(p. 303\)](#)

## Configuring Your Gateway to Use the VMXNET3 Network Adapter

Storage Gateway supports the E1000 network adapter type in both VMware ESXi and Microsoft Hyper-V hypervisor hosts. However, the VMXNET3 (10 GbE) network adapter type is supported in VMware ESXi hypervisor only. If your gateway is hosted on a VMware ESXi hypervisor, you can reconfigure your gateway to use the VMXNET3 (10 GbE) adapter type. For more information on this adapter, see the [VMware website](#).

### Important

To select VMXNET3, your guest operating system type must be **Other Linux64**.

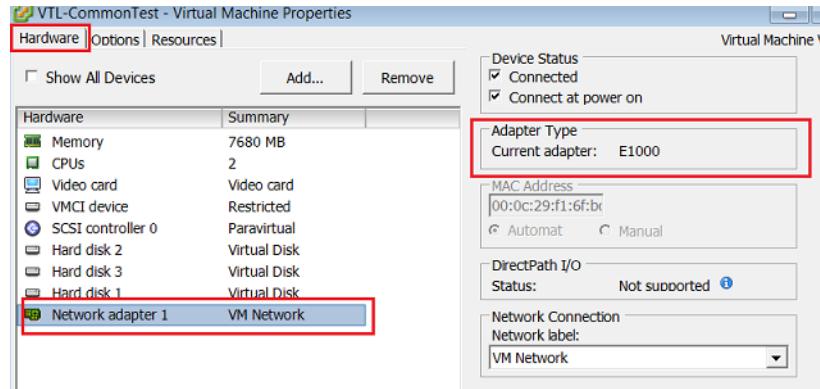
Following are the steps you take to configure your gateway to use the VMXNET3 adapter:

1. Remove the default E1000 adapter.
2. Add the VMXNET3 adapter.
3. Restart your gateway.
4. Configure the adapter for the network.

Details on how to perform each step follow.

### To remove the default E1000 adapter and configure your gateway to use the VMXNET3 adapter

1. In VMware, open the context (right-click) menu for your gateway and choose **Edit Settings**.
2. In the **Virtual Machine Properties** window, choose the **Hardware** tab.
3. For **Hardware**, choose **Network adapter**. Notice that the current adapter is E1000 in the **Adapter Type** section. You will replace this adapter with the VMXNET3 adapter.



4. Choose the E1000 network adapter, and then choose **Remove**. In this example, the E1000 network adapter is **Network adapter 1**.

### Note

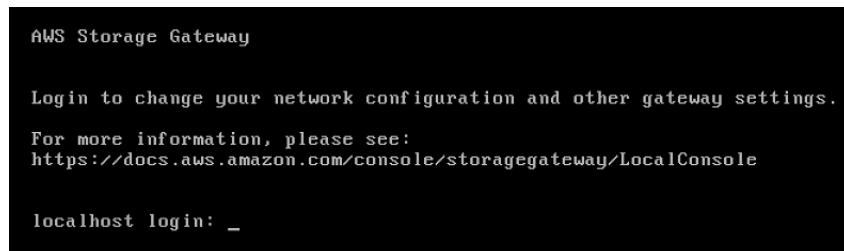
Although you can run the E1000 and VMXNET3 network adapters in your gateway at the same time, we don't recommend doing so because it can cause network problems.

5. Choose **Add** to open the Add Hardware wizard.
6. Choose **Ethernet Adapter**, and then choose **Next**.
7. In the Network Type wizard, select **VMXNET3** for **Adapter Type**, and then choose **Next**.
8. In the Virtual Machine properties wizard, verify in the **Adapter Type** section that **Current Adapter** is set to **VMXNET3**, and then choose **OK**.
9. In the VMware VSphere client, shut down your gateway.
10. In the VMware VSphere client, restart your gateway.

After your gateway restarts, reconfigure the adapter you just added to make sure that network connectivity to the internet is established.

### To configure the adapter for the network

1. In the VSphere client, choose the **Console** tab to start the local console. You will use the default login credentials to log in to the gateway's local console for this configuration task. For information about how to log in using the default credentials, see [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).

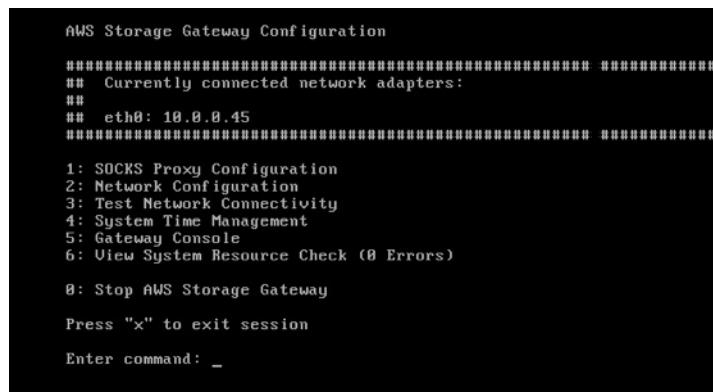


AWS Storage Gateway

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: \_



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: \_

2. At the prompt, type **2** to select **Network Configuration**, and then press **Enter** to open the network configuration menu.
3. At the prompt, type **4** to select **Reset to DHCP**, and then type **y** (for yes) at the prompt to reset the adapter you just added to use Dynamic Host Configuration Protocol (DHCP). You can type **5** to set all adapters to DHCP.
4. At the **Enter the adapter** prompt, type **eth0**, and then press **Enter** to continue. The only adapter available is **eth0**.

```
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: 2

Available adapters: eth0
Enter Network Adapter: eth0

Reset to DHCP [y/n]: y

Adapter eth0 set to use DHCP

You must exit Network Configuration to complete this configuration.

Press Return to Continue_
```

If your gateway is already activated, you must shut it down and restart it from the Storage Gateway Management Console. After the gateway restarts, you must test network connectivity to the internet. For information about how to test network connectivity, see [Testing Your Gateway Connection to the Internet \(p. 296\)](#).

## Configuring Your Gateway for Multiple NICs

If you configure your gateway to use multiple network adapters (NICs), it can be accessed by more than one IP address. You might want to do this in the following situations:

- **Maximizing throughput** – You might want to maximize throughput to a gateway when network adapters are a bottleneck.
- **Application separation** – You might need to separate how your applications write to a gateway's volumes. For example, you might choose to have a critical storage application exclusively use one particular adapter defined for your gateway.
- **Network constraints** – Your application environment might require that you keep your iSCSI targets and the initiators that connect to them in an isolated network that is different from the network by which the gateway communicates with AWS.

In a typical multiple-adapter use case, one adapter is configured as the route by which the gateway communicates with AWS (that is, as the default gateway). Except for this one adapter, initiators must be in the same subnet as the adapter that contains the iSCSI targets to which they connect. Otherwise, communication with the intended targets might not be possible. If a target is configured on the same adapter that is used for communication with AWS, then iSCSI traffic for that target and AWS traffic will flow through the same adapter.

When you configure one adapter to connect to the Storage Gateway console and then add a second adapter, storage gateway automatically configures the route table to use the second adapter as the preferred route. For instructions on how to configure multiple-adapters, see the following sections.

- [Configuring Your Gateway for Multiple NICs in a VMware ESXi Host \(p. 315\)](#)
- [Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host \(p. 317\)](#)

# Performing Tasks on the Amazon EC2 Local Console (Volume and Tape Gateways)

Some maintenance tasks require that you log in to the local console when running a gateway deployed on an Amazon EC2 instance. In this section, you can find information about how to log in to the local console and perform maintenance tasks.

## Topics

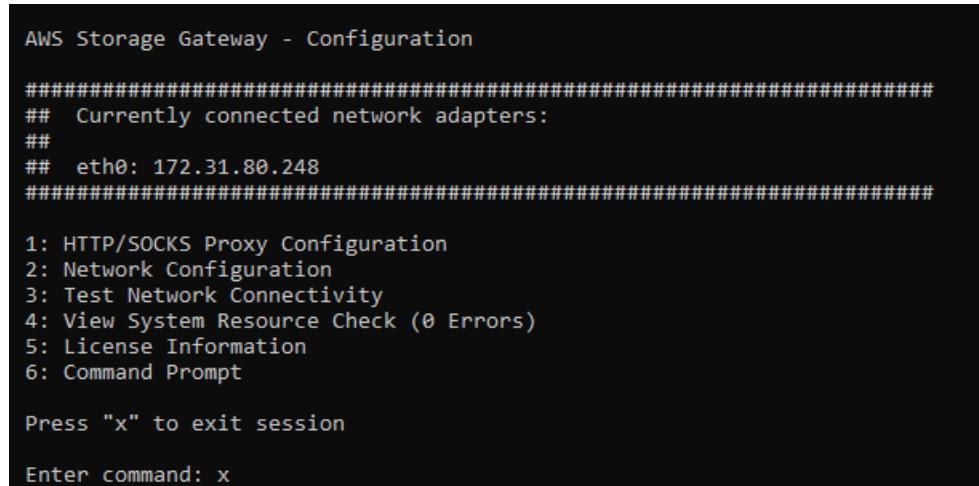
- [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#)
- [Routing Your Gateway Deployed on Amazon EC2 Through a Proxy \(p. 305\)](#)
- [Testing Your Gateway Connectivity to the Internet \(p. 306\)](#)
- [Running Storage Gateway Commands on the Local Console \(p. 307\)](#)
- [Viewing Your Gateway System Resource Status \(p. 309\)](#)

## Logging In to Your Amazon EC2 Gateway Local Console

You can connect to your Amazon EC2 instance by using a Secure Shell (SSH) client. For detailed information, see [Connect to Your Instance](#) in the *Amazon EC2 User Guide*. To connect this way, you will need the SSH key pair you specified when you launched the instance. For information about Amazon EC2 key pairs, see [Amazon EC2 Key Pairs](#) in the *Amazon EC2 User Guide*.

### To log in to the gateway local console

1. Log in to your local console. If you are connecting to your EC2 instance from a Windows computer, log in as *admin*.
2. After you log in, you see the **Storage Gateway Configuration** main menu, as shown in the following screenshot.



The screenshot shows a terminal window titled "AWS Storage Gateway - Configuration". It displays a menu with the following options:

```
AWS Storage Gateway - Configuration
#####
## Currently connected network adapters:
##
## eth0: 172.31.80.248
#####

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

Press "x" to exit session

Enter command: x
```

To	See
Configure a SOCKS proxy for your gateway	<a href="#">Routing Your Gateway Deployed on Amazon EC2 Through a Proxy (p. 305)</a>
Test network connectivity	<a href="#">Testing Your Gateway Connectivity to the Internet (p. 306)</a>

To	See
Run Storage Gateway console commands	<a href="#">Running Storage Gateway Commands on the Local Console (p. 307)</a>
View a system resource check	<a href="#">Logging In to Your Amazon EC2 Gateway Local Console (p. 304).</a>

To shut down the gateway, type **0**.

To exit the configuration session, type **x** to exit the menu.

## Routing Your Gateway Deployed on Amazon EC2 Through a Proxy

Storage Gateway supports the configuration of a Socket Secure version 5 (SOCKS5) proxy between your gateway deployed on Amazon EC2 and AWS.

### Note

The only proxy configuration Storage Gateway supports is SOCKS5.

If your gateway must use a proxy server to communicate to the internet, then you need to configure the SOCKS proxy settings for your gateway. You do this by specifying an IP address and port number for the host running your proxy. After you do so, Storage Gateway will route all HyperText Transfer Protocol Secure (HTTPS) traffic through your proxy server.

### To route your gateway internet traffic through a local proxy server

1. Log in to your gateway's local console. For instructions, see [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#).
2. On the **Storage Gateway Configuration** main menu, type **1** to begin configuring the SOCKS proxy.

```
AWS Storage Gateway - Configuration
#####
## Currently connected network adapters:
##
## eth0: 172.31.80.248
#####

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

Press "x" to exit session

Enter command: x
```

3. Choose one of the following options in the **Storage Gateway SOCKS Proxy Configuration** menu:

```
AWS Storage Gateway SOCKS Proxy Configuration
1: Configure SOCKS Proxy
2: View Current SOCKS Proxy Configuration
3: Remove SOCKS Proxy Configuration

Press "x" to exit

Enter command: _
```

To	Do This
Configure a SOCKS proxy	Type <b>1</b> .  You need to supply a host name and port to complete configuration.
View the current SOCKS proxy configuration	Type <b>2</b> .  If a SOCKS proxy is not configured, the message <code>SOCKS Proxy not configured</code> is displayed. If a SOCKS proxy is configured, the host name and port of the proxy are displayed.
Remove a SOCKS proxy configuration	Type <b>3</b> .  The message <code>SOCKS Proxy Configuration Removed</code> is displayed.
Exit this menu and return to the previous menu	Type <b>x</b> .

## Testing Your Gateway Connectivity to the Internet

You can use your gateway's local console to test your Internet connection. This test can be useful when you are troubleshooting network issues with your gateway.

### To test your gateway's connection to the internet

1. Log in to your gateway's local console. For instructions, see [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#).
2. In the **Storage Gateway Configuration** main menu, type **2** to begin testing network connectivity.

```
AWS Storage Gateway - Configuration

#####
## Currently connected network adapters:
##
## eth0: 172.31.80.248
#####

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

Press "x" to exit session

Enter command: x
```

The console displays the available regions.

3. Select the region you want to test. For example, us-east-2. For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas in the AWS General Reference](#).

Each endpoint in the region you select displays either a **[PASSED]** or **[FAILED]** message, as shown following.

Message	Description
<b>[PASSED]</b>	Storage Gateway has internet connectivity.
<b>[FAILED]</b>	Storage Gateway does not have internet connectivity.

## Running Storage Gateway Commands on the Local Console

The AWS Storage Gateway console helps provide a secure environment for configuring and diagnosing issues with your gateway. Using the console commands, you can perform maintenance tasks such as saving routing tables or connecting to AWS Support.

### To run a configuration or diagnostic command

1. Log in to your gateway's local console. For instructions, see [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#).
2. In the **Storage Gateway Configuration** main menu, type **3** for **Gateway Console**.

```
AWS Storage Gateway - Configuration

#####
## Currently connected network adapters:
##
## eth0: 172.31.80.248
#####

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

Press "x" to exit session

Enter command: x
```

3. In the Storage Gateway console, type **h**, and then press the **Return** key.

The console displays the **Available Commands** menu with the available commands. After the menu, a **Gateway Console** prompt appears, as shown in the following screenshot.

```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands

ip                                Show / manipulate routing, devices, policy routing and tunnels
save-routing-table                 Save newly added routing table entry
ifconfig                           View or configure network interfaces
iptables                          Administration tool for IPv4 packet filtering and NAT
save-iptables                     Persist IP tables
testconn                           Test network connectivity
man                               Display command manual pages
open-support-channel              Connect to Storage Gateway Support
h                                 Display available command list
exit                             Return to Storage Gateway Configuration menu

Gateway Console: █
```

4. To learn about a command, type `man + command name` at the **Gateway Console** prompt.

## Viewing Your Gateway System Resource Status

When your gateway starts, it checks its virtual CPU cores, root volume size, and RAM and determines whether these system resources are sufficient for your gateway to function properly. You can view the results of this check on the gateway's local console.

### To view the status of a system resource check

1. Log in to your gateway's local console. For instructions, see [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#).
2. In the **Storage Gateway Configuration** main menu, type **4** to view the results of a system resource check.

```
AWS Storage Gateway - Configuration
#####
## Currently connected network adapters:
##
## eth0: 172.31.80.248
#####

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

Press "x" to exit session

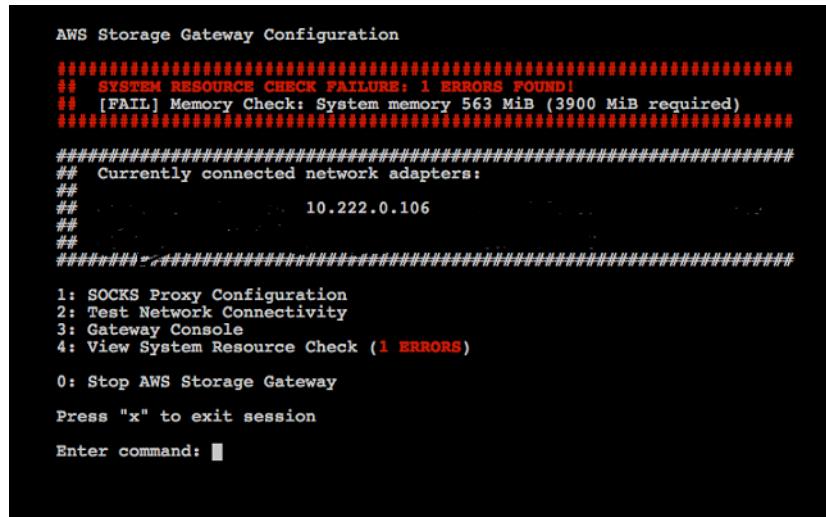
Enter command: x
```

The console displays an **[OK]**, **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
<b>[OK]</b>	The resource has passed the system resource check.
<b>[WARNING]</b>	The resource does not meet the recommended requirements, but your gateway will continue to function. Storage Gateway displays a message that describes the results of the resource check.
<b>[FAIL]</b>	The resource does not meet the minimum requirements. Your gateway might not function properly. Storage Gateway displays a message that describes the results of the resource check.

The console also displays the number of errors and warnings next to the resource check menu option.

The following screenshot shows a **[FAIL]** message and the accompanying error message.



```
AWS Storage Gateway Configuration

#####
## SYSTEM RESOURCE CHECK FAILURE: 1 ERRORS FOUND!
## [FAIL] Memory Check: System memory 563 MiB (3900 MiB required)
#####

#####
## Currently connected network adapters:
##
##          10.222.0.106
##
#####

1: SOCKS Proxy Configuration
2: Test Network Connectivity
3: Gateway Console
4: View System Resource Check (1 ERRORS)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: ■
```

## Accessing the Gateway Local Console

How you access your VM's local console depends on the type of the Hypervisor you deployed your gateway VM on. In this section, you can find information on how to access the VM local console using Linux Kernel-based Virtual Machine (KVM), VMware ESXi, and Microsoft Hyper-V Manager.

For instructions to access the gateway local console for Tape Gateway on Snowball Edge, see [Troubleshooting and best practices for Tape Gateway on Snowball Edge](#).

### Topics

- [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#)
- [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#)
- [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#)

## Accessing the Gateway Local Console with Linux KVM

There are different ways to configure virtual machines running on KVM, depending on the Linux distribution being used. Instructions for accessing KVM configuration options from the command line follow. Instructions might differ depending on your KVM implementation.

### To access your gateway's local console with KVM

1. Use the following command to list the VMs that are currently available in KVM.

```
# virsh list
```

You can choose available VMs by Id.

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

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

2. Use the following command to access the local console.

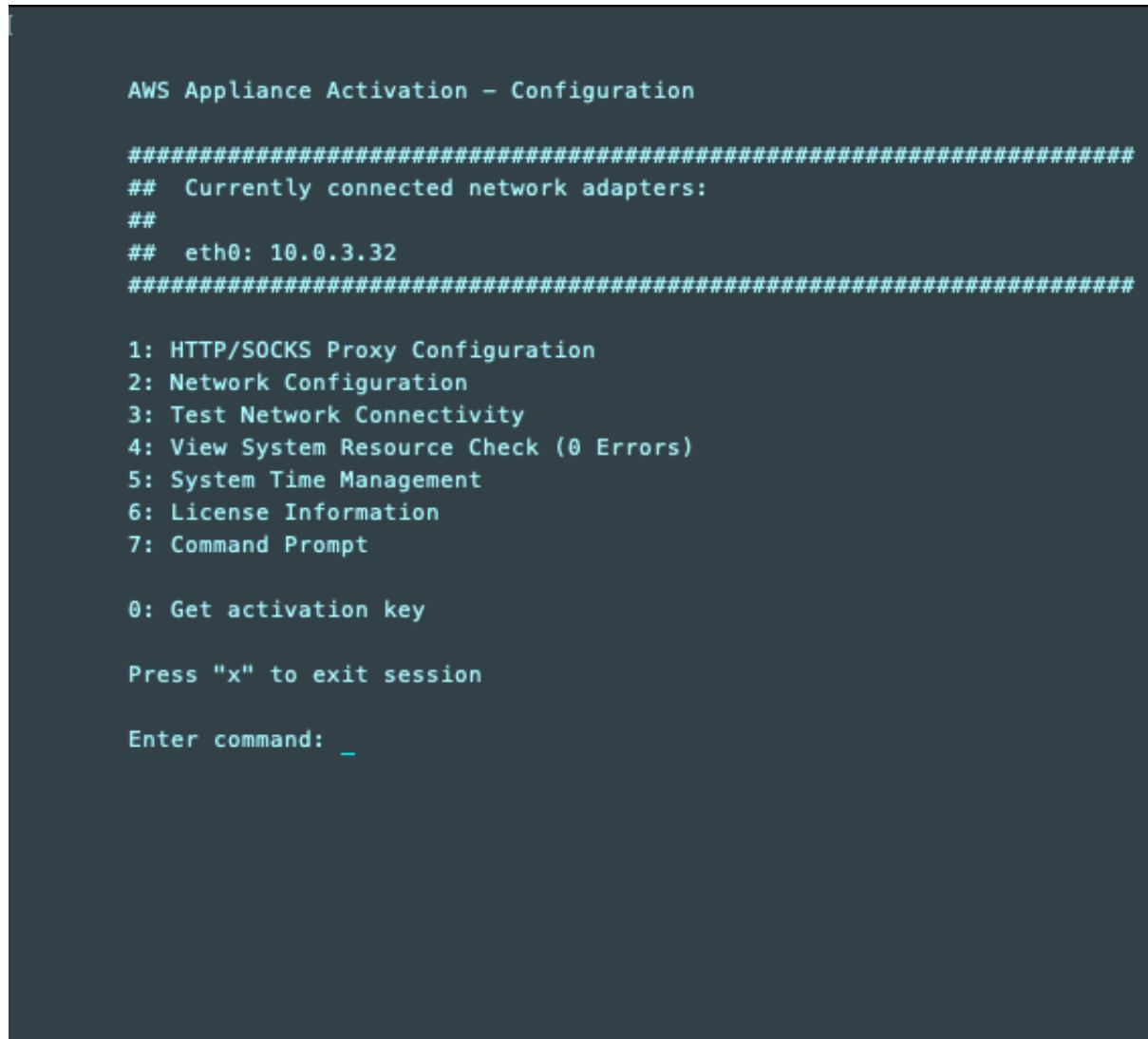
```
# virsh console VM_Id
```

```
[[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. To get default credentials to log in to the local console, see [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).
4. After you have logged in, you can activate and configure your gateway.



The screenshot shows a terminal window with the title "AWS Appliance Activation - Configuration". It displays a menu with various options numbered 1 through 7, plus an option 0. The menu includes descriptions for each option and a prompt to press "x" to exit. The background of the terminal window is dark.

```
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: _
```

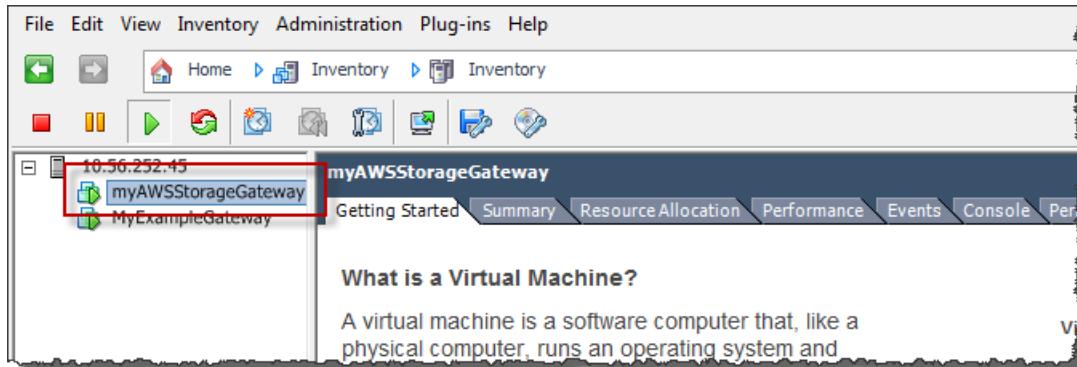
## Accessing the Gateway Local Console with VMware ESXi

### To access your gateway's local console with VMware ESXi

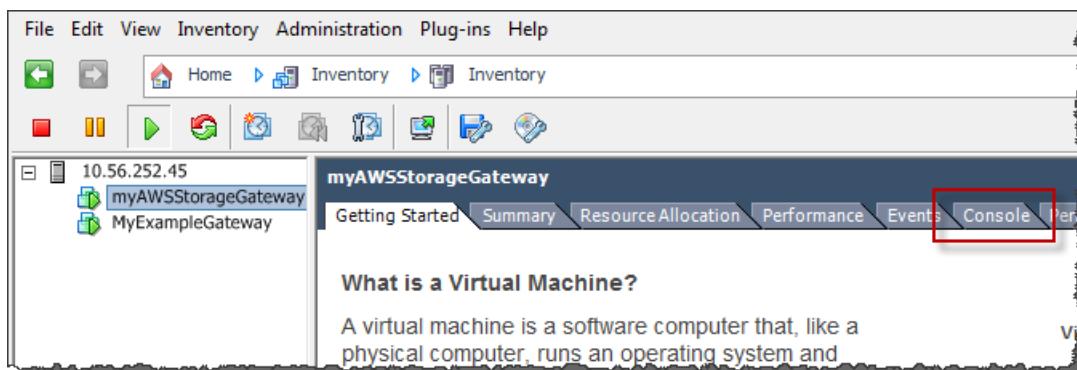
1. In the VMware vSphere client, select your gateway VM.
2. Make sure that the gateway is turned on.

#### Note

If your gateway VM is turned on, a green arrow icon appears with the VM icon, as shown in the following screenshot. If your gateway VM is not turned on, you can turn it on by choosing the green **Power On** icon on the **Toolbar** menu.



3. Choose the **Console** tab.



After a few moments, the VM is ready for you to log in.

**Note**

To release the cursor from the console window, press **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. To log in using the default credentials, continue to the procedure [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).

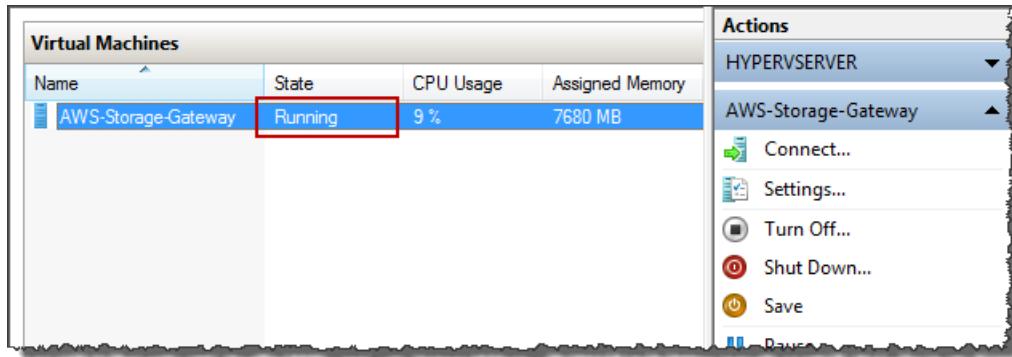
## Access the Gateway Local Console with Microsoft Hyper-V

### To access your gateway's local console (Microsoft Hyper-V)

1. In the **Virtual Machines** list of the Microsoft Hyper-V Manager, select your gateway VM.
2. Make sure that the gateway is turned on.

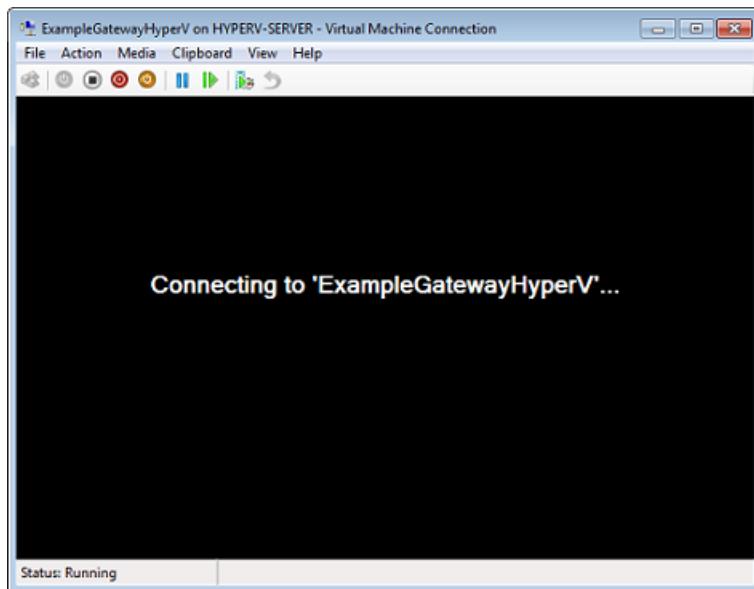
**Note**

If your gateway VM is turned on, Running is displayed as the **State** of the VM, as shown in the following screenshot. If your gateway VM is not turned on, you can turn it on by choosing **Start** in the **Actions** pane.

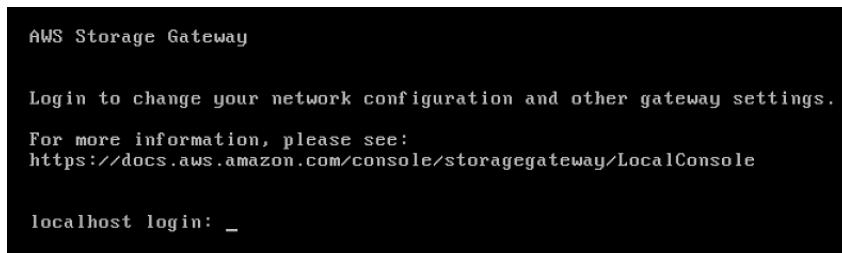


3. In the **Actions** pane, choose **Connect**.

The **Virtual Machine Connection** window appears. If an authentication window appears, type the user name and password provided to you by the hypervisor administrator.



After a few moments, the VM is ready for you to log in.



4. To log in using the default credentials, continue to the procedure [Logging in to the Local Console Using Default Credentials \(p. 288\)](#).

# Configuring Network Adapters for Your Gateway

In this section you can find information about how configure multiple network adapters for your gateway.

## Topics

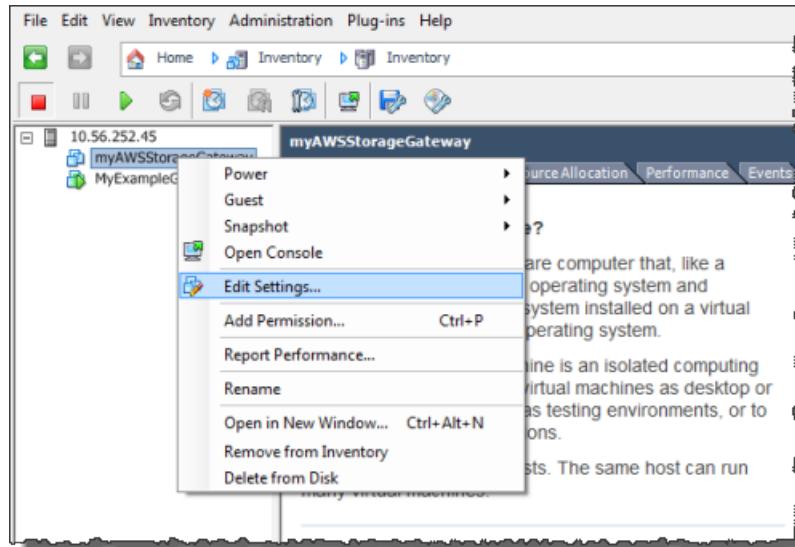
- [Configuring Your Gateway for Multiple NICs in a VMware ESXi Host \(p. 315\)](#)
- [Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host \(p. 317\)](#)

## Configuring Your Gateway for Multiple NICs in a VMware ESXi Host

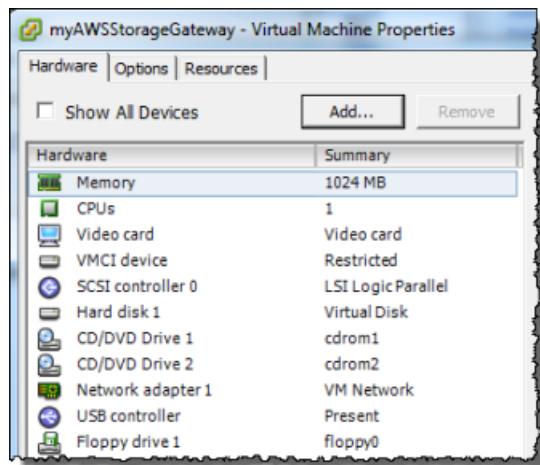
The following procedure assumes that your gateway VM already has one network adapter defined and that you are adding a second adapter. The following procedure shows how to add an adapter for VMware ESXi.

### To configure your gateway to use an additional network adapter in VMware ESXi host

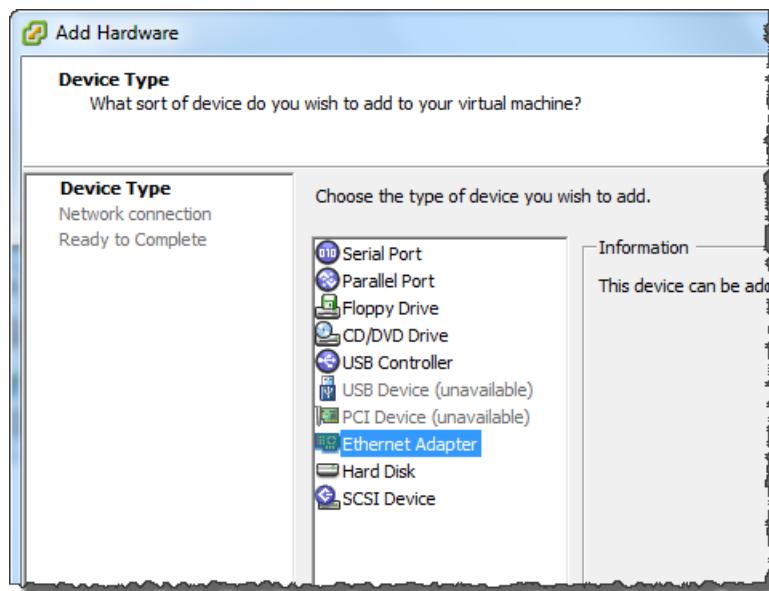
1. Shut down the gateway. For instructions, see [To stop a volume or tape gateway \(p. 253\)](#).
2. In the VMware vSphere client, select your gateway VM.  
The VM can remain turned on for this procedure.
3. In the client, open the context (right-click) menu for your gateway VM, and choose **Edit Settings**.



4. On the **Hardware** tab of the **Virtual Machine Properties** dialog box, choose **Add** to add a device.



5. Follow the Add Hardware wizard to add a network adapter.
- a. In the **Device Type** pane, choose **Ethernet Adapter** to add an adapter, and then choose **Next**.

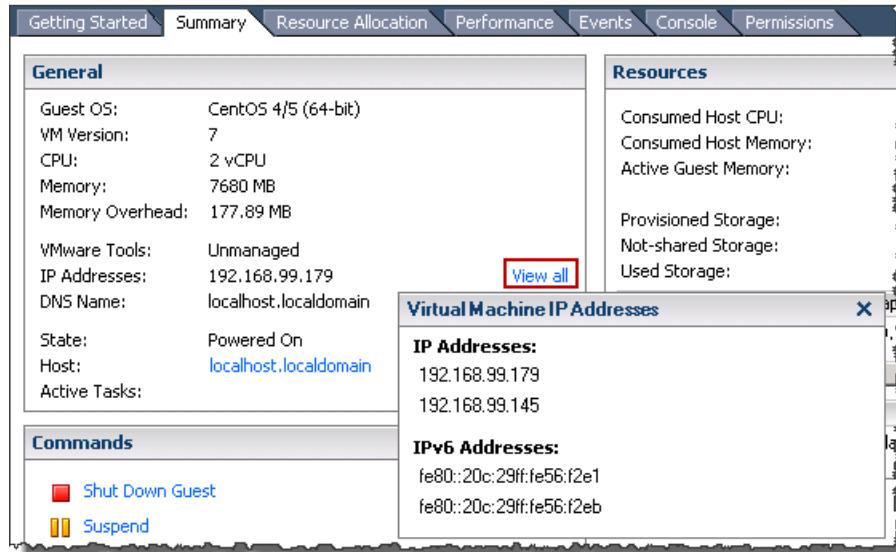


- b. In the **Network Type** pane, ensure that **Connect at power on** is selected for **Type**, and then choose **Next**.  
  
We recommend that you use the WmxBNet3 network adapter with Storage Gateway. For more information on the adapter types that might appear in the adapter list, see Network Adapter Types in the [ESXi and vCenter Server Documentation](#).
- c. In the **Ready to Complete** pane, review the information, and then choose **Finish**.
6. Choose the **Summary** tab of the VM, and choose **View All** next to the **IP Address** box. A **Virtual Machine IP Addresses** window displays all the IP addresses you can use to access the gateway. Confirm that a second IP address is listed for the gateway.

#### Note

It might take several moments for the adapter changes to take effect and the VM summary information to refresh.

The following image is for illustration only. In practice, one of the IP addresses will be the address by which the gateway communicates to AWS and the other will be an address in a different subnet.



7. On the Storage Gateway console, turn on the gateway. For instructions, see [To start a volume or tape gateway \(p. 254\)](#).
8. In the **Navigation** pane of the Storage Gateway console, choose **Gateways** and choose the gateway to which you added the adapter. Confirm that the second IP address is listed in the **Details** tab.

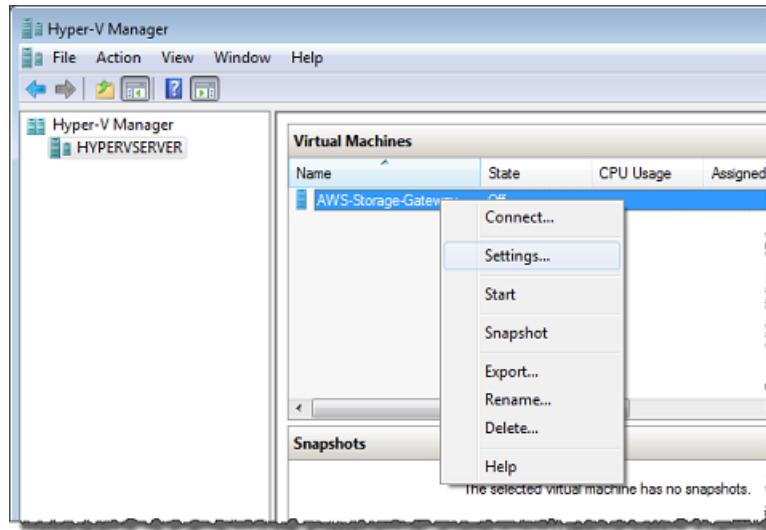
For information about local console tasks common to VMware, Hyper-V, and KVM hosts, see [Performing Tasks on the VM Local Console \(Volume and Tape Gateways\) \(p. 287\)](#)

## Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host

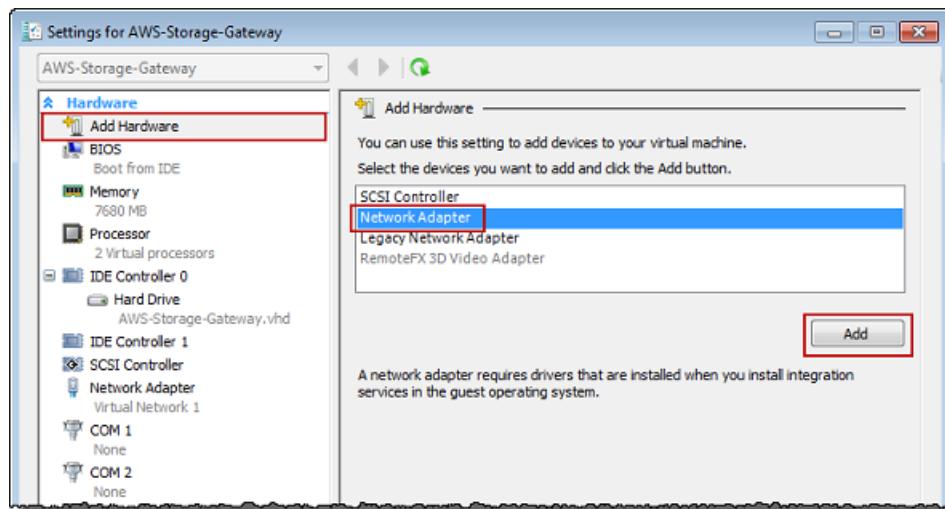
The following procedure assumes that your gateway VM already has one network adapter defined and that you are adding a second adapter. This procedure shows how to add an adapter for a Microsoft Hyper-V host.

### To configure your gateway to use an additional network adapter in a Microsoft Hyper-V Host

1. On the Storage Gateway console, turn off the gateway. For instructions, see [To stop a volume or tape gateway \(p. 253\)](#).
2. In the Microsoft Hyper-V Manager, select your gateway VM.
3. If the VM isn't turned off already, open the context (right-click) menu for your gateway and choose **Turn Off**.
4. In the client, open the context menu for your gateway VM and choose **Settings**.

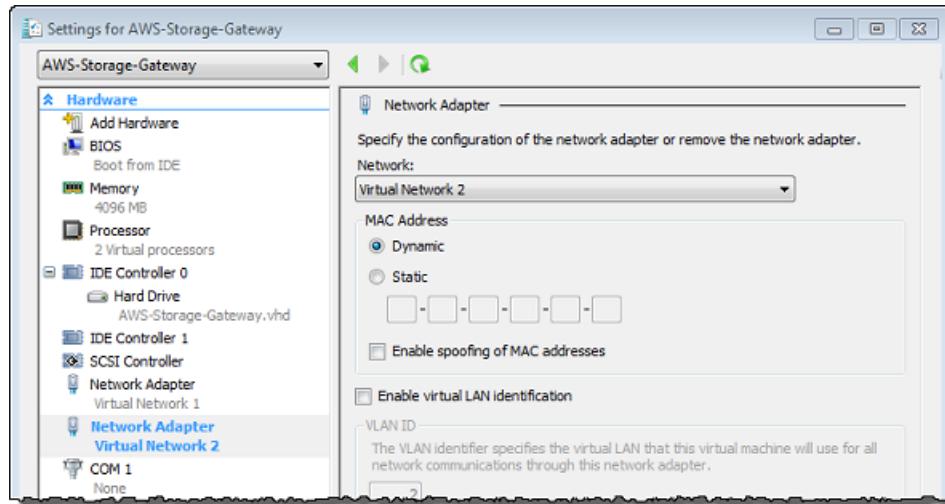


5. In the **Settings** dialog box for the VM, for **Hardware**, choose **Add Hardware**.
6. In the **Add Hardware** pane, choose **Network Adapter**, and then choose **Add** to add a device.



7. Configure the network adapter, and then choose **Apply** to apply settings.

In the following example, **Virtual Network 2** is selected for the new adapter.



8. In the **Settings** dialog box, for **Hardware**, confirm that the second adapter was added, and then choose **OK**.
9. On the Storage Gateway console, turn on the gateway. For instructions, see [To start a volume or tape gateway \(p. 254\)](#).
10. In the **Navigation** pane choose **Gateways**, then select the gateway to which you added the adapter. Confirm that the second IP address is listed in the **Details** tab.

For information about local console tasks common to VMware, Hyper-V, and KVM hosts, see [Performing Tasks on the VM Local Console \(Volume and Tape Gateways\) \(p. 287\)](#)

## Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources

If you don't plan to continue using your gateway, consider deleting the gateway and its associated resources. Removing resources avoids incurring charges for resources you don't plan to continue using and helps reduce your monthly bill.

When you delete a gateway, it no longer appears on the AWS Storage Gateway Management Console and its iSCSI connection to the initiator is closed. The procedure for deleting a gateway is the same for all gateway types; however, depending on the type of gateway you want to delete and the host it is deployed on, you follow specific instructions to remove associated resources.

You can delete a gateway using the Storage Gateway console or programmatically. You can find information following about how to delete a gateway using the Storage Gateway console. If you want to programmatically delete your gateway, see [AWS Storage Gateway API Reference](#).

### Topics

- [Deleting Your Gateway by Using the Storage Gateway Console \(p. 320\)](#)
- [Removing Resources from a Gateway Deployed On-Premises \(p. 320\)](#)
- [Removing Resources from a Gateway Deployed on an Amazon EC2 Instance \(p. 321\)](#)

# Deleting Your Gateway by Using the Storage Gateway Console

The procedure for deleting a gateway is the same for all gateway types. However, depending on the type of gateway you want to delete and the host the gateway is deployed on, you might have to perform additional tasks to remove resources associated with the gateway. Removing these resources helps you avoid paying for resources you don't plan to use.

## Note

For gateways deployed on an Amazon EC2 instance, the instance continues to exist until you delete it.

For gateways deployed on a virtual machine (VM), after you delete your gateway the gateway VM still exists in your virtualization environment. To remove the VM, use the VMware vSphere client, Microsoft Hyper-V Manager, or Linux Kernel-based Virtual Machine (KVM) client to connect to the host and remove the VM. Note that you can't reuse the deleted gateway's VM to activate a new gateway.

## To delete a gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose the gateway you want to delete.
3. For **Actions**, choose **Delete gateway**.
4. **Warning**  
Before you do this step, make sure that there are no applications currently writing to the gateway's volumes. If you delete the gateway while it is in use, data loss can occur. When a gateway is deleted, there is no way to get it back.

In the confirmation dialog box that appears, make sure the specified gateway ID matches the gateway you want to delete, then type the word *delete* in the text box, and click **Delete**.

5. (Optional) If you want to provide feedback about your deleted gateway, complete the feedback dialog box, then click **Submit**. Otherwise, click **Skip**.

## Important

You no longer pay software charges after you delete a gateway, but resources such as virtual tapes, Amazon Elastic Block Store (Amazon EBS) snapshots, and Amazon EC2 instances persist. You will continue to be billed for these resources. You can choose to remove Amazon EC2 instances and Amazon EBS snapshots by canceling your Amazon EC2 subscription. If you want to keep your Amazon EC2 subscription, you can delete your Amazon EBS snapshots using the Amazon EC2 console.

# Removing Resources from a Gateway Deployed On-Premises

You can use the instructions following to remove resources from a gateway that is deployed on-premises.

## Removing Resources from a Volume Gateway Deployed on a VM

If the gateway you want to delete are deployed on a virtual machine (VM), we suggest that you take the following actions to clean up resources:

- Delete the gateway. For instructions, see [Deleting Your Gateway by Using the Storage Gateway Console \(p. 320\)](#).

- Delete all Amazon EBS snapshots you don't need. For instructions, see [Deleting an Amazon EBS Snapshot](#) in the *Amazon EC2 User Guide for Linux Instances*.

## Removing Resources from a Tape Gateway Deployed on a VM

When you delete a gateway–virtual tape library (VTL), you perform additional cleanup steps before and after you delete the gateway. These additional steps help you remove resources you don't need so you don't continue to pay for them.

If the tape gateway you want to delete is deployed on a virtual machine (VM), we suggest that you take the following actions to clean up resources.

**Important**

Before you delete a tape gateway, you must cancel all tape retrieval operations and eject all retrieved tapes.

After you have deleted the tape gateway, you must remove any resources associated with the tape gateway that you don't need to avoid paying for those resources.

When you delete a tape gateway, you can encounter one of two scenarios.

- **The tape gateway is connected to AWS** – If the tape gateway is connected to AWS and you delete the gateway, the iSCSI targets associated with the gateway (that is, the virtual tape drives and media changer) will no longer be available.
- **The tape gateway is not connected to AWS** – If the tape gateway is not connected to AWS, for example if the underlying VM is turned off or your network is down, then you cannot delete the gateway. If you attempt to do so, after your environment is back up and running you might have a tape gateway running on-premises with available iSCSI targets. However, no tape gateway data will be uploaded to, or downloaded from, AWS.

If the tape gateway you want to delete is not functioning, you must first disable it before you delete it, as described following:

- To delete tapes that have the RETRIEVED status from the library, eject the tape using your backup software. For instructions, see [Archiving the Tape \(p. 146\)](#).

After disabling the tape gateway and deleting tapes, you can delete the tape gateway. For instructions on how to delete a gateway, see [Deleting Your Gateway by Using the Storage Gateway Console \(p. 320\)](#).

If you have tapes archived, those tapes remain and you continue to pay for storage until you delete them. For instruction on how to delete tapes from a archive. see [Deleting Tapes \(p. 204\)](#).

**Important**

You are charged for a minimum of 90 days storage for virtual tapes in a archive. If you retrieve a virtual tape that has been stored in the archive for less than 90 days, you are still charged for 90 days storage.

## Removing Resources from a Gateway Deployed on an Amazon EC2 Instance

If you want to delete a gateway that you deployed on an Amazon EC2 instance, we recommend that you clean up the AWS resources that were used with the gateway, specifically the Amazon EC2 instance, any Amazon EBS volumes, and also tapes if you deployed a tape gateway. Doing so helps avoid unintended usage charges.

## Removing Resources from Your Cached Volumes Deployed on Amazon EC2

If you deployed a gateway with cached volumes on EC2, we suggest that you take the following actions to delete your gateway and clean up its resources:

1. In the Storage Gateway console, delete the gateway as shown in [Deleting Your Gateway by Using the Storage Gateway Console \(p. 320\)](#).
2. In the Amazon EC2 console, stop your EC2 instance if you plan on using the instance again. Otherwise, terminate the instance. If you plan on deleting volumes, make note of the block devices that are attached to the instance and the devices' identifiers before terminating the instance. You will need these to identify the volumes you want to delete.
3. In the Amazon EC2 console, remove all Amazon EBS volumes that are attached to the instance if you don't plan on using them again. For more information, see [Clean Up Your Instance and Volume](#) in the *Amazon EC2 User Guide for Linux Instances*.

## Removing Resources from Your Tape Gateway Deployed on Amazon EC2

If you deployed a tape gateway, we suggest that you take the following actions to delete your gateway and clean up its resources:

1. Delete all virtual tapes that you have retrieved to your tape gateway. For more information, see [Deleting Tapes \(p. 204\)](#).
2. Delete all virtual tapes from the tape library. For more information, see [Deleting Tapes \(p. 204\)](#).
3. Delete the tape gateway. For more information, see [Deleting Your Gateway by Using the Storage Gateway Console \(p. 320\)](#).
4. Terminate all Amazon EC2 instances, and delete all Amazon EBS volumes. For more information, see [Clean Up Your Instance and Volume](#) in the *Amazon EC2 User Guide for Linux Instances*.
5. Delete all archived virtual tapes. For more information, see [Deleting Tapes \(p. 204\)](#).

**Important**

You are charged for a minimum of 90 days storage for virtual tapes in the archive. If you retrieve a virtual tape that has been stored in the archive for less than 90 days, you are still charged for 90 days storage.

# Performance

In this section, you can find information about Storage Gateway performance.

## Topics

- [Performance guidance for file gateways \(p. 323\)](#)
- [Performance guidance for tape gateways \(p. 325\)](#)
- [Optimizing Gateway Performance \(p. 327\)](#)
- [Using VMware vSphere High Availability with Storage Gateway \(p. 329\)](#)

## Performance guidance for file gateways

In this section, you can find configuration guidance for provisioning hardware for your file gateway VM. The Amazon EC2 instance sizes and types that are listed in the table are examples, and are provided for reference.

For best performance, the cache disk size must be tuned to the size of the active working set. Using multiple local disks for the cache increases write performance by parallelizing access to data and leads to higher IOPS.

In the following tables, *cache hit* read operations are reads from the file shares that are served from cache. *Cache miss* read operations are reads from the file shares that are served from Amazon S3.

### Note

We don't recommend using ephemeral storage. For information about using ephemeral storage, see [the section called "Using ephemeral storage with EC2 gateways" \(p. 257\)](#).

Following are example file gateway configurations.

## File gateway performance on Linux clients

Example Configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Root disk: 80, GB io1, 4,000 IOPS  Cache disk: 512 GiB cache, io1, 1,500 provisioned IOPS  Minimum network performance: 10 Gbps	NFSv3 - 1 thread	110 MiB/sec (0.92 Gbps)	590 MiB/sec (4.9 Gbps)	310 MiB/sec (2.6 Gbps)
	NFSv3 - 8 threads	160 MiB/sec (1.3 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
	NFSv4 - 1 thread	130 MiB/sec (1.1 Gbps)	590 MiB/sec (4.9 Gbps)	295 MiB/sec (2.5 Gbps)
	NFSv4 - 8 threads	160 MiB/sec (1.3 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
	SMBV3 - 1 thread	115 MiB/sec (1.0 Gbps)	325 MiB/sec (2.7 Gbps)	255 MiB/sec (2.1 Gbps)

<b>Example Configurations</b>	<b>Protocol</b>	<b>Write throughput (file sizes 1 GB)</b>	<b>Cache hit read throughput</b>	<b>Cache miss read throughput</b>
CPU: 16 vCPU   RAM: 32 GB  NFS protocol recommended for Linux	SMBV3 - 8 threads	190 MiB/sec (1.6 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
<b>Storage Gateway Hardware Appliance</b>  Minimum network performance: 10 Gbps	NFSv3 - 1 thread	265 MiB/sec (2.2 Gbps)	590 MiB/sec (4.9 Gbps)	310 MiB/sec (2.6 Gbps)
	NFSv3 - 8 threads	385 MiB/sec (3.1 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
	NFSv4 - 1 thread	310 MiB/sec (2.6 Gbps)	590 MiB/sec (4.9 Gbps)	295 MiB/sec (2.5 Gbps)
	NFSv4 - 8 threads	385 MiB/sec (3.1 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
	SMBV3 - 1 thread	275 MiB/sec (2.4 Gbps)	325 MiB/sec (2.7 Gbps)	255 MiB/sec (2.1 Gbps)
	SMBV3 - 8 threads	455 MiB/sec (3.8 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)
Root disk: 80 GB, io1 SSD, 4,000 IOPS  Cache disk: 4 x 2 TB NVME cache disks  Minimum network performance: 10 Gbps  CPU: 32 vCPU   RAM: 244 GB  NFS protocol recommended for Linux	NFSv3 - 1 thread	300 MiB/sec (2.5 Gbps)	590 MiB/sec (4.9 Gbps)	325 MiB/sec (2.7 Gbps)
	NFSv3 - 8 threads	585 MiB/sec (4.9 Gbps)	590 MiB/sec (4.9 Gbps)	580 MiB/sec (4.8 Gbps)
	NFSv4 - 1 thread	355 MiB/sec (3.0 Gbps)	590 MiB/sec (4.9 Gbps)	340 MiB/sec (2.9 Gbps)
	NFSv4 - 8 threads	575 MiB/sec (4.8 Gbps)	590 MiB/sec (4.9 Gbps)	575 MiB/sec (4.8 Gbps)
	SMBV3 - 1 thread	230 MiB/sec (1.9 Gbps)	325 MiB/sec (2.7 Gbps)	245 MiB/sec (2.0 Gbps)
	SMBV3 - 8 threads	585 MiB/sec (4.9 Gbps)	590 MiB/sec (4.9 Gbps)	580 MiB/sec (4.8 Gbps)

## File gateway performance on Windows clients

<b>Example Configurations</b>	<b>Protocol</b>	<b>Write throughput (file sizes 1 GB)</b>	<b>Cache hit read throughput</b>	<b>Cache miss read throughput</b>
Root disk: 80, GB io1, 4,000 IOPS	SMBV3 - 1 thread	150 MiB/sec (1.3 Gbps)	180 MiB/sec (1.5 Gbps)	20 MiB/sec (0.2 Gbps)
	SMBV3 - 8 threads	190 MiB/sec (1.6 Gbps)	335 MiB/sec (2.8 Gbps)	195 MiB/sec (1.6 Gbps)

Example Configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Cache disk: 512 GiB cache, io1, 1,500 provisioned IOPS  Minimum network performance: 10 Gbps  CPU: 16 vCPU   RAM: 32 GB  SMB protocol recommended for Windows	NFSv3 - 1 thread	95 MiB/sec (0.8 Gbps)	130 MiB/sec (1.1 Gbps)	20 MiB/sec (0.2 Gbps)
Storage Gateway Hardware Appliance  Minimum network performance: 10 Gbps	NFSv3 - 8 threads	190 MiB/sec (1.6 Gbps)	330 MiB/sec (2.8 Gbps)	190 MiB/sec (1.6 Gbps)
	SMBV3 - 1 thread	230 MiB/sec (1.9 Gbps)	255 MiB/sec (2.1 Gbps)	20 MiB/sec (0.2 Gbps)
	SMBV3 - 8 threads	835 MiB/sec (7.0 Gbps)	475 MiB/sec (4.0 Gbps)	195 MiB/sec (1.6 Gbps)
	NFSv3 - 1 thread	135 MiB/sec (1.1 Gbps)	185 MiB/sec (1.6 Gbps)	20 MiB/sec (0.2 Gbps)
Root disk: 80 GB, io1 SSD, 4,000 IOPS  Cache disk: 4 x 2 TB NVME cache disks  Minimum network performance: 10 Gbps  CPU: 32 vCPU   RAM: 244 GB  SMB protocol recommended for Windows	NFSv3 - 8 threads	545 MiB/sec (4.6 Gbps)	470 MiB/sec (4.0 Gbps)	190 MiB/sec (1.6 Gbps)
	SMBV3 - 1 thread	230 MiB/sec (1.9 Gbps)	265 MiB/sec (2.2 Gbps)	30 MiB/sec (0.3 Gbps)
	SMBV3 - 8 threads	835 MiB/sec (7.0 Gbps)	780 MiB/sec (6.5 Gbps)	250 MiB/sec (2.1 Gbps)
	NFSv3 - 1 thread	135 MiB/sec (1.1 Gbps)	220 MiB/sec (1.8 Gbps)	30 MiB/sec (0.3 Gbps)
	NFSv3 - 8 threads	545 MiB/sec (4.6 Gbps)	570 MiB/sec (4.8 Gbps)	240 MiB/sec (2.0 Gbps)

#### Note

Your performance might vary based on your host platform configuration and network bandwidth.

## Performance guidance for tape gateways

In this section, you can find configuration guidance for provisioning hardware for your tape gateway VM. The Amazon EC2 instance sizes and types that are listed in the table are examples, and are provided for reference.

<b>Configuration</b>	<b>Write Throughput Gbps</b>	<b>Read from Cache Throughput Gbps</b>	<b>Read from Amazon Web Services Cloud Throughput Gbps</b>
Host Platform: Amazon EC2 instance— c5.4xlarge  Root disk: 80 GB, io1 SSD, 4000 IOPs  Cache disk: 50 GB, io1 SSD, 2000 IOPs  Upload buffer disk: 450 GB, io1 SSD, 2000 IOPs  CPU: 16 vCPU   RAM: 32 GB  Network bandwidth to cloud: 10 Gbps	2.3	4.0	1.7
Host platform: <a href="#">Storage Gateway Hardware Appliance</a>  Cache disk: 2.5 TB  Upload buffer disk: 2 TB  CPU: 20 cores   RAM: 128 GB  Network bandwidth to cloud: 10 Gbps	2.3	4.2	1.4
Host platform: Amazon EC2instance— c5d.9xlarge  Root disk: 80 GB, io1 SSD, 4000 IOPs  Cache disk: 900 GB NVMe disk  Upload buffer disk: 900 GB NVMe disk  CPU: 36 vCPU   RAM: 72 GB  Network bandwidth to cloud: 10 Gbps	5.2	8.2	2.0

**Note**

This performance was achieved by using a 1 MB block size and three tape drives simultaneously. Your performance might vary based on your host platform configuration and network bandwidth.

To improve write and read throughput performance of your tape gateway, see [Optimize iSCSI Settings \(p. 328\)](#), [Use a Larger Block Size for Tape Drives \(p. 328\)](#), and [Optimize the Performance of Virtual Tape Drives in the Backup Software \(p. 329\)](#).

# Optimizing Gateway Performance

You can find information following about how to optimize the performance of your gateway. The guidance is based on adding resources to your gateway and adding resources to your application server.

## Add Resources to Your Gateway

You can optimize gateway performance by adding resources to your gateway in one or more of the following ways.

### Use higher-performance disks

To optimize gateway performance, you can add high-performance disks such as solid-state drives (SSDs) and a NVMe controller. You can also attach virtual disks to your VM directly from a storage area network (SAN) instead of the Microsoft Hyper-V NTFS. Improved disk performance generally results in better throughput and more input/output operations per second (IOPS).

To measure throughput, use the `ReadBytes` and `WriteBytes` metrics with the `Samples` Amazon CloudWatch statistic. For example, the `Samples` statistic of the `ReadBytes` metric over a sample period of 5 minutes divided by 300 seconds gives you the IOPS. As a general rule, when you review these metrics for a gateway, look for low throughput and low IOPS trends to indicate disk-related bottlenecks. For more information about gateway metrics, see [Measuring Performance Between Your Tape Gateway and AWS \(p. 250\)](#).

#### Note

CloudWatch metrics are not available for all gateways. For information about gateway metrics, see [Monitoring Storage Gateway \(p. 215\)](#).

### Add CPU resources to your gateway host

The minimum requirement for a gateway host server is four virtual processors. To optimize gateway performance, confirm that the four virtual processors that are assigned to the gateway VM are backed by four cores. In addition, confirm that you are not oversubscribing the CPUs of the host server.

When you add additional CPUs to your gateway host server, you increase the processing capability of the gateway. Doing this allows your gateway to deal with, in parallel, both storing data from your application to your local storage and uploading this data to Amazon S3. Additional CPUs also help ensure that your gateway gets enough CPU resources when the host is shared with other VMs. Providing enough CPU resources has the general effect of improving throughput.

Storage Gateway supports using 24 CPUs in your gateway host server. You can use 24 CPUs to significantly improve the performance of your gateway. We recommend the following gateway configuration for your gateway host server:

- 24 CPUs.
- 16 GiB of reserved RAM for file gateways

For volume and tape gateways, your hardware should dedicate the following amounts of RAM:

- 16 GiB of reserved RAM for gateways with cache size up to 16 TiB
- 32 GiB of reserved RAM for gateways with cache size 16 TiB to 32 TiB
- 48 GiB of reserved RAM for gateways with cache size 32 TiB to 64 TiB
- Disk 1 attached to paravirtual controller 1, to be used as the gateway cache as follows:
  - SSD using an NVMe controller.
- Disk 2 attached to paravirtual controller 1, to be used as the gateway upload buffer as follows:
  - SSD using an NVMe controller.
- Disk 3 attached to paravirtual controller 2, to be used as the gateway upload buffer as follows:

- SSD using an NVMe controller.
- Network adapter 1 configured on VM network 1:
  - Use VM network 1 and add VMXnet3 (10 Gbps) to be used for ingestion.
- Network adapter 2 configured on VM network 2:
  - Use VM network 2 and add a VMXnet3 (10 Gbps) to be used to connect to AWS.

#### Back gateway virtual disks with separate physical disks

When you provision gateway disks, we strongly recommend that you don't provision local disks for the upload buffer and cache storage that use the same underlying physical storage disk. For example, for VMware ESXi, the underlying physical storage resources are represented as a data store. When you deploy the gateway VM, you choose a data store on which to store the VM files. When you provision a virtual disk (for example, as an upload buffer), you can store the virtual disk in the same data store as the VM or a different data store.

If you have more than one data store, then we strongly recommend that you choose one data store for each type of local storage you are creating. A data store that is backed by only one underlying physical disk can lead to poor performance. An example is when you use such a disk to back both the cache storage and upload buffer in a gateway setup. Similarly, a data store that is backed by a less high-performing RAID configuration such as RAID 1 can lead to poor performance.

#### Change the volumes configuration

For volume gateways, if you find that adding more volumes to a gateway reduces the throughput to the gateway, consider adding the volumes to a separate gateway. In particular, if a volume is used for a high-throughput application, consider creating a separate gateway for the high-throughput application. However, as a general rule, you should not use one gateway for all of your high-throughput applications and another gateway for all of your low-throughput applications. To measure your volume throughput, use the `ReadBytes` and `WriteBytes` metrics.

For more information about these metrics, see [Measuring Performance Between Your Application and Gateway \(p. 239\)](#).

## Optimize iSCSI Settings

You can optimize iSCSI settings on your iSCSI initiator to achieve higher I/O performance. We recommend choosing 256 KiB for `MaxReceiveDataSegmentLength` and `FirstBurstLength`, and 1 MiB for `MaxBurstLength`. For more information about configuring iSCSI settings, see [Customizing iSCSI Settings \(p. 424\)](#).

#### Note

These recommended settings can enable overall better performance. However, the specific iSCSI settings that are needed to optimize performance vary depending on which backup software you use. For details, see your backup software documentation.

## Use a Larger Block Size for Tape Drives

For a tape gateway, the default block size for a tape drive is 64 KB. However, you can increase the block size up to 1 MB to improve I/O performance.

The block size that you choose depends on the maximum block size that your backup software supports. We recommend that you set the block size of the tape drives in your backup software to a size that is as large as possible. However, this block size must not be greater than the 1 MB maximum size that the gateway supports.

Tape gateways negotiate the block size for virtual tape drives to automatically match what is set on the backup software. When you increase the block size on the backup software, we recommend that

you also check the settings to ensure that the host initiator supports the new block size. For more information, see the documentation for your backup software. For more information about specific gateway performance guidance, see [Performance \(p. 323\)](#).

## Optimize the Performance of Virtual Tape Drives in the Backup Software

Your backup software can back up data on up to 10 virtual tape drives on a tape gateway at the same time. We recommend that you configure backup jobs in your backup software to use at least 4 virtual tape drives simultaneous on the tape gateway. You can achieve better write throughput when the backup software is backing up data to more than one virtual tape at the same time.

## Add Resources to Your Application Environment

### Increase the bandwidth between your application server and your gateway

To optimize gateway performance, ensure that the network bandwidth between your application and the gateway can sustain your application needs. You can use the `ReadBytes` and `WriteBytes` metrics of the gateway to measure the total data throughput. For more information about these metrics, see [Measuring Performance Between Your Tape Gateway and AWS \(p. 250\)](#).

For your application, compare the measured throughput with the desired throughput. If the measured throughput is less than the desired throughput, then increasing the bandwidth between your application and gateway can improve performance if the network is the bottleneck. Similarly, you can increase the bandwidth between your VM and your local disks, if they're not direct-attached.

### Add CPU resources to your application environment

If your application can use additional CPU resources, then adding more CPUs can help your application to scale its I/O load.

## Using VMware vSphere High Availability with Storage Gateway

Storage Gateway provides high availability on VMware through a set of application-level health checks integrated with VMware vSphere High Availability (VMware HA). This approach helps protect storage workloads against hardware, hypervisor, or network failures. It also helps protect against software errors, such as connection timeouts and file share or volume unavailability.

With this integration, a gateway deployed in a VMware environment on-premises or in a VMware Cloud on AWS automatically recovers from most service interruptions. It generally does this in under 60 seconds with no data loss.

To use VMware HA with Storage Gateway, take the steps listed following.

### Topics

- [Configure Your vSphere VMware HA Cluster \(p. 330\)](#)
- [Download the .ova Image for Your Gateway Type \(p. 331\)](#)
- [Deploy the Gateway \(p. 331\)](#)
- [\(Optional\) Add Override Options for Other VMs on Your Cluster \(p. 331\)](#)
- [Activate Your Gateway \(p. 332\)](#)
- [Test Your VMware High Availability Configuration \(p. 332\)](#)

# Configure Your vSphere VMware HA Cluster

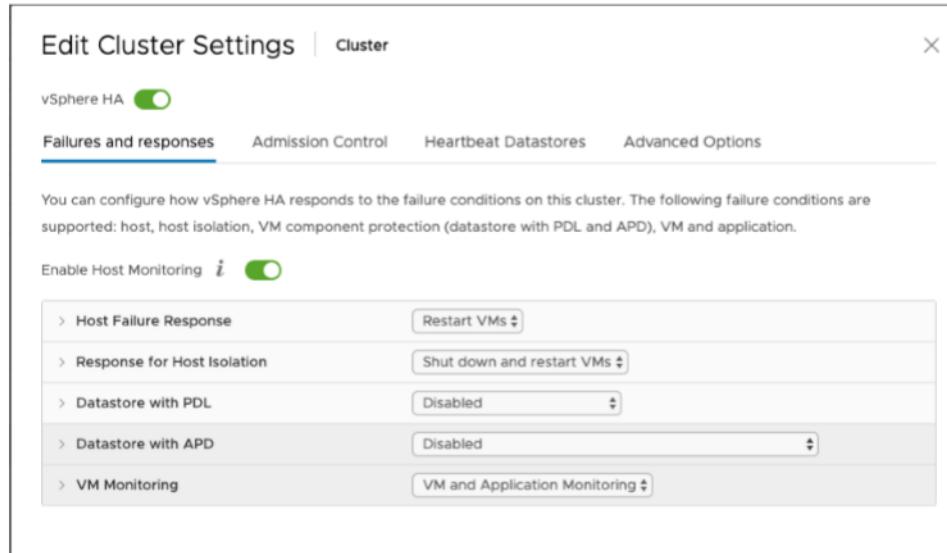
First, if you haven't already created a VMware cluster, create one. For information about how to create a VMware cluster, see [Create a vSphere HA Cluster](#) in the VMware documentation.

Next, configure your VMware cluster to work with Storage Gateway.

## To configure your VMware cluster

1. On the **Edit Cluster Settings** page in VMware vSphere, make sure that VM monitoring is configured for VM and application monitoring. To do so, set the following options as listed:
  - **Host Failure Response:** Restart VMs
  - **Response for Host Isolation:** Shut down and restart VMs
  - **Datastore with PDL:** Disabled
  - **Datastore with APD:** Disabled
  - **VM Monitoring:** VM and Application Monitoring

For an example, see the following screenshot.



2. Fine-tune the sensitivity of the cluster by adjusting the following values:
  - **Failure interval** – After this interval, the VM is restarted if a VM heartbeat isn't received.
  - **Minimum uptime** – The cluster waits this long after a VM starts to begin monitoring for VM tools' heartbeats.
  - **Maximum per-VM resets** – The cluster restarts the VM a maximum of this many times within the maximum resets time window.
  - **Maximum resets time window** – The window of time in which to count the maximum resets per-VM resets.

If you aren't sure what values to set, use these example settings:

- **Failure interval:** 30 seconds
- **Minimum uptime:** 120 seconds
- **Maximum per-VM resets:** 3

- **Maximum resets time window: 1 hour**

If you have other VMs running on the cluster, you might want to set these values specifically for your VM. You can't do this until you deploy the VM from the .ova. For more information on setting these values, see [\(Optional\) Add Override Options for Other VMs on Your Cluster \(p. 331\)](#).

## Download the .ova Image for Your Gateway Type

Use the following procedure to download the .ova image.

### To download the .ova image for your gateway type

- Download the .ova image for your gateway type from one of the following:
  - File gateway – [Creating a gateway \(p. 40\)](#)
  - Volume gateway – [Creating a Gateway \(p. 67\)](#)
  - Tape gateway – [Creating a Gateway \(p. 85\)](#)

## Deploy the Gateway

In your configured cluster, deploy the .ova image to one of the cluster's hosts.

### To deploy the gateway .ova image

1. Deploy the .ova image to one of the hosts in the cluster.
2. Make sure the data stores that you choose for the root disk and the cache are available to all hosts in the cluster.

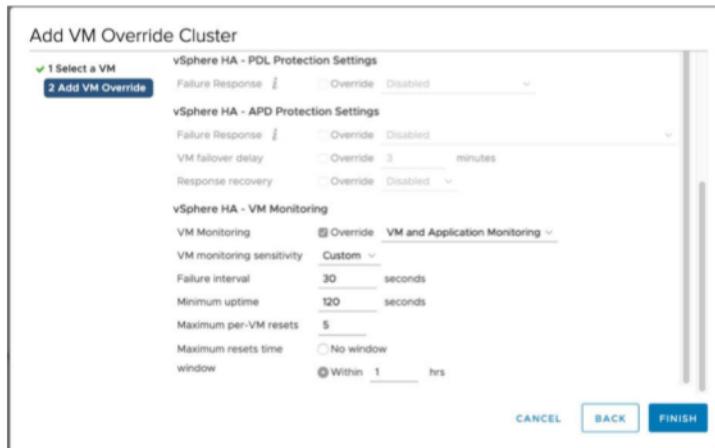
## (Optional) Add Override Options for Other VMs on Your Cluster

If you have other VMs running on your cluster, you might want to set the cluster values specifically for each VM.

### To add override options for other VMs on your cluster

1. On the **Summary** page in VMware vSphere, choose your cluster to open the cluster page, and then choose **Configure**.
2. Choose the **Configuration** tab, and then choose **VM Overrides**.
3. Add a new VM override option to change each value.

For override options, see the following screenshot.



## Activate Your Gateway

After the .ova for your gateway is deployed, activate your gateway. The instructions about how are different for each gateway type.

### To activate your gateway

- Choose activation instructions based on your gateway type:
  - File gateway – [Creating a gateway \(p. 40\)](#)
  - Volume gateway – [Creating a Gateway \(p. 67\)](#)
  - Tape gateway – [Creating a Gateway \(p. 85\)](#)

## Test Your VMware High Availability Configuration

After you activate your gateway, test your configuration.

### To test your VMware HA configuration

- Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
- On the navigation pane, choose **Gateways**, and then choose the gateway that you want to test for VMware HA.
- For **Actions**, choose **Verify VMware HA**.
- In the **Verify VMware High Availability Configuration** box that appears, choose **OK**.

#### Note

Testing your VMware HA configuration reboots your gateway VM and interrupts connectivity to your gateway. The test might take a few minutes to complete.

If the test is successful, the status of **Verified** appears in the details tab of the gateway in the console.

- Choose **Exit**.

You can find information about VMware HA events in the Amazon CloudWatch log groups. For more information, see [Getting file gateway health logs with CloudWatch Log Groups \(p. 225\)](#).

# Security in AWS Storage Gateway

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the Amazon Web Services Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](#). To learn about the compliance programs that apply to AWS Storage Gateway, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Storage Gateway. The following topics show you how to configure Storage Gateway to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Storage Gateway resources.

## Topics

- [Data protection in AWS Storage Gateway \(p. 333\)](#)
- [Authentication and Access Control for Storage Gateway \(p. 336\)](#)
- [Logging and Monitoring in AWS Storage Gateway \(p. 355\)](#)
- [Compliance validation for AWS Storage Gateway \(p. 357\)](#)
- [Resilience in AWS Storage Gateway \(p. 358\)](#)
- [Infrastructure Security in AWS Storage Gateway \(p. 358\)](#)
- [Security Best Practices for Storage Gateway \(p. 359\)](#)

## Data protection in AWS Storage Gateway

The AWS [shared responsibility model](#) applies to data protection in AWS Storage Gateway. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Storage Gateway or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

## Data encryption using AWS KMS

Storage Gateway uses SSL/TLS (Secure Socket Layers/Transport Layer Security) to encrypt data that is transferred between your gateway appliance and AWS storage. By default, Storage Gateway uses Amazon S3-Managed Encryption Keys (SSE-S3) to server-side encrypt all data it stores in Amazon S3. You have an option to use the Storage Gateway API to configure your gateway to encrypt data stored in the cloud using server-side encryption with AWS Key Management Service (SSE-KMS) customer master keys (CMKs).

### Important

When you use an AWS KMS CMK for server-side encryption, you must choose a symmetric CMK. Storage Gateway does not support asymmetric CMKs. For more information, see [Using symmetric and asymmetric keys in the AWS Key Management Service Developer Guide](#).

### Encrypting a file share

For a file share, you can configure your gateway to encrypt your objects with AWS KMS-managed keys by using SSE-KMS. For information on using the Storage Gateway API to encrypt data written to a file share, see [CreateNFSFileShare](#) in the *AWS Storage Gateway API Reference*.

### Encrypting a volume

For cached and stored volumes, you can configure your gateway to encrypt volume data stored in the cloud with AWS KMS-managed keys by using the Storage Gateway API. You can specify one of the managed customer master keys (CMKs) as the KMS key. The CMK that you use to encrypt your volume can't be changed after the volume is created. For information on using the Storage Gateway API to encrypt data written to a cached or stored volume, see [CreateCachediSCSIVolume](#) or [CreateStorediSCSIVolume](#) in the *AWS Storage Gateway API Reference*.

### Encrypting a tape

For a virtual tape, you can configure your gateway to encrypt tape data stored in the cloud with AWS KMS-managed keys by using the Storage Gateway API. You can specify one of the managed customer master keys (CMKs) as the KMS key. The CMK that you use to encrypt your tape data can't be changed after the tape is created. For information on using the Storage Gateway API to encrypt data written to a virtual tape, see [CreateTapes](#) in the *AWS Storage Gateway API Reference*.

When using AWS KMS to encrypt your data, keep the following in mind:

- Your data is encrypted at rest in the cloud. That is, the data is encrypted in Amazon S3.
- IAM users must have the required permissions to call the AWS KMS API operations. For more information, see [Using IAM policies with AWS KMS in the AWS Key Management Service Developer Guide](#).
- If you delete or disable your CMK or revoke the grant token, you can't access the data on the volume or tape. For more information, see [Deleting customer master keys in the AWS Key Management Service Developer Guide](#).

- If you create a snapshot from a volume that is KMS-encrypted, the snapshot is encrypted. The snapshot inherits the volume's KMS key.
- If you create a new volume from a snapshot that is KMS-encrypted, the volume is encrypted. You can specify a different KMS key for the new volume.

**Note**

Storage Gateway doesn't support creating an unencrypted volume from a recovery point of a KMS-encrypted volume or a KMS-encrypted snapshot.

For more information about AWS KMS, see [What is AWS Key Management Service?](#)

## Configuring CHAP authentication for your volumes

In Storage Gateway, your iSCSI initiators connect to your volumes as iSCSI targets. Storage Gateway uses Challenge-Handshake Authentication Protocol (CHAP) to authenticate iSCSI and initiator connections. CHAP provides protection against playback attacks by requiring authentication to access storage volume targets. For each volume target, you can define one or more CHAP credentials. You can view and edit these credentials for the different initiators in the Configure CHAP credentials dialog box.

### To configure CHAP credentials

1. In the Storage Gateway Console, choose **Volumes** and select the volume for which you want to configure CHAP credentials.
2. For **Actions**, choose **Configure CHAP authentication**.
3. For **Initiator name**, type the name of your initiator. The name must be at least 1 character and at most 255 characters long.
4. For **Initiator secret**, provide the secret phrase you want to used to authenticate your iSCSI initiator. The initiator secret phrase must be at least 12 characters and at most 16 characters long.
5. For **Target secret**, provide the secret phrase you want used to authenticate your target for mutual CHAP. The target secret phrase must be at least 12 characters and at most 16 characters long.
6. Choose **Save** to save your entries.

To view or update CHAP credentials, you must have the necessary IAM role permissions to that allows you to perform that operation.

## Viewing and editing CHAP credentials

You can add, remove or update CHAP credentials for each user. To view or edit CHAP credentials, you must have the necessary IAM role permissions that allows you to perform that operation and the gateway the initiator target is attached to must be a functioning gateway.

Initiator name	Initiator secret	Target secret
initiator2	.....	.....
initiator1	.....	.....

This volume accepts only connections from authenticated iSCSI initiators. [Learn more](#)

**Cancel** **Save**

### To add CHAP credentials

1. In the Storage Gateway Console, choose **Volumes** and select the volume for which you want to add CHAP credentials.
2. For **Actions**, choose **Configure CHAP authentication**.
3. In the Configure CHAPS page, provide the **Initiator name**, **Initiator secret**, and **Target secret** in the respective boxes and choose **Save**.

### To remove CHAP credentials

1. In the Storage Gateway Console, choose **Volumes** and select the volume for which you want to remove CHAP credentials.
2. For **Actions**, choose **Configure CHAP authentication**.
3. Click the **X** next to the credentials you want to remove and choose **Save**.

### To update CHAP credentials

1. In the Storage Gateway Console, choose **Volumes** and select the volume for which you want to update CHAP.
2. For **Actions**, choose **Configure CHAP authentication**.
3. In Configure CHAP credentials page, change the entries for the credentials you to update.
4. Choose **Save**.

## Authentication and Access Control for Storage Gateway

Access to AWS Storage Gateway requires credentials that AWS can use to authenticate your requests. Those credentials must have permissions to access AWS resources, such as a gateway, file share, volume, or tape. The following sections provide details on how you can use [AWS Identity and Access Management \(IAM\)](#) and Storage Gateway to help secure your resources by controlling who can access them:

- [Authentication \(p. 336\)](#)
- [Access Control \(p. 337\)](#)

## Authentication

You can access AWS as any of the following types of identities:

- **AWS account root user** – When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](#). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.
- **IAM user** – An [IAM user](#) is an identity within your AWS account that has specific custom permissions (for example, permissions to create a gateway in Storage Gateway). You can use an IAM user name and password to sign in to secure AWS webpages like the [AWS Management Console](#), [AWS Discussion Forums](#), or the [AWS Support Center](#).

In addition to a user name and password, you can also generate [access keys](#) for each user. You can use these keys when you access AWS services programmatically, either through [one of the several SDKs](#) or by using the [AWS Command Line Interface \(CLI\)](#). The SDK and CLI tools use the access keys to cryptographically sign your request. If you don't use AWS tools, you must sign the request yourself. Storage Gateway supports *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see [Signature Version 4 signing process](#) in the [AWS General Reference](#).

- **IAM role** – An [IAM role](#) is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session. IAM roles with temporary credentials are useful in the following situations:
  - **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an [identity provider](#). For more information about federated users, see [Federated users and roles](#) in the *IAM User Guide*.
  - **AWS service access** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
  - **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

## Access Control

You can have valid credentials to authenticate your requests, but unless you have permissions you cannot create or access Storage Gateway resources. For example, you must have permissions to create a gateway in Storage Gateway.

The following sections describe how to manage permissions for Storage Gateway. We recommend that you read the overview first.

- [Overview of Managing Access Permissions to Your Storage Gateway \(p. 338\)](#)
- [Identity-Based Policies \(IAM Policies\) \(p. 339\)](#)

# Overview of Managing Access Permissions to Your Storage Gateway

Every AWS resource is owned by an Amazon Web Services account, and permissions to create or access a resource are governed by permissions policies. An account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles), and some services (such as AWS Lambda) also support attaching permissions policies to resources.

## Note

An *account administrator* (or administrator user) is a user with administrator privileges. For more information, see [IAM Best Practices](#) in the *IAM User Guide*.

When granting permissions, you decide who is getting the permissions, the resources they get permissions for, and the specific actions that you want to allow on those resources.

## Topics

- [Storage Gateway Resources and Operations \(p. 338\)](#)
- [Understanding Resource Ownership \(p. 339\)](#)
- [Managing Access to Resources \(p. 339\)](#)
- [Specifying Policy Elements: Actions, Effects, Resources, and Principals \(p. 340\)](#)
- [Specifying Conditions in a Policy \(p. 341\)](#)

## Storage Gateway Resources and Operations

In Storage Gateway, the primary resource is a *gateway*. Storage Gateway also supports the following additional resource types: file share, volume, virtual tape, iSCSI target, and virtual tape library (VTL) device. These are referred to as *subresources* and they don't exist unless they are associated with a gateway.

These resources and subresources have unique Amazon Resource Names (ARNs) associated with them as shown in the following table.

Resource Type	ARN Format
Gateway ARN	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:gateway/<i>gateway-id</i></code>
File Share ARN	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:share/<i>share-id</i></code>
Volume ARN	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:gateway/<i>gateway-id</i>/volume/<i>volume-id</i></code>
Tape ARN	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:tape/<i>tapebarcode</i></code>
Target ARN (iSCSI target)	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:gateway/<i>gateway-id</i>/target/<i>iSCSITarget</i></code>
VTL Device ARN	<code>arn:aws:storagegateway:<i>region</i>:<i>account-id</i>:gateway/<i>gateway-id</i>/device/<i>vtddevice</i></code>

## Note

Storage Gateway resource IDs are in uppercase. When you use these resource IDs with the Amazon EC2 API, Amazon EC2 expects resource IDs in lowercase. You must change your resource

ID to lowercase to use it with the EC2 API. For example, in Storage Gateway the ID for a volume might be `vol-1122AABB`. When you use this ID with the EC2 API, you must change it to `vol-1122aabb`. Otherwise, the EC2 API might not behave as expected.

ARNs for gateways activated prior to September 2, 2015, contain the gateway name instead of the gateway ID. To obtain the ARN for your gateway, use the `DescribeGatewayInformation` API operation.

To grant permissions for specific API operations, such as creating a tape, Storage Gateway defines a set of actions that you can specify in a permissions policy to grant permissions for specific API operations. An API operation can require permissions for more than one action. For a table showing all the Storage Gateway API actions and the resources they apply to, see [Storage Gateway API Permissions: Actions, Resources, and Conditions Reference \(p. 349\)](#).

## Understanding Resource Ownership

A *resource owner* is the Amazon Web Services account that created the resource. That is, the resource owner is the Amazon Web Services account of the *principal entity* (the root account, an IAM user, or an IAM role) that authenticates the request that creates the resource. The following examples illustrate how this works:

- If you use the root account credentials of your Amazon Web Services account to activate a gateway, your Amazon Web Services account is the owner of the resource (in Storage Gateway, the resource is the gateway).
- If you create an IAM user in your Amazon Web Services account and grant permissions to the `ActivateGateway` action to that user, the user can activate a gateway. However, your Amazon Web Services account, to which the user belongs, owns the gateway resource.
- If you create an IAM role in your Amazon Web Services account with permissions to activate a gateway, anyone who can assume the role can activate a gateway. Your Amazon Web Services account, to which the role belongs, owns the gateway resource.

## Managing Access to Resources

A permissions policy describes who has access to what. The following section explains the available options for creating permissions policies.

### Note

This section discusses using IAM in the context of Storage Gateway. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see [What is IAM](#) in the *IAM User Guide*. For information about IAM policy syntax and descriptions, see [AWS IAM Policy Reference](#) in the *IAM User Guide*.

Policies attached to an IAM identity are referred to as *identity-based* policies (IAM policies) and policies attached to a resource are referred to as *resource-based* policies. Storage Gateway supports only identity-based policies (IAM policies).

### Topics

- [Identity-Based Policies \(IAM Policies\) \(p. 339\)](#)
- [Resource-Based Policies \(p. 340\)](#)

## Identity-Based Policies (IAM Policies)

You can attach policies to IAM identities. For example, you can do the following:

- **Attach a permissions policy to a user or a group in your account** – An account administrator can use a permissions policy that is associated with a particular user to grant permissions for that user to create an Storage Gateway resource, such as a gateway, volume, or tape.
- **Attach a permissions policy to a role (grant cross-account permissions)** – You can attach an identity-based permissions policy to an IAM role to grant cross-account permissions. For example, the administrator in Account A can create a role to grant cross-account permissions to another Amazon Web Services account (for example, Account B) or an AWS service as follows:
  1. Account A administrator creates an IAM role and attaches a permissions policy to the role that grants permissions on resources in Account A.
  2. Account A administrator attaches a trust policy to the role identifying Account B as the principal who can assume the role.
  3. Account B administrator can then delegate permissions to assume the role to any users in Account B. Doing this allows users in Account B to create or access resources in Account A. The principal in the trust policy can also be an AWS service principal if you want to grant an AWS service permissions to assume the role.

For more information about using IAM to delegate permissions, see [Access Management](#) in the *IAM User Guide*.

The following is an example policy that grants permissions to all `List*` actions on all resources. This action is a read-only action. Thus, the policy doesn't allow the user to change the state of the resources.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAllListActionsOnAllResources",  
            "Effect": "Allow",  
            "Action": [  
                "storagegateway>List*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

For more information about using identity-based policies with Storage Gateway, see [Using Identity-Based Policies \(IAM Policies\) for Storage Gateway \(p. 341\)](#). For more information about users, groups, roles, and permissions, see [Identities \(Users, Groups, and Roles](#) in the *IAM User Guide*.

## Resource-Based Policies

Other services, such as Amazon S3, also support resource-based permissions policies. For example, you can attach a policy to an S3 bucket to manage access permissions to that bucket. Storage Gateway doesn't support resource-based policies.

## Specifying Policy Elements: Actions, Effects, Resources, and Principals

For each Storage Gateway resource (see [Storage Gateway API Permissions: Actions, Resources, and Conditions Reference \(p. 349\)](#)), the service defines a set of API operations (see [Actions](#)). To grant permissions for these API operations, Storage Gateway defines a set of actions that you can specify in a policy. For example, for the Storage Gateway gateway resource, the following actions are defined: `ActivateGateway`, `DeleteGateway`, and `DescribeGatewayInformation`. Note that, performing an API operation can require permissions for more than one action.

The following are the most basic policy elements:

- **Resource** – In a policy, you use an Amazon Resource Name (ARN) to identify the resource to which the policy applies. For Storage Gateway resources, you always use the wildcard character (\*) in IAM policies. For more information, see [Storage Gateway Resources and Operations \(p. 338\)](#).
- **Action** – You use action keywords to identify resource operations that you want to allow or deny. For example, depending on the specified Effect, the storagegateway:ActivateGateway permission allows or denies the user permissions to perform the Storage Gateway ActivateGateway operation.
- **Effect** – You specify the effect when the user requests the specific action—this can be either allow or deny. If you don't explicitly grant access to (allow) a resource, access is implicitly denied. You can also explicitly deny access to a resource, which you might do to make sure that a user cannot access it, even if a different policy grants access.
- **Principal** – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal. For resource-based policies, you specify the user, account, service, or other entity that you want to receive permissions (applies to resource-based policies only). Storage Gateway doesn't support resource-based policies.

To learn more about IAM policy syntax and descriptions, see [AWS IAM Policy Reference](#) in the *IAM User Guide*.

For a table showing all of the Storage Gateway API actions, see [Storage Gateway API Permissions: Actions, Resources, and Conditions Reference \(p. 349\)](#).

## Specifying Conditions in a Policy

When you grant permissions, you can use the IAM policy language to specify the conditions when a policy should take effect when granting permissions. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy language, see [Condition](#) in the *IAM User Guide*.

To express conditions, you use predefined condition keys. There are no condition keys specific to Storage Gateway. However, there are AWS-wide condition keys that you can use as appropriate. For a complete list of AWS-wide keys, see [Available Keys](#) in the *IAM User Guide*.

## Using Identity-Based Policies (IAM Policies) for Storage Gateway

This topic provides examples of identity-based policies in which an account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles).

### Important

We recommend that you first review the introductory topics that explain the basic concepts and options available for you to manage access to your Storage Gateway resources. For more information, see [Overview of Managing Access Permissions to Your Storage Gateway \(p. 338\)](#).

The sections in this topic cover the following:

- [Permissions Required to Use the Storage Gateway Console \(p. 342\)](#)
- [AWS Managed Policies for Storage Gateway \(p. 343\)](#)
- [Customer Managed Policy Examples \(p. 343\)](#)

The following shows an example of a permissions policy.

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

```
{
    "Sid": "AllowsSpecifiedActionsOnAllGateways",
    "Effect": "Allow",
    "Action": [
        "storagegateway:ActivateGateway",
        "storagegateway>ListGateways"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeSnapshots",
        "ec2>DeleteSnapshot"
    ],
    "Resource": "*"
}
]
```

The policy has two statements (note the `Action` and `Resource` elements in both the statements):

- The first statement grants permissions for two Storage Gateway actions (`storagegateway:ActivateGateway` and `storagegateway>ListGateways`) on a gateway resource.

The wildcard character (\*) means that this statement can match any resource. In this case, the statement allows the `storagegateway:ActivateGateway` and `storagegateway>ListGateways` actions on any gateway. The wildcard character is used here because you don't know the resource ID until after you create the gateway. For information about how to use a wildcard character (\*) in a policy, see [Example 2: Allow Read-Only Access to a Gateway \(p. 344\)](#).

**Note**

ARNs uniquely identify AWS resources. For more information, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#) in the *AWS General Reference*.

To limit permissions for a particular action to a specific gateway only, create a separate statement for that action in the policy and specify the gateway ID in that statement.

- The second statement grants permissions for the `ec2:DescribeSnapshots` and `ec2>DeleteSnapshot` actions. These Amazon Elastic Compute Cloud (Amazon EC2) actions require permissions because snapshots generated from Storage Gateway are stored in Amazon Elastic Block Store (Amazon EBS) and managed as Amazon EC2 resources, and thus they require corresponding EC2 actions. For more information, see [Actions in the Amazon EC2 API Reference](#). Because these Amazon EC2 actions don't support resource-level permissions, the policy specifies the wildcard character (\*) as the `Resource` value instead of specifying a gateway ARN.

For a table showing all of the Storage Gateway API actions and the resources that they apply to, see [Storage Gateway API Permissions: Actions, Resources, and Conditions Reference \(p. 349\)](#).

## Permissions Required to Use the Storage Gateway Console

To use the Storage Gateway console, you need to grant read-only permissions. If you plan to describe snapshots, you also need to grant permissions for additional actions as shown in the following permissions policy:

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshots"
        ],
        "Resource": "*"
    }
]
```

This additional permission is required because the Amazon EBS snapshots generated from Storage Gateway are managed as Amazon EC2 resources.

To set up the minimum permissions required to navigate the Storage Gateway console, see [Example 2: Allow Read-Only Access to a Gateway \(p. 344\)](#).

## AWS Managed Policies for Storage Gateway

AWS addresses many common use cases by providing standalone IAM policies that are created and administered by AWS. Managed policies grant necessary permissions for common use cases so you can avoid having to investigate what permissions are needed. For more information about AWS managed policies, see [AWS Managed Policies](#) in the *IAM User Guide*.

The following AWS managed policies, which you can attach to users in your account, are specific to Storage Gateway:

- **AWSStorageGatewayReadOnlyAccess** – Grants read-only access to AWS Storage Gateway resources.
- **AWSStorageGatewayFullAccess** – Grants full access to AWS Storage Gateway resources.

### Note

You can review these permissions policies by signing in to the IAM console and searching for specific policies there.

You can also create your own custom IAM policies to allow permissions for AWS Storage Gateway API actions. You can attach these custom policies to the IAM users or groups that require those permissions.

## Customer Managed Policy Examples

In this section, you can find example user policies that grant permissions for various Storage Gateway actions. These policies work when you are using AWS SDKs and the AWS CLI. When you are using the console, you need to grant additional permissions specific to the console, which is discussed in [Permissions Required to Use the Storage Gateway Console \(p. 342\)](#).

### Note

All examples use the US West (Oregon) Region (`us-west-2`) and contain fictitious account IDs.

### Topics

- [Example 1: Allow Any Storage Gateway Actions on All Gateways \(p. 344\)](#)
- [Example 2: Allow Read-Only Access to a Gateway \(p. 344\)](#)
- [Example 3: Allow Access to a Specific Gateway \(p. 345\)](#)
- [Example 4: Allow a User to Access a Specific Volume \(p. 346\)](#)
- [Example 5: Allow All Actions on Gateways with a Specific Prefix \(p. 347\)](#)

## Example 1: Allow Any Storage Gateway Actions on All Gateways

The following policy allows a user to perform all the Storage Gateway actions. The policy also allows the user to perform Amazon EC2 actions ([DescribeSnapshots](#) and [DeleteSnapshot](#)) on the Amazon EBS snapshots generated from Storage Gateway.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowsAllAWSStorageGatewayActions",  
            "Action": [  
                "storagegateway:*"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        },  
        {  
            You can use Windows ACLs only with file shares that are enabled for Active  
            Directory.  
            "Sid": "AllowsSpecifiedEC2Actions",  
            "Action": [  
                "ec2:DescribeSnapshots",  
                "ec2:DeleteSnapshot"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

## Example 2: Allow Read-Only Access to a Gateway

The following policy allows all `List*` and `Describe*` actions on all resources. Note that these actions are read-only actions. Thus, the policy doesn't allow the user to change the state of any resources—that is, the policy doesn't allow the user to perform actions such as `DeleteGateway`, `ActivateGateway`, and `ShutdownGateway`.

The policy also allows the `DescribeSnapshots` Amazon EC2 action. For more information, see [DescribeSnapshots](#) in the *Amazon EC2 API Reference*.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowReadOnlyAccessToAllGateways",  
            "Action": [  
                "storagegateway>List*",  
                "storagegateway>Describe*"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        },  
        {  
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",  
            "Action": [  
                "ec2:DescribeSnapshots"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

In the preceding policy, instead of using a wildcard character (\*), you can scope resources covered by the policy to a specific gateway, as shown in the following example. The policy then allows the actions only on the specific gateway.

```
"Resource": [
    "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
    "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
]
```

Within a gateway, you can further restrict the scope of the resources to only the gateway volumes, as shown in the following example:

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/*"
```

### Example 3: Allow Access to a Specific Gateway

The following policy allows all actions on a specific gateway. The user is restricted from accessing other gateways you might have deployed.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway>List*",
                "storagegateway>Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2>DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:**"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

The preceding policy works if the user to which the policy is attached uses either the API or an AWS SDK to access the gateway. However, if the user is going to use the Storage Gateway console, you must also grant permissions to allow the `ListGateways` action, as shown in the following example:

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway>ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}

```

## Example 4: Allow a User to Access a Specific Volume

The following policy allows a user to perform all actions to a specific volume on a gateway. Because a user doesn't get any permissions by default, the policy restricts the user to accessing only a specific volume.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway>ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}

```

The preceding policy works if the user to whom the policy is attached uses either the API or an AWS SDK to access the volume. However, if this user is going to use the Storage Gateway console, you must also grant permissions to allow the `ListGateways` action, as shown in the following example:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {

```

```

    "Sid": "GrantsPermissionsToSpecificVolume",
    "Action": [
        "storagegateway:*"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
},
{
    "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
    "Action": [
        "storagegateway>ListGateways"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
}

```

### Example 5: Allow All Actions on Gateways with a Specific Prefix

The following policy allows a user to perform all Storage Gateway actions on gateways with names that start with `DeptX`. The policy also allows the `DescribeSnapshots` Amazon EC2 action which is required if you plan to describe snapshots.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}

```

The preceding policy works if the user to whom the policy is attached uses either the API or an AWS SDK to access the gateway. However, if this user plans to use the Storage Gateway console, you must grant additional permissions as described in [Example 3: Allow Access to a Specific Gateway \(p. 345\)](#).

## Using Microsoft Windows ACLs to Control Access to an SMB File Share

In this section, you can find information about how to use Microsoft Windows access control lists (ACLs) on SMB file shares enabled with Microsoft Active Directory (AD). By using Windows ACLs, you can set fine-grained permissions on files and folders in your SMB file share.

By default, file gateways support POSIX permissions to control access to files and directories that are stored through an NFS or SMB file share. For files and directories that are stored through SMB file shares,

file gateways enable you to use Windows ACLs instead of POSIX permissions to control access. This type of access control simulates Windows ACLs for native Windows file shares.

Following are some important characteristics of Windows ACLs on SMB file shares:

- By default, Windows ACLs on SMB file shares aren't enabled. To enable Windows ACLs, set the [SmbAclEnabled](#) option to `true` for your file share by using the [UpdateSMBFileShare](#) operation with the Storage Gateway SDK or the AWS CLI.
- When ACLs are enabled, the ACL information is persisted in Amazon S3 object metadata.
- The gateway preserves up to 10 ACLs per file or folder.
- When you use an SMB file share enabled with ACLs to access S3 objects created outside your gateway, the objects inherit ACLs' information from the parent folder.
- The default root ACL for an SMB file share gives full access to everyone, but you can change the permissions of the root ACL. You can use root ACLs to control access to the file share. You can set who can mount the file share (map the drive) and what permissions the user gets to the files and folders recursively in the file share. However, we recommend that you set this permission on the top-level folder in the S3 bucket so that your ACL is persisted.

You can enable Windows ACLs when you create a new SMB file share by using the [CreateSMBFileShare](#) API operation. Or you can enable Windows ACLs on an existing SMB file share by using the [UpdateSMBFileShare](#) API operation.

## Enabling Windows ACLs on a New SMB File Share

Take the following steps to enable Windows ACLs on a new SMB file share.

### To enable Windows ACLs when creating a new SMB file share

1. Create a file gateway if you don't already have one. For more information, see [Creating a file gateway \(p. 40\)](#).
2. If the gateway is not joined to a domain, add it to a domain. For more information, see [Using Active Directory to authenticate users \(p. 170\)](#).
3. Create an SMB file share. For more information, see [Creating a file share \(p. 46\)](#).
4. Enable Windows ACL on the file share from the Storage Gateway console.

To use the Storage Gateway Console, do the following:

- a. Choose the file share and choose **Edit file share**.
  - b. For the **File/directory access controlled by** option, choose **Windows Access Control List**.
5. (Optional) Add an admin user to the [AdminUsersList](#), if you want the admin user to have privileges to update ACLs on all files and folders in the file share.
  6. Update the ACLs for the parent folders under the root folder. To do this, use Windows File Explorer to configure the ACLs on the folders in the SMB file share.

#### Note

If you configure the ACLs on the root instead of the parent folder under root, the ACL permissions aren't persisted in Amazon S3.

We recommend setting ACLs at the top-level folder under the root of your file share, instead of setting ACLs directly at the root of the file share. This approach persists the information as object metadata in Amazon S3.

7. Enable inheritance as appropriate.

#### Note

You can enable inheritance for file shares created after May 8, 2019.

If you enable inheritance and update the permissions recursively, Storage Gateway updates all the objects in the S3 bucket. Depending on the number of objects in the bucket, the update can take a while to complete.

## Enabling Windows ACLs on an Existing SMB File Share

Take the following steps to enable Windows ACLs on an existing SMB file share that has POSIX permissions.

### To enable Windows ACLs on an existing SMB file share using the Storage Gateway Console

1. Choose the file share and choose **Edit file share**.
2. For the **File/directory access controlled by** option, choose **Windows Access Control List**.
3. Enable inheritance as appropriate.

**Note**

We don't recommend setting the ACLs at the root level, because if you do this and delete your gateway, you need to reset the ACLs again.

If you enable inheritance and update the permissions recursively, Storage Gateway updates all the objects in the S3 bucket. Depending on the number of objects in the bucket, the update can take a while to complete.

## Limitations When Using Windows ACLs

Keep the following limitations in mind when using Windows ACLs to control access to SMB file shares:

- Windows ACLs are only supported on file shares that are enabled for Active Directory when you use Windows SMB clients to access the file shares.
- File gateways support a maximum of 10 ACL entries for each file and directory.
- File gateways don't support Audit and Alarm entries, which are system access-control list (SACL) entries. File gateways support Allow and Deny entries, which are discretionary access control list (DACL) entries.
- The root ACL settings of SMB file shares are only on the gateway, and the settings are persisted across gateway updates and restarts.

**Note**

If you configure the ACLs on the root instead of the parent folder under the root, the ACL permissions aren't persisted in Amazon S3.

Given these conditions, make sure to do the following:

- If you configure multiple gateways to access the same Amazon S3 bucket, configure the root ACL on each of the gateways to keep the permissions consistent.
- If you delete a file share and recreate it on the same Amazon S3 bucket, make sure that you use the same set of root ACLs.

## Storage Gateway API Permissions: Actions, Resources, and Conditions Reference

When you set up [access control \(p. 337\)](#) and write permissions policies that you can attach to an IAM identity (identity-based policies), you can use the following table as a reference. The table lists each Storage Gateway API operation, the corresponding actions for which you can grant permissions to perform the action, and the AWS resource for which you can grant the permissions. You specify the actions in the policy's Action field, and you specify the resource value in the policy's Resource field.

You can use AWS-wide condition keys in your Storage Gateway policies to express conditions. For a complete list of AWS-wide keys, see [Available Keys](#) in the *IAM User Guide*.

**Note**

To specify an action, use the `storagegateway:` prefix followed by the API operation name (for example, `storagegateway:ActivateGateway`). For each Storage Gateway action, you can specify a wildcard character (\*) as the resource.

For a list of Storage Gateway resources with their ARN formats, see [Storage Gateway Resources and Operations \(p. 338\)](#).

**The Storage Gateway API and required permissions for actions are as follows.**

[ActivateGateway](#)

**Action(s):** `storagegateway:ActivateGateway`

**Resource:** \*

[AddCache](#)

**Action(s):** `storagegateway:AddCache`

**Resource:** `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[AddTagsToResource](#)

**Action(s):** `storagegateway:AddTagsToResource`

**Resource:** `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

or

`arn:aws:storagegateway:region:account-id:gateway/gateway-id/volume/volume-id`

or

`arn:aws:storagegateway:region:account-id:tape/tapebarcode`

[AddUploadBuffer](#)

**Action(s):** `storagegateway:AddUploadBuffer`

**Resource:** `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[AddWorkingStorage](#)

**Action(s):** `storagegateway:AddWorkingStorage`

**Resource:** `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[CancelArchival](#)

**Action(s):** `storagegateway:CancelArchival`

**Resource:** `arn:aws:storagegateway:region:account-id:tape/tapebarcode`

[CancelRetrieval](#)

**Action(s):** `storagegateway:CancelRetrieval`

**Resource:** `arn:aws:storagegateway:region:account-id:tape/tapebarcode`

[CreateCachediSCSIVolume](#)

**Action(s):** `storagegateway>CreateCachediSCSIVolume`

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**CreateSnapshot**

**Action(s):** storagegateway:CreateSnapshot

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
volume/*volume-id*

**CreateSnapshotFromVolumeRecoveryPoint**

**Action(s):** storagegateway:CreateSnapshotFromVolumeRecoveryPoint

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
volume/*volume-id*

**CreateStorediSCSIVolume**

**Action(s):** storagegateway:CreateStorediSCSIVolume

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**CreateTapes**

**Action(s):** storagegateway:CreateTapes

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**DeleteBandwidthRateLimit**

**Action(s):** storagegateway:DeleteBandwidthRateLimit

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**DeleteChapCredentials**

**Action(s):** storagegateway:DeleteChapCredentials

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
target/*iSCSITarget*

**DeleteGateway**

**Action(s):** storagegateway:DeleteGateway

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**DeleteSnapshotSchedule**

**Action(s):** storagegateway:DeleteSnapshotSchedule

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
volume/*volume-id*

**DeleteTape**

**Action(s):** storagegateway:DeleteTape

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
**DeleteTapeArchive**

**Action(s):** storagegateway:DeleteTapeArchive

**Resource:** \*

**DeleteVolume**

**Action(s):** storagegateway:DeleteVolume

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

DescribeBandwidthRateLimit

**Action(s):** storagegateway:DescribeBandwidthRateLimit

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

DescribeCache

**Action(s):** storagegateway:DescribeCache

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

DescribeCachediSCSIVolumes

**Action(s):** storagegateway:DescribeCachediSCSIVolumes

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

DescribeChapCredentials

**Action(s):** storagegateway:DescribeChapCredentials

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/target/iSCSITarget*

DescribeGatewayInformation

**Action(s):** storagegateway:DescribeGatewayInformation

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

DescribeMaintenanceStartTime

**Action(s):** storagegateway:DescribeMaintenanceStartTime

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

DescribeSnapshotSchedule

**Action(s):** storagegateway:DescribeSnapshotSchedule

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

DescribeStorediSCSIVolumes

**Action(s):** storagegateway:DescribeStorediSCSIVolumes

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

DescribeTapeArchives

**Action(s):** storagegateway:DescribeTapeArchives

**Resource:** \*

DescribeTapeRecoveryPoints

**Action(s):** storagegateway:DescribeTapeRecoveryPoints

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[DescribeTapes](#)

**Action(s):** storagegateway:DescribeTapes

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[DescribeUploadBuffer](#)

**Action(s):** storagegateway:DescribeUploadBuffer

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[DescribeVTLDevices](#)

**Action(s):** storagegateway:DescribeVTLDevices

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[DescribeWorkingStorage](#)

**Action(s):** storagegateway:DescribeWorkingStorage

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[DisableGateway](#)

**Action(s):** storagegateway:DisableGateway

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[ListGateways](#)

**Action(s):** storagegateway>ListGateways

**Resource:** \*

[ListLocalDisks](#)

**Action(s):** storagegateway>ListLocalDisks

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[ListTagsForResource](#)

**Action(s):** storagegateway>ListTagsForResource

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

or

arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

or

arn:aws:storagegateway:*region:account-id:tape/tapebarcode*

[ListTapes](#)

**Action(s):** storagegateway>ListTapes

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[ListVolumeInitiators](#)

**Action(s):** storagegateway>ListVolumeInitiators

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

[ListVolumeRecoveryPoints](#)

**Action(s):** storagegateway>ListVolumeRecoveryPoints

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*  
[ListVolumes](#)

**Action(s):** storagegateway>ListVolumes

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*  
[RemoveTagsFromResource](#)

**Action(s):** storagegateway>RemoveTagsFromResource

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

or

arn:aws:storagegateway:*region:account-id:gateway/gateway-id/volume/volume-id*

or

arn:aws:storagegateway:*region:account-id:tape/tapebarcode*

[ResetCache](#)

**Action(s):** storagegateway>ResetCache

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[RetrieveTapeArchive](#)

**Action(s):** storagegateway>RetrieveTapeArchive

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[RetrieveTapeRecoveryPoint](#)

**Action(s):** storagegateway>RetrieveTapeRecoveryPoint

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[ShutdownGateway](#)

**Action(s):** storagegateway>ShutdownGateway

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[StartGateway](#)

**Action(s):** storagegateway>StartGateway

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[UpdateBandwidthRateLimit](#)

**Action(s):** storagegateway>UpdateBandwidthRateLimit

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id*

[UpdateChapCredentials](#)

**Action(s):** storagegateway>UpdateChapCredentials

**Resource:** arn:aws:storagegateway:*region:account-id:gateway/gateway-id/target/*iSCSITarget**

### [UpdateGatewayInformation](#)

**Action(s):** storagegateway:UpdateGatewayInformation

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
[UpdateGatewaySoftwareNow](#)

**Action(s):** storagegateway:UpdateGatewaySoftwareNow

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
[UpdateMaintenanceStartTime](#)

**Action(s):** storagegateway:UpdateMaintenanceStartTime

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*  
[UpdateSnapshotSchedule](#)

**Action(s):** storagegateway:UpdateSnapshotSchedule

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
volume/*volume-id*

[UpdateVTLDeviceType](#)

**Action(s):** storagegateway:UpdateVTLDeviceType

**Resource:** arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/  
device/*vtdldevice*

### Related Topics

- [Access Control \(p. 337\)](#)
- [Customer Managed Policy Examples \(p. 343\)](#)

## Logging and Monitoring in AWS Storage Gateway

Storage Gateway is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Storage Gateway. CloudTrail captures all API calls for Storage Gateway as events. The calls captured include calls from the Storage Gateway console and code calls to the Storage Gateway API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Storage Gateway. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Storage Gateway, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

## Storage Gateway Information in CloudTrail

CloudTrail is enabled on your Amazon Web Services account when you create the account. When activity occurs in Storage Gateway, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your Amazon Web Services account. For more information, see [Viewing Events with CloudTrail Event History](#).

For an ongoing record of events in your Amazon Web Services account, including events for Storage Gateway, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from

all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for Creating a Trail](#)
- [CloudTrail Supported Services and Integrations](#)
- [Configuring Amazon SNS Notifications for CloudTrail](#)
- [Receiving CloudTrail Log Files from Multiple Regions](#) and [Receiving CloudTrail Log Files from Multiple Accounts](#)

All of the Storage Gateway actions are logged and are documented in the [Actions](#) topic. For example, calls to the `ActivateGateway`, `ListGateways`, and `ShutdownGateway` actions generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity Element](#).

## Understanding Storage Gateway Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the action.

```
{ "Records": [ { "eventVersion": "1.02", "userIdentity": { "type": "IAMUser", "principalId": "AIDAI5AUEPBH2M7JTNVC", "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe", "accountId": "111122223333", "accessKeyId": "AKIAIOSFODNN7EXAMPLE", "userName": "JohnDoe" }, "eventTime": "2014-12-04T16:19:00Z", "eventSource": "storagegateway.amazonaws.com", "eventName": "ActivateGateway", "awsRegion": "us-east-2", "sourceIPAddress": "192.0.2.0", "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5", "requestParameters": { "gatewayTimezone": "GMT-5:00", "gatewayName": "cloudtrailgatewayvtl", "gatewayRegion": "us-east-2", "activationKey": "EHBFBX-1NDD0-P0IVU-PI259-DHK88", "gatewayType": "VTL" } } ] }
```

```

        },
        "responseElements": {
            "gatewayARN": "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
        },
        "requestID": "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEUE3KPGG6F0KSTAUU0",
        "eventID": "635f2ea2-7e42-45f0-bed1-8b17d7b74265",
        "eventType": "AwsApiCall",
        "apiVersion": "20130630",
        "recipientAccountId": "444455556666"
    }
}

```

The following example shows a CloudTrail log entry that demonstrates the ListGateways action.

```

{
    "Records": [
        {
            "eventVersion": "1.02",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAI5AUEPBH2M7JTNVC",
                "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": "6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEUE3KPGG6F0KSTAUU0",
            "eventID": "f76e5919-9362-48ff-a7c4-d203a189ec8d",
            "eventType": "AwsApiCall",
            "apiVersion": "20130630",
            "recipientAccountId": "444455556666"
        }
    ]
}

```

## Compliance validation for AWS Storage Gateway

Third-party auditors assess the security and compliance of AWS Storage Gateway as part of multiple AWS compliance programs. These include SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR, and HITRUST CSF.

For a list of AWS services in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#). For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using Storage Gateway is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Evaluating resources with rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

## Resilience in AWS Storage Gateway

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

In addition to the AWS global infrastructure, Storage Gateway offers several features to help support your data resiliency and backup needs:

- Use VMware vSphere High Availability (VMware HA) to help protect storage workloads against hardware, hypervisor, or network failures. For more information, see [Using VMware vSphere High Availability with Storage Gateway \(p. 329\)](#).
- Use AWS Backup to back up your volumes. For more information, see [Backing Up Your Volumes \(p. 81\)](#).
- Clone your volume from a recovery point. For more information, see [Cloning a Volume \(p. 179\)](#).
- Archive virtual tapes in Amazon S3 Glacier. For more information, see [Archiving Virtual Tapes \(p. 202\)](#).

## Infrastructure Security in AWS Storage Gateway

As a managed service, AWS Storage Gateway is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access Storage Gateway through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

# Security Best Practices for Storage Gateway

AWS Storage Gateway provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions. For more information, see [AWS Security Best Practices](#).

# Troubleshooting your gateway

Following, you can find information about troubleshooting issues related to gateways, file shares, volumes, virtual tapes, and snapshots. The on-premises gateway troubleshooting information covers gateways deployed on both the VMware ESXi and Microsoft Hyper-V clients. The troubleshooting information for file shares applies to the file gateway type. The troubleshooting information for volumes applies to the volume gateway type. The troubleshooting information for tapes applies to the tape gateway type. The troubleshooting information for gateway issues applies to using CloudWatch metrics. The troubleshooting information for high availability issues covers gateways running on VMware vSphere High Availability (HA) platform.

## Topics

- [Troubleshooting on-premises gateway issues \(p. 360\)](#)
- [Troubleshooting Microsoft Hyper-V setup \(p. 364\)](#)
- [Troubleshooting Amazon EC2 gateway issues \(p. 366\)](#)
- [Troubleshooting hardware appliance issues \(p. 369\)](#)
- [Troubleshooting file gateway issues \(p. 371\)](#)
- [Troubleshooting file share issues \(p. 375\)](#)
- [Troubleshooting volume issues \(p. 379\)](#)
- [Troubleshooting virtual tape issues \(p. 383\)](#)
- [Troubleshooting high availability issues \(p. 386\)](#)
- [Best practices for recovering your data \(p. 388\)](#)

## Troubleshooting on-premises gateway issues

You can find information following about typical issues that you might encounter working with your on-premises gateways, and how to enable AWS Support to help troubleshoot your gateway.

The following table lists typical issues that you might encounter working with your on-premises gateways.

Issue	Action to Take
You cannot find the IP address of your gateway.	<p>Use the hypervisor client to connect to your host to find the gateway IP address.</p> <ul style="list-style-type: none"><li>• For VMware ESXi, the VM's IP address can be found in the vSphere client on the <b>Summary</b> tab. For more information, see <a href="#">Activating Your Gateway (p. 88)</a>.</li><li>• For Microsoft Hyper-V, the VM's IP address can be found by logging into the local console. For more information, see <a href="#">Activating Your Gateway (p. 88)</a>.</li></ul> <p>If you are still having trouble finding the gateway IP address:</p> <ul style="list-style-type: none"><li>• Check that the VM is turned on. Only when the VM is turned on does an IP address get assigned to your gateway.</li><li>• Wait for the VM to finish startup. If you just turned on your VM, then it might take several minutes for the gateway to finish its boot sequence.</li></ul>

Issue	Action to Take
You're having network or firewall problems.	<ul style="list-style-type: none"> <li>Allow the appropriate ports for your gateway.</li> <li>If you use a firewall or router to filter or limit network traffic, you must configure your firewall and router to allow these service endpoints for outbound communication to AWS. For more information about network and firewall requirements, see <a href="#">Network and firewall requirements (p. 13)</a>.</li> </ul>
Your gateway's activation fails when you click the <b>Proceed to Activation</b> button in the Storage Gateway Management Console.	<ul style="list-style-type: none"> <li>Check that the gateway VM can be accessed by pinging the VM from your client.</li> <li>Check that your VM has network connectivity to the internet. Otherwise, you'll need to configure a SOCKS proxy. For more information on doing so, see <a href="#">Routing Your On-Premises Gateway Through a Proxy (p. 290)</a>.</li> <li>Check that the host has the correct time, that the host is configured to synchronize its time automatically to a Network Time Protocol (NTP) server, and that the gateway VM has the correct time. For information about synchronizing the time of hypervisor hosts and VMs, see <a href="#">Synchronizing Your Gateway VM Time (p. 297)</a>.</li> <li>After performing these steps, you can retry the gateway deployment using the Storage Gateway console and the <b>Setup and Activate Gateway</b> wizard.</li> <li>Check that your VM has at least 7.5 GB of RAM. Gateway allocation fails if there is less than 7.5 GB of RAM. For more information, see <a href="#">Requirements (p. 11)</a>.</li> </ul>
You need to remove a disk allocated as upload buffer space. For example, you might want to reduce the amount of upload buffer space for a gateway, or you might need to replace a disk used as an upload buffer that has failed.	For instructions about removing a disk allocated as upload buffer space, see <a href="#">Volume Gateway (p. 404)</a> .
You need to improve bandwidth between your gateway and AWS.	You can improve the bandwidth from your gateway to AWS by setting up your internet connection to AWS on a network adapter (NIC) separate from that connecting your applications and the gateway VM. Taking this approach is useful if you have a high-bandwidth connection to AWS and you want to avoid bandwidth contention, especially during a snapshot restore. For high-throughput workload needs, you can use <a href="#">AWS Direct Connect</a> to establish a dedicated network connection between your on-premises gateway and AWS. To measure the bandwidth of the connection from your gateway to AWS, use the CloudBytesDownloaded and CloudBytesUploaded metrics of the gateway. For more on this subject, see <a href="#">Measuring Performance Between Your Gateway and AWS (p. 241)</a> . Improving your internet connectivity helps to ensure that your upload buffer does not fill up.

Issue	Action to Take
Throughput to or from your gateway drops to zero.	<ul style="list-style-type: none"> <li>On the <b>Gateway</b> tab of the Storage Gateway console, verify that the IP addresses for your gateway VM are the same that you see using your hypervisor client software (that is, the VMware vSphere client or Microsoft Hyper-V Manager). If you find a mismatch, restart your gateway from the Storage Gateway console, as shown in <a href="#">Shutting Down Your Gateway VM (p. 253)</a>. After the restart, the addresses in the <b>IP Addresses</b> list in the Storage Gateway console's <b>Gateway</b> tab should match the IP addresses for your gateway, which you determine from the hypervisor client.           <ul style="list-style-type: none"> <li>For VMware ESXi, the VM's IP address can be found in the vSphere client on the <b>Summary</b> tab. For more information, see <a href="#">Activating Your Gateway (p. 88)</a>.</li> <li>For Microsoft Hyper-V, the VM's IP address can be found by logging into the local console. For more information, see <a href="#">Activating Your Gateway (p. 88)</a>.</li> </ul> </li> <li>Check your gateway's connectivity to AWS as described in <a href="#">Testing Your Gateway Connection to the Internet (p. 296)</a>.</li> <li>Check your gateway's network adapter configuration, and ensure that all the interfaces you intended to be enabled for the gateway are enabled. To view the network adapter configuration for your gateway, follow the instructions in <a href="#">Configuring Your Gateway Network (p. 293)</a> and select the option for viewing your gateway's network configuration.</li> </ul> <p>You can view the throughput to and from your gateway from the Amazon CloudWatch console. For more information about measuring throughput to and from your gateway to AWS, see <a href="#">Measuring Performance Between Your Gateway and AWS (p. 241)</a>.</p>
You are having trouble importing (deploying) Storage Gateway on Microsoft Hyper-V.	See <a href="#">Troubleshooting Microsoft Hyper-V setup (p. 364)</a> , which discusses some of the common issues of deploying a gateway on Microsoft Hyper-V.
You receive a message that says: "The data that has been written to the volume in your gateway isn't securely stored at AWS".	You receive this message if your gateway VM was created from a clone or snapshot of another gateway VM. If this isn't the case, contact AWS Support.

## Enabling AWS Support to help troubleshoot your gateway hosted on-premises

Storage Gateway provides a local console you can use to perform several maintenance tasks, including enabling AWS Support to access your gateway to assist you with troubleshooting gateway issues. By default, AWS Support access to your gateway is disabled. You enable this access through the host's local console. To give AWS Support access to your gateway, you first log in to the local console for the host, navigate to the storage gateway's console, and then connect to the support server.

## To enable AWS Support access to your gateway

1. Log in to your host's local console.
  - VMware ESXi – for more information, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - Microsoft Hyper-V – for more information, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).

The local console looks like the following.

```
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: _
```

2. At the prompt, enter **5** to open the AWS Support Channel console.
3. Enter **h** to open the **AVAILABLE COMMANDS** window.
4. Do one of the following:
  - If your gateway is using a public endpoint, in the **AVAILABLE COMMANDS** window, enter **open-support-channel** to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.
  - If your gateway is using a VPC endpoint, in the **AVAILABLE COMMANDS** window, enter **open-support-channel**. If your gateway is not activated, provide the VPC endpoint or IP address to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.

```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands
ip Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig View or configure network interfaces
iptables Administration tool for IPv4 packet filtering and NAT
save-iptables Persist IP tables
testconn Test network connectivity
man Display command manual pages
open-support-channel Connect to Storage Gateway Support
h Display available command list
exit Return to Storage Gateway Configuration menu
Gateway Console: open-support-channel
```

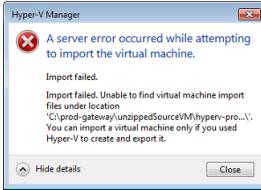
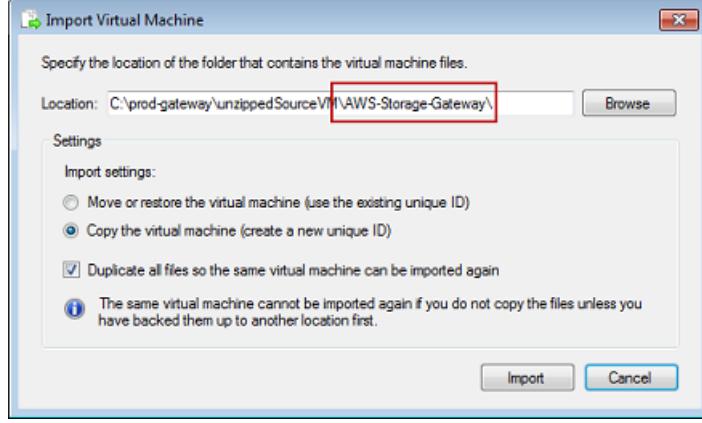
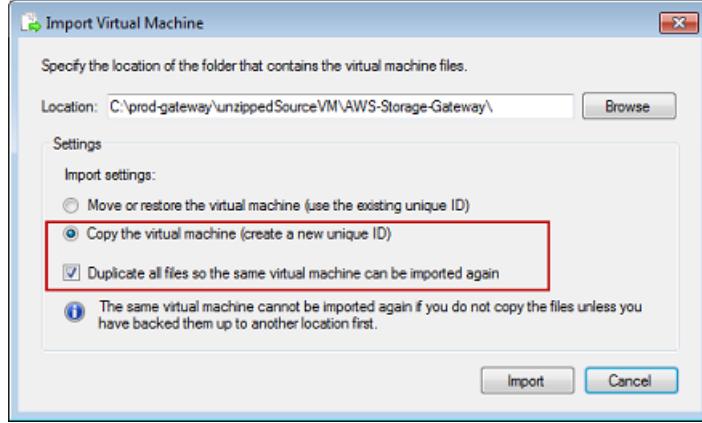
### Note

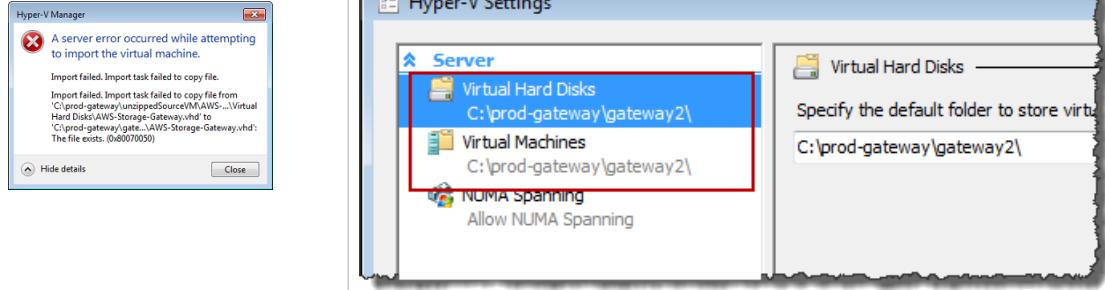
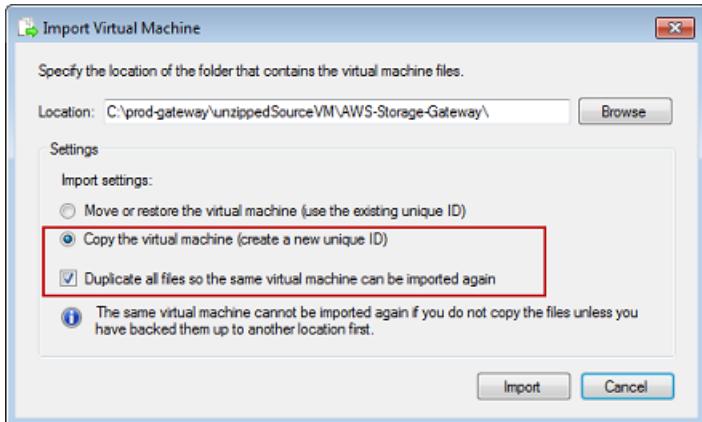
The channel number is not a Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number. Instead, the gateway makes a Secure Shell (SSH) (TCP 22) connection to Storage Gateway servers and provides the support channel for the connection.

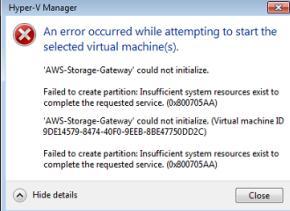
5. After the support channel is established, provide your support service number to AWS Support so AWS Support can provide troubleshooting assistance.
6. When the support session is completed, enter **q** to end it. Don't close the session until AWS Support notifies you that the support session is complete.
7. Enter **exit** to log out of the Storage Gateway console.
8. Follow the prompts to exit the local console.

# Troubleshooting Microsoft Hyper-V setup

The following table lists typical issues that you might encounter when deploying Storage Gateway on the Microsoft Hyper-V platform.

Issue	Action to Take
<p>You try to import a gateway and receive the error message: "Import failed. Unable to find virtual machine import file under location ...".</p> 	<p>This error can occur for the following reasons:</p> <ul style="list-style-type: none"> <li>If you are not pointing to the root of the unzipped gateway source files. The last part of the location you specify in the <b>Import Virtual Machine</b> dialog box should be AWS-Storage-Gateway, as the following example shows:</li> </ul> 
<p>You try to import a gateway and receive the error</p>	<p>If you have already deployed a gateway and you did not select the <b>Copy the virtual machine</b> option and check the <b>Duplicate all files</b> option in the <b>Import Virtual Machine</b> dialog box, then the VM was created in the location where you have the unzipped gateway files and you cannot import from this location again. To fix this problem, get a fresh copy of the unzipped gateway source files and copy to a new location. Use the new location as the source of the import. The following example shows the options that you must check if you plan on creating multiple gateways from one unzipped source files location.</p> 

Issue	Action to Take
message: "Import failed. Import task failed to copy file."	<p>configuration files, then this error will occur. To fix this problem, specify new locations in the <b>Hyper-V Settings</b> dialog box.</p> 
You try to import a gateway and receive an error message: "Import failed. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."	<p>When you import the gateway make sure you select the <b>Copy the virtual machine</b> option and check the <b>Duplicate all files</b> option in the <b>Import Virtual Machine</b> dialog box to create a new unique ID for the VM. The following example shows the options in the <b>Import Virtual Machine</b> dialog box that you should use.</p> 
You try to start a gateway VM and receive an error message "The child partition processor setting is incompatible with parent partition."	<p>This error is likely caused by a CPU discrepancy between the required CPUs for the gateway and the available CPUs on the host. Ensure that the VM CPU count is supported by the underlying hypervisor.</p> <p>For more information about the requirements for Storage Gateway, see <a href="#">Requirements (p. 11)</a>.</p> 

Issue	Action to Take
You try to start a gateway VM and receive an error message "Failed to create partition: Insufficient resources exist to complete the requested service."	<p>This error is likely caused by a RAM discrepancy between the required RAM for the gateway and the available RAM on the host.</p> <p>For more information about the requirements for Storage Gateway, see <a href="#">Requirements (p. 11)</a>.</p> 
Your snapshots and gateway software updates are occurring at slightly different times than expected.	The gateway VM's clock might be offset from the actual time, known as clock drift. Check and correct the VM's time using local gateway console's time synchronization option. For more information, see <a href="#">Synchronizing Your Gateway VM Time (p. 297)</a> .
You need to put the unzipped Microsoft Hyper-V Storage Gateway files on the host file system.	Access the host as you do a typical Microsoft Windows server. For example, if the hypervisor host is name <code>hyperv-server</code> , then you can use the following UNC path <code>\hyperv-server\c\$</code> , which assumes that the name <code>hyperv-server</code> can be resolved or is defined in your local hosts file.
You are prompted for credentials when connecting to hypervisor.	Add your user credentials as a local administrator for the hypervisor host by using the <code>Sconfig.cmd</code> tool.

## Troubleshooting Amazon EC2 gateway issues

In the following sections, you can find typical issues that you might encounter working with your gateway deployed on Amazon EC2. For more information about the difference between an on-premises gateway and a gateway deployed in Amazon EC2, see [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#). For information about using ephemeral storage, see [Using ephemeral storage with EC2 gateways \(p. 257\)](#).

### Topics

- [Your gateway activation hasn't occurred after a few moments \(p. 367\)](#)
- [You can't find your EC2 gateway instance in the instance list \(p. 367\)](#)
- [You created an Amazon EBS volume but can't attach it to your EC2 gateway instance \(p. 367\)](#)
- [You can't attach an initiator to a volume target of your EC2 gateway \(p. 367\)](#)
- [You get a message that you have no disks available when you try to add storage volumes \(p. 368\)](#)

- You want to remove a disk allocated as upload buffer space to reduce upload buffer space (p. 368)
- Throughput to or from your EC2 gateway drops to zero (p. 368)
- You want AWS Support to help troubleshoot your EC2 gateway (p. 368)

## Your gateway activation hasn't occurred after a few moments

Check the following in the Amazon EC2 console:

- Port 80 is enabled in the security group that you associated with the instance. For more information about adding a security group rule, see [Adding a security group rule](#) in the *Amazon EC2 User Guide for Linux Instances*.
- The gateway instance is marked as running. In the Amazon EC2 console, the **State** value for the instance should be RUNNING.
- Make sure that your Amazon EC2 instance type meets the minimum requirements, as described in [Storage requirements \(p. 13\)](#).

After correcting the problem, try activating the gateway again. To do this, open the Storage Gateway console, choose **Deploy a new Gateway on Amazon EC2**, and re-enter the IP address of the instance.

## You can't find your EC2 gateway instance in the instance list

If you didn't give your instance a resource tag and you have many instances running, it can be hard to tell which instance you launched. In this case, you can take the following actions to find the gateway instance:

- Check the name of the Amazon Machine Image (AMI) on the **Description** tab of the instance. An instance based on the Storage Gateway AMI should start with the text **aws-storage-gateway-ami**.
- If you have several instances based on the Storage Gateway AMI, check the instance launch time to find the correct instance.

## You created an Amazon EBS volume but can't attach it to your EC2 gateway instance

Check that the Amazon EBS volume in question is in the same Availability Zone as the gateway instance. If there is a discrepancy in Availability Zones, create a new Amazon EBS volume in the same Availability Zone as your instance.

## You can't attach an initiator to a volume target of your EC2 gateway

Check that the security group that you launched the instance with includes a rule that allows the port that you are using for iSCSI access. The port is usually set as 3260. For more information on connecting to volumes, see [Connecting to Your Volumes to a Windows Client \(p. 415\)](#).

## You get a message that you have no disks available when you try to add storage volumes

For a newly activated gateway, no volume storage is defined. Before you can define volume storage, you must allocate local disks to the gateway to use as an upload buffer and cache storage. For a gateway deployed to Amazon EC2, the local disks are Amazon EBS volumes attached to the instance. This error message likely occurs because no Amazon EBS volumes are defined for the instance.

Check block devices defined for the instance that is running the gateway. If there are only two block devices (the default devices that come with the AMI), then you should add storage. For more information on doing so, see [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#). After attaching two or more Amazon EBS volumes, try creating volume storage on the gateway.

## You want to remove a disk allocated as upload buffer space to reduce upload buffer space

Follow the steps in [Determining the size of upload buffer to allocate \(p. 255\)](#).

## Throughput to or from your EC2 gateway drops to zero

Verify that the gateway instance is running. If the instance is starting due to a reboot, for example, wait for the instance to restart.

Also, verify that the gateway IP has not changed. If the instance was stopped and then restarted, the IP address of the instance might have changed. In this case, you need to activate a new gateway.

You can view the throughput to and from your gateway from the Amazon CloudWatch console. For more information about measuring throughput to and from your gateway to AWS, see [Measuring Performance Between Your Gateway and AWS \(p. 241\)](#).

## You want AWS Support to help troubleshoot your EC2 gateway

Storage Gateway provides a local console you can use to perform several maintenance tasks, including enabling AWS Support to access your gateway to assist you with troubleshooting gateway issues. By default, AWS Support access to your gateway is disabled. You enable this access through the Amazon EC2 local console. You log in to the Amazon EC2 local console through a Secure Shell (SSH). To successfully log in through SSH, your instance's security group must have a rule that opens TCP port 22.

### Note

If you add a new rule to an existing security group, the new rule applies to all instances that use that security group. For more information about security groups and how to add a security group rule, see [Amazon EC2 security groups](#) in the *Amazon EC2 User Guide*.

To let AWS Support connect to your gateway, you first log in to the local console for the Amazon EC2 instance, navigate to the storage gateway's console, and then provide the access.

### To enable AWS Support access to a gateway deployed on an Amazon EC2 instance

1. Log in to the local console for your Amazon EC2 instance. For instructions, go to [Connect to your instance](#) in the *Amazon EC2 User Guide*.

You can use the following command to log in to the EC2 instance's local console.

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

**Note**

The **PRIVATE-KEY** is the .pem file containing the private certificate of the EC2 key pair that you used to launch the Amazon EC2 instance. For more information, see [Retrieving the public key for your key pair in the Amazon EC2 User Guide](#).

The **INSTANCE-PUBLIC-DNS-NAME** is the public Domain Name System (DNS) name of your Amazon EC2 instance that your gateway is running on. You obtain this public DNS name by selecting the Amazon EC2 instance in the EC2 console and clicking the **Description** tab.

2. At the prompt, enter **6 – Command Prompt** to open the AWS Support Channel console.
3. Enter **h** to open the **AVAILABLE COMMANDS** window.
4. Do one of the following:
  - If your gateway is using a public endpoint, in the **AVAILABLE COMMANDS** window, enter **open-support-channel** to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.
  - If your gateway is using a VPC endpoint, in the **AVAILABLE COMMANDS** window, enter **open-support-channel**. If your gateway is not activated, provide the VPC endpoint or IP address to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.

**Note**

The channel number is not a Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number. Instead, the gateway makes a Secure Shell (SSH) (TCP 22) connection to Storage Gateway servers and provides the support channel for the connection.

5. After the support channel is established, provide your support service number to AWS Support so AWS Support can provide troubleshooting assistance.
6. When the support session is completed, enter **q** to end it. Don't close the session until AWS Support notifies you that the support session is complete.
7. Enter **exit** to exit the Storage Gateway console.
8. Follow the console menus to log out of the Storage Gateway instance.

## Troubleshooting hardware appliance issues

The following topics discuss issues that you might encounter with the Storage Gateway Hardware Appliance, and suggestions on troubleshooting these.

### You can't determine the service IP address

When attempting to connect to your service, make sure that you are using the service's IP address and not the host IP address. Configure the service IP address in the service console, and the host IP address in the hardware console. You see the hardware console when you start the hardware appliance. To go to the service console from the hardware console, choose **Open Service Console**.

### How do you perform a factory reset?

If you need to perform a factory reset on your appliance, contact the Storage Gateway Hardware Appliance team for support, as described in the Support section following.

## Where do you obtain Dell iDRAC support?

The Dell PowerEdge R640 server comes with the Dell iDRAC management interface. We recommend the following:

- If you use the iDRAC management interface, you should change the default password. For more information about the iDRAC credentials, see [Dell PowerEdge - What is the default username and password for iDRAC?](#).
- Make sure that the firmware is up-to-date to prevent security breaches.
- Moving the iDRAC network interface to a normal (em) port can cause performance issues or prevent the normal functioning of the appliance.

## You can't find the hardware appliance serial number

To find the serial number of the hardware appliance, go to the **Hardware** page in the Storage Gateway console, as shown following.

The screenshot shows the AWS Storage Gateway console with the 'Hardware' tab selected. A success message at the top says 'Successfully launched File Gateway on praksuji-bh'. Below it is a table of hardware appliances. One row is highlighted for 'praksuji-bh' with the details: Name: praksuji-bh, ID: v15louei9yotyn5, Model: Dell PowerEdge R640, Launched Gateway: File Gateway. In the 'Details' section, the Serial Number is listed as 5Q8Y0M2, which is highlighted with a red box. Other columns include Vendor (Dell), Model (Dell PowerEdge R640), RAID Volume Manager (ZFS), and Time Zone (GMT).

## Where to obtain hardware appliance support

To contact the Storage Gateway Hardware Appliance support, see [AWS Support](#).

The AWS Support team might ask you to activate the support channel to troubleshoot your gateway issues remotely. You don't need this port to be open for the normal operation of your gateway, but it is required for troubleshooting. You can activate the support channel from the hardware console as shown in the procedure following.

### To open a support channel for AWS

1. Open the hardware console.
2. Choose **Open Support Channel** as shown following.



The assigned port number should appear within 30 seconds, if there are no network connectivity or firewall issues.

3. Note the port number and provide it to AWS Support.

## Troubleshooting file gateway issues

You can configure your file gateway with an Amazon CloudWatch log group when you run VMware vSphere High Availability (HA). If you do, you receive notifications about your file gateway's health status and about errors that the file gateway encounters. You can find information about these error and health notifications in CloudWatch Logs.

In the following sections, you can find information that can help you understand the cause of each error and health notification and how to fix issues.

### Topics

- [Error: InaccessibleStorageClass \(p. 371\)](#)
- [Error: S3AccessDenied \(p. 371\)](#)
- [Error: InvalidObjectState \(p. 372\)](#)
- [Error: ObjectMissing \(p. 372\)](#)
- [Notification: Reboot \(p. 372\)](#)
- [Notification: HardReboot \(p. 373\)](#)
- [Notification: HealthCheckFailure \(p. 373\)](#)
- [Notification: AvailabilityMonitorTest \(p. 373\)](#)
- [Error: RoleTrustRelationshipInvalid \(p. 373\)](#)
- [Troubleshooting with CloudWatch metrics \(p. 373\)](#)

## Error: InaccessibleStorageClass

You can get an `InaccessibleStorageClass` error when an object has moved out of the Amazon S3 Standard storage class.

Here, usually your file gateway encounters the error when it tries to either upload the specified object to S3 bucket or read the object from S3 bucket. With this error, generally the object has moved to Amazon S3 Glacier and is in either the S3 Glacier or S3 Glacier Deep Archive storage class.

### To resolve an `InaccessibleStorageClass` error

- Move the object from the S3 Glacier or S3 Glacier Deep Archive storage class back to S3.

If you move the object to the S3 bucket to fix an upload error, the file is eventually uploaded. If you move the object to the S3 bucket to fix a read error, the file gateway's SMB or NFS client can then read the file.

## Error: S3AccessDenied

You can get an `S3AccessDenied` error for a file share's Amazon S3 bucket access AWS Identity and Access Management (IAM) role. In this case, the S3 bucket access IAM role that is specified by `roleArn` in the error doesn't allow the operation involved. The operation isn't allowed because of the permissions for the objects in the directory specified by the Amazon S3 prefix.

### To resolve an `S3AccessDenied` error

- Modify the Amazon S3 access policy that is attached to `roleArn` in the file gateway health log to allow permissions for the Amazon S3 operation. Make sure that the access policy allows permission

for the operation that caused the error. Also, allow permission for the directory specified in the log for `prefix`. For information about Amazon S3 permissions, see [Specifying permissions in a policy](#) in *Amazon Simple Storage Service User Guide*.

These operations can cause an `S3AccessDenied` error to occur:

- `S3HeadObject`
- `S3GetObject`
- `S3ListObjects`
- `S3DeleteObject`
- `S3PutObject`

## Error: InvalidObjectState

You can get an `InvalidObjectState` error when a writer other than the specified file gateway modifies the specified file in the specified S3 bucket. As a result, the state of the file for the file gateway doesn't match its state in Amazon S3. Any subsequent uploads of the file to Amazon S3 or retrievals of the file from Amazon S3 fail.

### To resolve an InvalidObjectState error

If the operation that modifies the file is `S3Upload` or `S3GetObject`, do the following:

1. Save the latest copy of the file to the local file system of your SMB or NFS client (you need this file copy in step 4). If the version of the file in Amazon S3 is the latest, download that version. You can do this using the AWS Management Console or AWS CLI.
2. Delete the file in Amazon S3 using the AWS Management Console or AWS CLI.
3. Delete the file from the file gateway using your SMB or NFS client.
4. Copy the latest version of the file that you saved in step 1 to Amazon S3 using your SMB or NFS client. Do this through your file gateway.

## Error: ObjectMissing

You can get an `ObjectMissing` error when a writer other than the specified file gateway deletes the specified file from the S3 bucket. Any subsequent uploads to Amazon S3 or retrievals from Amazon S3 for the object fail.

### To resolve an ObjectMissing error

If the operation that modifies the file is `S3Upload` or `S3GetObject`, do the following:

1. Save the latest copy of the file to the local file system of your SMB or NFS client (you need this file copy in step 3).
2. Delete the file from the file gateway using your SMB or NFS client.
3. Copy the latest version of the file that you saved in step 1 using your SMB or NFS client. Do this through your file gateway.

## Notification: Reboot

You can get a reboot notification when the gateway VM is restarted. You can restart a gateway VM by using the VM Hypervisor Management console or the Storage Gateway console. You can also restart by using the gateway software during the gateway's maintenance cycle.

If the time of the reboot is within 10 minutes of the gateway's configured [maintenance start time \(p. 263\)](#), this reboot is probably a normal occurrence and not a sign of any problem. If the reboot occurred significantly outside the maintenance window, check whether the gateway was restarted manually.

## Notification: HardReboot

You can get a **HardReboot** notification when the gateway VM is restarted unexpectedly. Such a restart can be due to loss of power, a hardware failure, or another event. For VMware gateways, a reset by vSphere High Availability Application Monitoring can trigger this event.

When your gateway runs in such an environment, check for the presence of the **HealthCheckFailure** notification and consult the VMware events log for the VM.

## Notification: HealthCheckFailure

For a gateway on VMware vSphere HA, you can get a **HealthCheckFailure** notification when a health check fails and a VM restart is requested. This event also occurs during a test to monitor availability, indicated by an **AvailabilityMonitorTest** notification. In this case, the **HealthCheckFailure** notification is expected.

**Note**

This notification is for VMware gateways only.

If this event repeatedly occurs without an **AvailabilityMonitorTest** notification, check your VM infrastructure for issues (storage, memory, and so on). If you need additional assistance, contact AWS Support.

## Notification: AvailabilityMonitorTest

You get an **AvailabilityMonitorTest** notification when you [run a test \(p. 332\)](#) of the [Availability and application monitoring](#) system on gateways running on a VMware vSphere HA platform.

## Error: RoleTrustRelationshipInvalid

You get this error when the IAM role for a file share has a misconfigured IAM trust relationship (that is, the IAM role does not trust the Storage Gateway principal named `storagegateway.amazonaws.com`). As a result, the file gateway would not be able to get the credentials to run any operations on the S3 bucket that backs the file share.

**To resolve an `RoleTrustRelationshipInvalid` error**

- Use the IAM console or IAM API to include `storagegateway.amazonaws.com` as a principal that is trusted by your file share's IAMrole. For information about IAM role, see [Tutorial: delegate access across Amazon Web Services accounts using IAM roles](#).

## Troubleshooting with CloudWatch metrics

You can find information following about actions to address issues in using Amazon CloudWatch metrics with Storage Gateway.

**Topics**

- [Your gateway reacts slowly when browsing directories \(p. 374\)](#)
- [Your gateway isn't responding \(p. 374\)](#)
- [Your gateway is slow transferring data to Amazon S3 \(p. 374\)](#)

- Your gateway backup job fails or there are errors when writing to your gateway (p. 374)

## Your gateway reacts slowly when browsing directories

If your file gateway reacts slowly when you run the `ls` command or browse directories, check the `IndexFetch` and `IndexEviction` CloudWatch metrics:

- If the `IndexFetch` metric is greater than 0 when you run an `ls` command or browse directories, your file gateway started without information on the contents of the directory affected and had to access Amazon S3. Subsequent efforts to list the contents of that directory should go faster.
- If the `IndexEviction` metric is greater than 0, it means that your file gateway has reached the limit of what it can manage in its cache at that time. In this case, your file gateway has to free some storage space from the least recently accessed directory to list a new directory. If this occurs frequently and there is a performance impact, contact AWS Support. Discuss with AWS Support the contents of the related S3 bucket and recommendations to improve performance based on your use case.

## Your gateway isn't responding

If your file gateway isn't responding, do the following:

- If there was a recent reboot or software update, then check the `IOWaitPercent` metric. This metric shows the percentage of time that the CPU is idle when there is an outstanding disk I/O request. In some cases, this might be high (10 or greater) and might have risen after the server was rebooted or updated. In these cases, then your file gateway might be bottlenecked by a slow root disk as it rebuilds the index cache to RAM. You can address this issue by using a faster physical disk for the root disk.
- If the `MemUsedBytes` metric is at or nearly the same as the `MemTotalBytes` metric, then your file gateway is running out of available RAM. Make sure that your file gateway has at least the minimum required RAM. If it already does, consider adding more RAM to your file gateway based on your workload and use case.

If the file share is SMB, the issue might also be due to the number of SMB clients connected to the file share. To see the number of clients connected at any given time, check the `SMBV(1/2/3)Sessions` metric. If there are many clients connected, you might need to add more RAM to your file gateway.

## Your gateway is slow transferring data to Amazon S3

If your file gateway is slow transferring data to Amazon S3, do the following:

- If the `CachePercentDirty` metric is 80 or greater, your file gateway is writing data faster to disk than it can upload the data to Amazon S3. Consider increasing the bandwidth for upload from your file gateway, adding one or more cache disks, or slowing down client writes.
- If the `CachePercentDirty` metric is low, check the `IOWaitPercent` metric. If `IOWaitPercent` is greater than 10, your file gateway might be bottlenecked by the speed of the local cache disk. We recommend local solid state drive (SSD) disks for your cache, preferably NVMe Express (NVMe). If such disks aren't available, try using multiple cache disks from separate physical disks for a performance improvement.

## Your gateway backup job fails or there are errors when writing to your gateway

If your file gateway backup job fails or there are errors when writing to your file gateway, do the following:

- If the `CachePercentDirty` metric is 90 percent or greater, your file gateway can't accept new writes to disk because there is not enough available space on the cache disk. To see how fast your file gateway is uploading to Amazon S3, view the `CloudBytesUploaded` metric. Compare that metric with the `WriteBytes` metric, which shows how fast the client is writing files to your file gateway. If your file gateway is writing faster than it can upload to Amazon S3, add more cache disks to cover the size of the backup job at a minimum. Or, increase the upload bandwidth.
- If a backup job fails but the `CachePercentDirty` metric is less than 80 percent, your file gateway might be hitting a client-side session timeout. For SMB, you can increase this timeout using the PowerShell command `Set-SmbClientConfiguration -SessionTimeout 300`. Running this command sets the timeout to 300 seconds. For NFS, make sure that the client is mounted using a hard mount instead of a soft mount.

## Troubleshooting file share issues

You can find information following about actions to take if you experience unexpected issues with your file share.

### Topics

- [Your file share is stuck in CREATING status \(p. 375\)](#)
- [You can't create a file share \(p. 376\)](#)
- [SMB file shares don't allow multiple different access methods \(p. 376\)](#)
- [Multiple file shares can't write to the mapped S3 bucket \(p. 376\)](#)
- [Can't upload files into your S3 bucket \(p. 376\)](#)
- [Can't change the default encryption to use SSE-KMS to encrypt objects stored in my S3 bucket \(p. 376\)](#)
- [Changes made directly in an S3 bucket with object versioning enabled may affect what you see in your file share \(p. 377\)](#)
- [When writing to an S3 bucket with object versioning enabled, the file gateway may create multiple versions of an S3 object \(p. 377\)](#)
- [Changes to an S3 bucket are not reflected in Storage Gateway \(p. 378\)](#)
- [ACL permissions aren't working as expected \(p. 379\)](#)
- [Your gateway performance declined after you performed a recursive operation \(p. 379\)](#)

## Your file share is stuck in CREATING status

When your file share is being created, the status is CREATING. The status transitions to AVAILABLE status after the file share is created. If your file share gets stuck in the CREATING status, do the following:

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Make sure the S3 bucket that you mapped your file share to exists. If the bucket doesn't exist, create it. After you create the bucket, the file share status transitions to AVAILABLE. For information about how to create an S3 bucket, see [Create a bucket](#) in the *Amazon Simple Storage Service User Guide*.
3. Make sure your bucket name complies with the rules for bucket naming in Amazon S3. For more information, see [Rules for bucket naming](#) in the *Amazon Simple Storage Service User Guide*.
4. Make sure the IAM role you used to access the S3 bucket has the correct permissions and verify that the S3 bucket is listed as a resource in the IAM policy. For more information, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).

## You can't create a file share

1. If you can't create a file share because your file share is stuck in CREATING status, verify that the S3 bucket you mapped your file share to exists. For information on how to do so, see [Your file share is stuck in CREATING status \(p. 375\)](#), preceding.
2. If the S3 bucket exists, then verify that AWS Security Token Service is enabled in the region where you are creating the file share. If a security token is not enabled, you should enable it. For information about how to enable a token using AWS Security Token Service, see [Activating and deactivating AWS STS in an AWS Region](#) in the *IAM User Guide*.

## SMB file shares don't allow multiple different access methods

SMB file shares have the following restrictions:

1. When the same client attempts to mount both an Active Directory and Guest access SMB file share the following error message is displayed: **Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.**
2. A Windows client can't mount both a Guest Access and an Active Directory SMB file share that is exported by the same gateway.

## Multiple file shares can't write to the mapped S3 bucket

We don't recommend configuring your S3 bucket to allow multiple file shares to write to one S3 bucket. This approach can cause unpredictable results.

Instead, we recommend that you allow only one file share to write to each S3 bucket. You create a bucket policy to allow only the role associated with your file share to write to the bucket. For more information, see [File share best practices \(p. 176\)](#).

## Can't upload files into your S3 bucket

If you can't upload files into your S3 bucket, do the following:

1. Make sure you have granted the required access for the file gateway to upload files into your S3 bucket. For more information, see [Granting access to an Amazon S3 bucket \(p. 163\)](#).
2. Make sure the role that created the bucket has permission to write to the S3 bucket. For more information, see [File share best practices \(p. 176\)](#).

## Can't change the default encryption to use SSE-KMS to encrypt objects stored in my S3 bucket

If you change the default encryption and make SSE-KMS (server-side encryption with AWS KMS-managed keys) the default for your S3 bucket, objects that a file gateway stores in the bucket are not encrypted with SSE-KMS. By default, a file gateway uses server-side encryption managed with Amazon

S3 (SSE-S3) when it writes data to an S3 bucket. Changing the default won't automatically change your encryption.

To change the encryption to use SSE-KMS with your own AWS KMS key, you must enable SSE-KMS encryption. To do so, you provide the Amazon Resource Name (ARN) of the KMS key when you create your file share. You can also update KMS settings for your file share by using the [UpdateNFSFileShare](#) or [UpdateSMBFileShare](#) API operation. This update applies to objects stored in the S3 buckets after the update. For more information, see [Data encryption using AWS KMS \(p. 334\)](#).

## Changes made directly in an S3 bucket with object versioning enabled may affect what you see in your file share

If your S3 bucket has objects written to it by another client, your view of the S3 bucket might not be up-to-date as a result of S3 bucket object versioning. You should always refresh your cache before examining files of interest.

*Object versioning* is an optional S3 bucket feature that helps protect data by storing multiple copies of the same-named object. Each copy has a separate ID value, for example `file1.jpg: ID="xxx"` and `file1.jpg: ID="yyy"`. The number of identically named objects and their lifetimes is controlled by Amazon S3 lifecycle policies. For more details on these Amazon S3 concepts, see [Using versioning](#) and [Object lifecycle management](#) in the *Amazon S3 Developer Guide*.

When you delete a versioned object, that object is flagged with a delete marker but retained. Only an S3 bucket owner can permanently delete an object with versioning turned on.

In your file gateway, files shown are the most recent versions of objects in an S3 bucket at the time the object was fetched or the cache was refreshed. File gateways ignore any older versions or any objects marked for deletion. When reading a file, you read data from the latest version. When you write a file in your file share, your file gateway creates a new version of a named object with your changes, and that version becomes the latest version.

Your file gateway continues to read from the earlier version, and updates that you make are based on the earlier version should a new version be added to the S3 bucket outside of your application. To read the latest version of an object, use the [RefreshCache](#) API action or refresh from the console as described in [Refreshing objects in your Amazon S3 bucket \(p. 173\)](#).

**Important**

We don't recommend that objects or files be written to your file gateway S3 bucket from outside of the file share.

## When writing to an S3 bucket with object versioning enabled, the file gateway may create multiple versions of an S3 object

With object versioning enabled, you may have multiple versions of an object created in Amazon S3 on every update to a file from your NFS or SMB client. Here are scenarios that can result in multiple versions of an object being created in your S3 bucket:

- When a file is modified in the file gateway by an NFS or SMB client after it has been uploaded to Amazon S3, the file gateway uploads the new or modified data instead of uploading the whole file. The file modification results in a new version of the Amazon S3 object being created.
- When a file is written to the file gateway by an NFS or SMB client, the file gateway uploads the file's data to Amazon S3 followed by its metadata, (ownerships, timestamps, etc.). Uploading the file data

creates an Amazon S3 object, and uploading the metadata for the file updates the metadata for the Amazon S3 object. This process creates another version of the object, resulting in two versions of an object.

- When the file gateway is uploading larger files, it might need to upload smaller chunks of the file before the client is done writing to the file gateway. Some reasons for this include to free up cache space or a high rate of writes to a file. This can result in multiple versions of an object in the S3 bucket.

You should monitor your S3 bucket to determine how many versions of an object exist before setting up lifecycle policies to move objects to different storage classes. You should configure lifecycle expiration for previous versions to minimize the number of versions you have for an object in your S3 bucket. The use of Same-Region replication (SRR) or Cross-Region replication (CRR) between S3 buckets will increase the storage used. For more information about replication, see [Replication](#).

**Important**

Do not configure replication between S3 buckets until you understand how much storage is being used when object versioning is enabled.

Use of versioned S3 buckets can greatly increase the amount of storage in Amazon S3 because each modification to a file creates a new version of the S3 object. By default, Amazon S3 continues to store all of these versions unless you specifically create a policy to override this behavior and limit the number of versions that are kept. If you notice unusually large storage usage with object versioning enabled, check that you have your storage policies set appropriately. An increase in the number of HTTP 503-slow down responses for browser requests can also be the result of problems with object versioning.

If you enable object versioning after installing a file gateway, all unique objects are retained (`ID="NULL"`) and you can see them all in the file system. New versions of objects are assigned a unique ID (older versions are retained). Based on the object's timestamp only the newest versioned object is viewable in the NFS file system.

After you enable object versioning, your S3 bucket can't be returned to a nonversioned state. You can, however, suspend versioning. When you suspend versioning, a new object is assigned an ID. If the same named object exists with an `ID="NULL"` value, the older version is overwritten. However, any version that contains a non-`NULL` ID is retained. Timestamps identify the new object as the current one, and that is the one that appears in the NFS file system.

## Changes to an S3 bucket are not reflected in Storage Gateway

Storage Gateway updates the file share cache automatically when you write files to the cache locally using the file share. However, Storage Gateway doesn't automatically update the cache when you upload a file directly to Amazon S3. When you do this, you must perform a RefreshCache operation to see the changes on the file share. If you have more than one file share, then you must run the RefreshCache operation on each file share.

You can refresh the cache using the Storage Gateway console and the AWS Command Line Interface (AWS CLI):

- To refresh the cache using the Storage Gateway console, see Refreshing objects in your Amazon S3 bucket.
- To refresh the cache using the AWS CLI:
  1. Run the command `aws storagegateway list-file-shares`
  2. Copy the Amazon Resource Number (ARN) of the file share with the cache that you want to refresh.
  3. Run the `refresh-cache` command with your ARN as the value for `--file-share-arn`:

```
aws storagegateway refresh-cache --file-share-arn  
arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
```

To automate the RefreshCache operation, see [How can I automate the RefreshCache operation on Storage Gateway?](#)

## ACL permissions aren't working as expected

If access control list (ACL) permissions aren't working as you expect with your SMB file share, you can perform a test.

To do this, first test the permissions on a Microsoft Windows file server or a local Windows file share. Then compare the behavior to your gateway's file share.

## Your gateway performance declined after you performed a recursive operation

In some cases, you might perform a recursive operation, such as renaming a directory or enabling inheritance for an ACL, and force it down the tree. If you do this, your file gateway recursively applies the operation to all objects in the file share.

For example, suppose that you apply inheritance to existing objects in an S3 bucket. Your file gateway recursively applies inheritance to all objects in the bucket. Such operations can cause your gateway performance to decline.

## Troubleshooting volume issues

You can find information about the most typical issues you might encounter when working with volumes, and actions that we suggest that you take to fix them.

### Topics

- [The Console Says That Your Volume Is Not Configured \(p. 379\)](#)
- [The Console Says That Your Volume Is Irrecoverable \(p. 380\)](#)
- [Your Cached Gateway is Unreachable And You Want to Recover Your Data \(p. 380\)](#)
- [The Console Says That Your Volume Has PASS THROUGH Status \(p. 380\)](#)
- [You Want to Verify Volume Integrity and Fix Possible Errors \(p. 381\)](#)
- [Your Volume's iSCSI Target Doesn't Appear in Windows Disk Management Console \(p. 381\)](#)
- [You Want to Change Your Volume's iSCSI Target Name \(p. 381\)](#)
- [Your Scheduled Volume Snapshot Did Not Occur \(p. 381\)](#)
- [You Need to Remove or Replace a Disk That Has Failed \(p. 381\)](#)
- [Throughput from Your Application to a Volume Has Dropped to Zero \(p. 382\)](#)
- [A Cache Disk in Your Gateway Encounters a Failure \(p. 382\)](#)
- [A Volume Snapshot Has PENDING Status Longer Than Expected \(p. 382\)](#)
- [High Availability Health Notifications \(p. 383\)](#)

## The Console Says That Your Volume Is Not Configured

If the Storage Gateway console indicates that your volume has a status of UPLOAD BUFFER NOT CONFIGURED, add upload buffer capacity to your gateway. You cannot use a gateway to store your application data if the upload buffer for the gateway is not configured. For more information, see [To add and configure upload buffer or cache storage \(p. 257\)](#).

## The Console Says That Your Volume Is Irrecoverable

For stored volumes, if the Storage Gateway console indicates that your volume has a status of IRRECOVERABLE, you can no longer use this volume. You can try to delete the volume in the Storage Gateway console. If there is data on the volume, then you can recover the data when you create a new volume based on the local disk of the VM that was initially used to create the volume. When you create the new volume, select **Preserve existing data**. Make sure to delete pending snapshots of the volume before deleting the volume. For more information, see [Deleting a Snapshot \(p. 185\)](#). If deleting the volume in the Storage Gateway console does not work, then the disk allocated for the volume might have been improperly removed from the VM and cannot be removed from the appliance.

For cached volumes, if the Storage Gateway console indicates that your volume has a status of IRRECOVERABLE, you can no longer use this volume. If there is data on the volume, you can create a snapshot of the volume and then recover your data from the snapshot or you can clone the volume from the last recovery point. You can delete the volume after you have recovered your data. For more information, see [Your Cached Gateway is Unreachable And You Want to Recover Your Data \(p. 380\)](#).

For stored volumes, you can create a new volume from the disk that was used to create the irrecoverable volume. For more information, see [Creating a volume \(p. 72\)](#). For information about volume status, see [Understanding Volume Statuses and Transitions \(p. 193\)](#).

## Your Cached Gateway is Unreachable And You Want to Recover Your Data

When your gateway becomes unreachable (such as when you shut it down), you have the option of either creating a snapshot from a volume recovery point and using that snapshot, or cloning a new volume from the last recovery point for an existing volume. Cloning from a volume recovery point is faster and more cost effective than creating a snapshot. For more information about cloning a volume, see [Cloning a Volume \(p. 179\)](#).

Storage Gateway provides recovery points for each volume in a cached volume gateway architecture. A *volume recovery point* is a point in time at which all data of the volume is consistent and from which you can create a snapshot or clone a volume.

## The Console Says That Your Volume Has PASS THROUGH Status

In some cases, the Storage Gateway console might indicate that your volume has a status of PASSTHROUGH. A volume can have PASSTHROUGH status for several reasons. Some reasons require action, and some do not.

An example of when you should take action if your volume has the PASS THROUGH status is when your gateway has run out of upload buffer space. To verify if your upload buffer was exceeded in the past, you can view the `UploadBufferPercentUsed` metric in the Amazon CloudWatch console; for more information, see [Monitoring the upload buffer \(p. 220\)](#). If your gateway has the PASS THROUGH status because it has run out of upload buffer space, you should allocate more upload buffer space to your gateway. Adding more buffer space will cause your volume to transition from PASS THROUGH to BOOTSTRAPPING to AVAILABLE automatically. While the volume has the BOOTSTRAPPING status, the gateway reads data off the volume's disk, uploads this data to Amazon S3, and catches up as needed. When the gateway has caught up and saved the volume data to Amazon S3, the volume status becomes AVAILABLE and snapshots can be started again. Note that when your volume has the PASS THROUGH or BOOTSTRAPPING status, you can continue to read and write data from the volume disk. For more information about adding more upload buffer space, see [Determining the size of upload buffer to allocate \(p. 255\)](#).

To take action before the upload buffer is exceeded, you can set a threshold alarm on a gateway's upload buffer. For more information, see [To set an upper threshold alarm for a gateway's upload buffer \(p. 220\)](#).

In contrast, an example of not needing to take action when a volume has the PASS THROUGH status is when the volume is waiting to be bootstrapped because another volume is currently being bootstrapped. The gateway bootstraps volumes one at a time.

Infrequently, the PASS THROUGH status can indicate that a disk allocated for an upload buffer has failed. In this case, you should remove the disk. For more information, see [Volume Gateway \(p. 404\)](#). For information about volume status, see [Understanding Volume Statuses and Transitions \(p. 193\)](#).

## You Want to Verify Volume Integrity and Fix Possible Errors

If you want to verify volume integrity and fix possible errors, and your gateway uses Microsoft Windows initiators to connect to its volumes, you can use the Windows CHDKS utility to verify the integrity of your volumes and fix any errors on the volumes. Windows can automatically run the CHDKS tool when volume corruption is detected, or you can run it yourself.

## Your Volume's iSCSI Target Doesn't Appear in Windows Disk Management Console

If your volume's iSCSI target does not show up in the Disk Management Console in Windows, check that you have configured the upload buffer for the gateway. For more information, see [To add and configure upload buffer or cache storage \(p. 257\)](#).

## You Want to Change Your Volume's iSCSI Target Name

If you want to change the iSCSI target name of your volume, you must delete the volume and add it again with a new target name. If you do so, you can preserve the data on the volume.

## Your Scheduled Volume Snapshot Did Not Occur

If your scheduled snapshot of a volume did not occur, check whether your volume has the PASSTHROUGH status, or if the gateway's upload buffer was filled just prior to the scheduled snapshot time. You can check the `UploadBufferPercentUsed` metric for the gateway in the Amazon CloudWatch console and create an alarm for this metric. For more information, see [Monitoring the upload buffer \(p. 220\)](#) and [To set an upper threshold alarm for a gateway's upload buffer \(p. 220\)](#).

## You Need to Remove or Replace a Disk That Has Failed

If you need to replace a volume disk that has failed or replace a volume because it isn't needed, you should remove the volume first using the Storage Gateway console. For more information, see [To remove a volume \(p. 182\)](#). You then use the hypervisor client to remove the backing storage:

- For VMware ESXi, remove the backing storage as described in [Deleting a Volume \(p. 181\)](#).
- For Microsoft Hyper-V, remove the backing storage.

## Throughput from Your Application to a Volume Has Dropped to Zero

If throughput from your application to a volume has dropped to zero, try the following:

- If you are using the VMware vSphere client, check that your volume's **Host IP** address matches one of the addresses that appears in the vSphere client on the **Summary** tab. You can find the **Host IP** address for a storage volume in the Storage Gateway console in the **Details** tab for the volume. A discrepancy in the IP address can occur, for example, when you assign a new static IP address to your gateway. If there is a discrepancy, restart your gateway from the Storage Gateway console as shown in [Shutting Down Your Gateway VM \(p. 253\)](#). After the restart, the **Host IP** address in the **iSCSI Target Info** tab for a storage volume should match an IP address shown in the vSphere client on the **Summary** tab for the gateway.
- If there is no IP address in the **Host IP** box for the volume and the gateway is online. For example, this could occur if you create a volume associated with an IP address of a network adapter of a gateway that has two or more network adapters. When you remove or disable the network adapter that the volume is associated with, the IP address might not appear in the **Host IP** box. To address this issue, delete the volume and then re-create it preserving its existing data.
- Check that the iSCSI initiator your application uses is correctly mapped to the iSCSI target for the storage volume. For more information about connecting to storage volumes, see [Connecting to Your Volumes to a Windows Client \(p. 415\)](#).

You can view the throughput for volumes and create alarms from the Amazon CloudWatch console. For more information about measuring throughput from your application to a volume, see [Measuring Performance Between Your Application and Gateway \(p. 239\)](#).

## A Cache Disk in Your Gateway Encounters a Failure

If one or more cache disks in your gateway encounters a failure, the gateway prevents read and write operations to your virtual tapes and volumes. To resume normal functionality, reconfigure your gateway as described following:

- If the cache disk is inaccessible or unusable, delete the disk from your gateway configuration.
- If the cache disk is still accessible and useable, reconnect it to your gateway.

### Note

If you delete a cache disk, tapes or volumes that have clean data (that is, for which data in the cache disk and Amazon S3 are synchronized) will continue to be available when the gateway resumes normal functionality. For example, if your gateway has three cache disks and you delete two, tapes or volumes that are clean will have AVAILABLE status. Other tapes and volumes will have IRRECOVERABLE status.

If you use ephemeral disks as cache disks for your gateway or mount your cache disks on an ephemeral drive, your cache disks will be lost when you shut down the gateway. Shutting down the gateway when your cache disk and Amazon S3 are not synchronized can result in data loss. As a result, we don't recommend using ephemeral drives or disks.

## A Volume Snapshot Has PENDING Status Longer Than Expected

If a volume snapshot remains in PENDING state longer than expected, the gateway VM might have crashed unexpectedly or the status of a volume might have changed to PASS THROUGH or IRRECOVERABLE. If any of these are the case, the snapshot remains in PENDING status and the snapshot

does not successfully complete. In these cases, we recommend that you delete the snapshot. For more information, see [Deleting a Snapshot \(p. 185\)](#).

When the volume returns to AVAILABLE status, create a new snapshot of the volume. For information about volume status, see [Understanding Volume Statuses and Transitions \(p. 193\)](#).

## High Availability Health Notifications

When running your gateway on the VMware vSphere High Availability (HA) platform, you may receive health notifications. For more information about health notifications, see [Troubleshooting high availability issues \(p. 386\)](#).

## Troubleshooting virtual tape issues

You can find information following about actions to take if you experience unexpected issues with your virtual tapes.

### Topics

- [Recovering a Virtual Tape From An Unrecoverable Gateway \(p. 383\)](#)
- [Troubleshooting Irrecoverable Tapes \(p. 385\)](#)
- [High Availability Health Notifications \(p. 383\)](#)

## Recovering a Virtual Tape From An Unrecoverable Gateway

Although it is rare, your tape gateway might encounter an unrecoverable failure. Such a failure can occur in your hypervisor host, the gateway itself, or the cache disks. If a failure occurs, you can recover your tapes by following the troubleshooting instructions in this section.

### Topics

- [You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway \(p. 383\)](#)
- [You Need to Recover a Virtual Tape from a Malfunctioning Cache Disk \(p. 384\)](#)

## You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway

If your tape gateway or the hypervisor host encounters an unrecoverable failure, you can recover any data that has already been uploaded to AWS to another tape gateway.

Note that the data written to a tape might not be completely uploaded until that tape has been successfully archived into VTS. The data on tapes recovered to another gateway in this manner may be incomplete or empty. We recommend performing an inventory on all recovered tapes to ensure they contain the expected content.

### To recover a tape to another tape gateway

1. Identify an existing functioning tape gateway to serve as your recovery target gateway. If you don't have a tape gateway to recover your tapes to, create a new tape gateway. For information about how to create a gateway, see [Choosing a Gateway Type \(p. 85\)](#).
2. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.

3. In the navigation pane, choose **Gateways**, and then choose the tape gateway you want to recover tapes from.
4. Choose the **Details** tab. A tape recovery message is displayed in the tab.
5. Choose **Create recovery tapes** to disable the gateway.
6. In the dialog box that appears, choose **Disable gateway**.

This process permanently halts normal function of your tape gateway and exposes any available recovery points. For instructions, see [Disabling Your Tape Gateway \(p. 205\)](#).

7. From the tapes that the disabled gateway displays, choose the virtual tape and the recovery point you want to recover. A virtual tape can have multiple recovery points.
8. To begin recovering any tapes you need to the target tape gateway, choose **Create recovery tape**.
9. In the **Create recovery tape** dialog box, verify the barcode of the virtual tape you want to recover.
10. For **Gateway**, choose the tape gateway you want to recover the virtual tape to.
11. Choose **Create recovery tape**.
12. Delete the failed tape gateway so you don't get charged. For instructions, see [Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources \(p. 319\)](#).

Storage Gateway moves the tape from the failed tape gateway to the tape gateway you specified. The tape gateway marks the tape status as RECOVERED.

## You Need to Recover a Virtual Tape from a Malfunctioning Cache Disk

If your cache disk encounters an error, the gateway prevents read and write operations on virtual tapes in the gateway. For example, an error can occur when a disk is corrupted or removed from the gateway. The Storage Gateway console displays a message about the error.

In the error message, Storage Gateway prompts you to take one of two actions that can recover your tapes:

- **Shut Down and Re-Add Disks** – Take this approach if the disk has intact data and has been removed. For example, if the error occurred because a disk was removed from your host by accident but the disk and the data is intact, you can re-add the disk. To do this, see the procedure later in this topic.
- **Reset Cache Disk** – Take this approach if the cache disk is corrupted or not accessible. If the disk error causes the cache disk to be inaccessible, unusable, or corrupted, you can reset the disk. If you reset the cache disk, tapes that have clean data (that is, tapes for which data in the cache disk and Amazon S3 are synchronized) will continue to be available for you to use. However, tapes that have data that is not synchronized with Amazon S3 are automatically recovered. The status of these tapes is set to RECOVERED, but the tapes will be read-only. For information about how to remove a disk from your host, see [Determining the size of upload buffer to allocate \(p. 255\)](#).

### Important

If the cache disk you are resetting contains data that has not been uploaded to Amazon S3 yet, that data can be lost. After you reset cache disks, no configured cache disks will be left in the gateway, so you must configure at least one new cache disk for your gateway to function properly.

To reset the cache disk, see the procedure later in this topic.

### To shut down and re-add a disk

1. Shut down the gateway. For information about how to shut down a gateway, see [Shutting Down Your Gateway VM \(p. 253\)](#).

2. Add the disk back to your host, and make sure the disk node number of the disk has not changed. For information about how to add a disk, see [Determining the size of upload buffer to allocate \(p. 255\)](#).
3. Restart the gateway. For information about how to restart a gateway, see [Shutting Down Your Gateway VM \(p. 253\)](#).

After the gateway restarts, you can verify the status of the cache disks. The status of a disk can be one of the following:

- **present** – The disk is available to use.
- **missing** – The disk is no longer connected to the gateway.
- **mismatch** – The disk node is occupied by a disk that has incorrect metadata, or the disk content is corrupted.

#### To reset and reconfigure a cache disk

1. In the **A disk error has occurred** error message illustrated preceding, choose **Reset Cache Disk**.
2. On the **Configure Your Activated Gateway** page, configure the disk for cache storage. For information about how to do so, see [Configuring Local Disks \(p. 90\)](#).
3. After you have configured cache storage, shut down and restart the gateway as described in the previous procedure.

The gateway should recover after the restart. You can then verify the status of the cache disk.

#### To verify the status of a cache disk

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Gateways**, and then choose your gateway.
3. For **Actions**, choose **Configure Local Storage** to display the **Configure Local Storage** dialog box. This dialog box shows all local disks in the gateway.

The cache disk node status is displayed next to the disk.

##### Note

If you don't complete the recovery process, the gateway displays a banner that prompts you to configure local storage.

## Troubleshooting Irrecoverable Tapes

If your virtual tape fails unexpectedly, Storage Gateway sets the status of the failed virtual tape to IRRECOVERABLE. The action you take depends on the circumstances. You can find information following on some issues you might find, and how to troubleshoot them.

### You Need to Recover Data From an IRRECOVERABLE Tape

If you have a virtual tape with the status IRRECOVERABLE, and you need to work with it, try one of the following:

- Activate a new tape gateway if you don't have one activated. For more information, see [Choosing a Gateway Type \(p. 85\)](#).
- Disable the tape gateway that contains the irrecoverable tape, and recover the tape from a recovery point to the new tape gateway. For more information, see [You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway \(p. 383\)](#).

**Note**

You have to reconfigure your iSCSI initiator and backup application to use the new tape gateway. For more information, see [Connecting Your VTL Devices \(p. 96\)](#).

## You Don't Need an IRRECOVERABLE Tape That Isn't Archived

If you have a virtual tape with the status IRRECOVERABLE, you don't need it, and the tape has never been archived, you should delete the tape. For more information, see [Deleting Tapes \(p. 204\)](#).

## A Cache Disk in Your Gateway Encounters a Failure

If one or more cache disks in your gateway encounters a failure, the gateway prevents read and write operations to your virtual tapes and volumes. To resume normal functionality, reconfigure your gateway as described following:

- If the cache disk is inaccessible or unusable, delete the disk from your gateway configuration.
- If the cache disk is still accessible and useable, reconnect it to your gateway.

**Note**

If you delete a cache disk, tapes or volumes that have clean data (that is, for which data in the cache disk and Amazon S3 are synchronized) will continue to be available when the gateway resumes normal functionality. For example, if your gateway has three cache disks and you delete two, tapes or volumes that are clean will have AVAILABLE status. Other tapes and volumes will have IRRECOVERABLE status.

If you use ephemeral disks as cache disks for your gateway or mount your cache disks on an ephemeral drive, your cache disks will be lost when you shut down the gateway. Shutting down the gateway when your cache disk and Amazon S3 are not synchronized can result in data loss. As a result, we don't recommend using ephemeral drives or disks.

## High Availability Health Notifications

When running your gateway on the VMware vSphere High Availability (HA) platform, you may receive health notifications. For more information about health notifications, see [Troubleshooting high availability issues \(p. 386\)](#).

## Troubleshooting high availability issues

You can find information following about actions to take if you experience availability issues.

**Topics**

- [Health notifications \(p. 386\)](#)
- [Metrics \(p. 387\)](#)

## Health notifications

When you run your gateway on VMware vSphere HA, all gateways produce the following health notifications to your configured Amazon CloudWatch log group. These notifications go into a log stream called `AvailabilityMonitor`.

**Topics**

- [Notification: Reboot \(p. 372\)](#)
- [Notification: HardReboot \(p. 373\)](#)
- [Notification: HealthCheckFailure \(p. 373\)](#)
- [Notification: AvailabilityMonitorTest \(p. 373\)](#)

## Notification: Reboot

You can get a reboot notification when the gateway VM is restarted. You can restart a gateway VM by using the VM Hypervisor Management console or the Storage Gateway console. You can also restart by using the gateway software during the gateway's maintenance cycle.

### Action to Take

If the time of the reboot is within 10 minutes of the gateway's configured [maintenance start time \(p. 263\)](#), this is probably a normal occurrence and not a sign of any problem. If the reboot occurred significantly outside the maintenance window, check whether the gateway was restarted manually.

## Notification: HardReboot

You can get a HardReboot notification when the gateway VM is restarted unexpectedly. Such a restart can be due to loss of power, a hardware failure, or another event. For VMware gateways, a reset by vSphere High Availability Application Monitoring can trigger this event.

### Action to Take

When your gateway runs in such an environment, check for the presence of the `HealthCheckFailure` notification and consult the VMware events log for the VM.

## Notification: HealthCheckFailure

For a gateway on VMware vSphere HA, you can get a `HealthCheckFailure` notification when a health check fails and a VM restart is requested. This event also occurs during a test to monitor availability, indicated by an `AvailabilityMonitorTest` notification. In this case, the `HealthCheckFailure` notification is expected.

### Note

This notification is for VMware gateways only.

### Action to Take

If this event repeatedly occurs without an `AvailabilityMonitorTest` notification, check your VM infrastructure for issues (storage, memory, and so on). If you need additional assistance, contact AWS Support.

## Notification: AvailabilityMonitorTest

For a gateway on VMware vSphere HA, you can get an `AvailabilityMonitorTest` notification when you [run a test \(p. 332\)](#) of the [Availability and application monitoring](#) system in VMware.

## Metrics

The `AvailabilityNotifications` metric is available on all gateways. This metric is a count of the number of availability-related health notifications generated by the gateway. Use the `Sum` statistic

to observe whether the gateway is experiencing any availability-related events. Consult with your configured CloudWatch log group for details about the events.

## Best practices for recovering your data

Although it is rare, your gateway might encounter an unrecoverable failure. Such a failure can occur in your virtual machine (VM), the gateway itself, the local storage, or elsewhere. If a failure occurs, we recommend that you follow the instructions in the appropriate section following to recover your data.

### Important

Storage Gateway doesn't support recovering a gateway VM from a snapshot that is created by your hypervisor or from your Amazon EC2 Amazon Machine Image (AMI). If your gateway VM malfunctions, activate a new gateway and recover your data to that gateway using the instructions following.

### Topics

- [Recovering from an unexpected virtual machine shutdown \(p. 388\)](#)
- [Recovering your data from a malfunctioning gateway or VM \(p. 388\)](#)
- [Recovering your data from an irrecoverable volume \(p. 389\)](#)
- [Recovering your data from an irrecoverable tape \(p. 389\)](#)
- [Recovering your data from a malfunctioning cache disk \(p. 390\)](#)
- [Recovering your data from a corrupted file system \(p. 390\)](#)
- [Recovering your data from an inaccessible data center \(p. 391\)](#)

## Recovering from an unexpected virtual machine shutdown

If your VM shuts down unexpectedly, for example during a power outage, your gateway becomes unreachable. When power and network connectivity are restored, your gateway becomes reachable and starts to function normally. Following are some steps you can take at that point to help recover your data:

- If an outage causes network connectivity issues, you can troubleshoot the issue. For information about how to test network connectivity, see [Testing Your Gateway Connection to the Internet \(p. 296\)](#).
- For cached volumes and tapes setups, when your gateway becomes reachable, your volumes or tapes go into BOOTSTRAPPING status. This functionality ensures that your locally stored data continues to be synchronized with AWS. For more information on this status, see [Understanding Volume Statuses and Transitions \(p. 193\)](#).
- If your gateway malfunctions and issues occur with your volumes or tapes as a result of an unexpected shutdown, you can recover your data. For information about how to recover your data, see the sections following that apply to your scenario.

## Recovering your data from a malfunctioning gateway or VM

If your gateway or virtual machine malfunctions, you can recover data that has been uploaded to AWS and stored on a volume in Amazon S3. For cached volumes gateways, you recover data from a recovery snapshot. For stored volumes gateways, you can recover data from your most recent Amazon EBS

snapshot of the volume. For tape gateways, you recover one or more tapes from a recovery point to a new tape gateway.

If your cached volumes gateway becomes unreachable, you can use the following steps to recover your data from a recovery snapshot:

1. In the AWS Management Console, choose the malfunctioning gateway, choose the volume you want to recover, and then create a recovery snapshot from it.
2. Deploy and activate a new volume gateway. Or, if you have an existing functioning volume gateway, you can use that gateway to recover your volume data.
3. Find the snapshot you created and restore it to a new volume on the functioning gateway.
4. Mount the new volume as an iSCSI device on your on-premises application server.

For detailed information on how to recover cached volumes data from a recovery snapshot, see [Your Cached Gateway is Unreachable And You Want to Recover Your Data \(p. 380\)](#).

If your tape gateway or the hypervisor host encounters an unrecoverable failure, you can use the following steps to recover the tapes from the malfunctioning tape gateway to another tape gateway:

1. Identify the tape gateway that you want to use as the recovery target, or create a new one.
2. Disable the malfunctioning gateway.
3. Create recovery tapes for each tape that you want to recover and specify the target tape gateway.
4. Delete the malfunctioning tape gateway.

For detailed information on how to recover the tapes from a malfunctioning tape gateway to another tape gateway, see [You Need to Recover a Virtual Tape from a Malfunctioning Tape Gateway \(p. 383\)](#).

## Recovering your data from an irrecoverable volume

If the status of your volume is IRRECOVERABLE, you can no longer use this volume.

For stored volumes, you can retrieve your data from the irrecoverable volume to a new volume by using the following steps:

1. Create a new volume from the disk that was used to create the irrecoverable volume.
2. Preserve existing data when you are creating the new volume.
3. Delete all pending snapshot jobs for the irrecoverable volume.
4. Delete the irrecoverable volume from the gateway.

For cached volumes, we recommend using the last recovery point to clone a new volume.

For detailed information about how to retrieve your data from an irrecoverable volume to a new volume, see [The Console Says That Your Volume Is Irrecoverable \(p. 380\)](#).

## Recovering your data from an irrecoverable tape

If your tape encounters a failure and the status of the tape is IRRECOVERABLE, we recommend you use one of the following options to recover your data or resolve the failure depending on your situation:

- If you need the data on the irrecoverable tape, you can recover the tape to a new gateway.
- If you don't need the data on the tape, and the tape has never been archived, you can simply delete the tape from your tape gateway.

For detailed information about how to recover your data or resolve the failure if your tape is IRRECOVERABLE, see [Troubleshooting Irrecoverable Tapes \(p. 385\)](#).

## Recovering your data from a malfunctioning cache disk

If your cache disk encounters a failure, we recommend you use the following steps to recover your data depending on your situation:

- If the malfunction occurred because a cache disk was removed from your host, shut down the gateway, re-add the disk, and restart the gateway.
- If the cache disk is corrupted or not accessible, shut down the gateway, reset the cache disk, reconfigure the disk for cache storage, and restart the gateway.

For detailed information, see [You Need to Recover a Virtual Tape from a Malfunctioning Cache Disk \(p. 384\)](#).

## Recovering your data from a corrupted file system

If your file system gets corrupted, you can use the **fsck** command to check your file system for errors and repair it. If you can repair the file system, you can then recover your data from the volumes on the file system, as described following:

1. Shut down your virtual machine and use the Storage Gateway Management Console to create a recovery snapshot. This snapshot represents the most current data stored in AWS.

**Note**

You use this snapshot as a fallback if your file system can't be repaired or the snapshot creation process can't be completed successfully.

For information about how to create a recovery snapshot, see [Your Cached Gateway is Unreachable And You Want to Recover Your Data \(p. 380\)](#).

2. Use the **fsck** command to check your file system for errors and attempt a repair.
3. Restart your gateway VM.
4. When your hypervisor host starts to boot up, press and hold down shift key to enter the grub boot menu.
5. From the menu, press **e** to edit.
6. Choose the kernel line (the second line), and then press **e** to edit.
7. Append the following option to the kernel command line: **init=/bin/bash**. Use a space to separate the previous option from the option you just appended.
8. Delete both **console=** lines, making sure to delete all values following the = symbol, including those separated by commas.
9. Press **Return** to save the changes.

10Press **b** to boot your computer with the modified kernel option. Your computer will boot to a **bash#** prompt.

11Enter **/sbin/fsck -f /dev/sda1** to run this command manually from the prompt, to check and repair your file system. If the command does not work with the **/dev/sda1** path, you can use **lsblk** to determine the root filesystem device for **/** and use that path instead.

12When the file system check and repair is complete, reboot the instance. The grub settings will revert to the original values, and the gateway will boot up normally.

13 Wait for snapshots that are in-progress from the original gateway to complete, and then validate the snapshot data.

You can continue to use the original volume as-is, or you can create a new gateway with a new volume based on either the recovery snapshot or the completed snapshot. Alternatively, you can create a new volume from any of your completed snapshots from this volume.

## Recovering your data from an inaccessible data center

If your gateway or data center becomes inaccessible for some reason, you can recover your data to another gateway in a different data center or recover to a gateway hosted on an Amazon EC2 instance. If you don't have access to another data center, we recommend creating the gateway on an Amazon EC2 instance. The steps you follow depends on the gateway type you are covering the data from.

### To recover data from a volume gateway in an inaccessible data center

1. Create and activate a new volume gateway on an Amazon EC2 host. For more information, see [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#).

**Note**

Gateway stored volumes can't be hosted on Amazon EC2 instance.

2. Create a new volume and choose the EC2 gateway as the target gateway. For more information, see [Creating a volume \(p. 72\)](#).

Create the new volume based on an Amazon EBS snapshot or clone from last recovery point of the volume you want to recover.

If your volume is based on a snapshot, provide the snapshot id.

If you are cloning a volume from a recovery point, choose the source volume.

### To recover data from a tape gateway in an inaccessible data center

1. Create and activate a new tape gateway on an Amazon EC2 host. For more information, see [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#).
2. Recover the tapes from the source gateway in the data center to the new gateway you created on Amazon EC2. For more information, see [Recovering a Virtual Tape From An Unrecoverable Gateway \(p. 383\)](#).

Your tapes should be covered to the new Amazon EC2 gateway.

### To recover data from a file gateway in an inaccessible data center

For file gateway, you map a new file share to the Amazon S3 bucket that contains the data you want to recover.

1. Create and activate a new file gateway on an Amazon EC2 host. For more information, see [Deploying a file gateway on an Amazon EC2 host \(p. 401\)](#).
2. Create a new file share on the EC2 gateway you created. For more information, see [Creating a file share \(p. 46\)](#).
3. Mount your file share on your client and map it to the S3 bucket that contains the data that you want to recover. For more information, see [Using your file share \(p. 61\)](#).

# Additional Storage Gateway Resources

In this section, you can find information about AWS and third-party software, tools, and resources that can help you set up or manage your gateway, and also about Storage Gateway quotas.

## Topics

- [Host Setup \(p. 392\)](#)
- [Volume Gateway \(p. 404\)](#)
- [Tape Gateway \(p. 407\)](#)
- [Getting an Activation Key for Your Gateway \(p. 413\)](#)
- [Connecting iSCSI Initiators \(p. 414\)](#)
- [Using AWS Direct Connect with Storage Gateway \(p. 437\)](#)
- [Port Requirements \(p. 437\)](#)
- [Connecting to Your Gateway \(p. 440\)](#)
- [Understanding Storage Gateway Resources and Resource IDs \(p. 441\)](#)
- [Tagging Storage Gateway Resources \(p. 442\)](#)
- [Working with Open-Source Components for AWS Storage Gateway \(p. 443\)](#)
- [AWS Storage Gateway quotas \(p. 444\)](#)

## Host Setup

### Topics

- [Configuring VMware for Storage Gateway \(p. 392\)](#)
- [Synchronizing Your Gateway VM Time \(p. 397\)](#)
- [Deploying a Volume or Tape Gateway on an Amazon EC2 Host \(p. 399\)](#)
- [Deploying a file gateway on an Amazon EC2 host \(p. 401\)](#)

## Configuring VMware for Storage Gateway

When configuring VMware for Storage Gateway, make sure to synchronize your VM time with your host time, configure VM to use paravirtualized disk controllers when provisioning storage and provide protection from failures in the infrastructure layer supporting a gateway VM.

### Topics

- [Synchronizing VM Time with Host Time \(p. 392\)](#)
- [Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers \(p. 395\)](#)
- [Using Storage Gateway with VMware High Availability \(p. 396\)](#)

## Synchronizing VM Time with Host Time

To successfully activate your gateway, you must ensure that your VM time is synchronized to the host time, and that the host time is correctly set. In this section, you first synchronize the time on the VM to

the host time. Then you check the host time and, if needed, set the host time and configure the host to synchronize its time automatically to a Network Time Protocol (NTP) server.

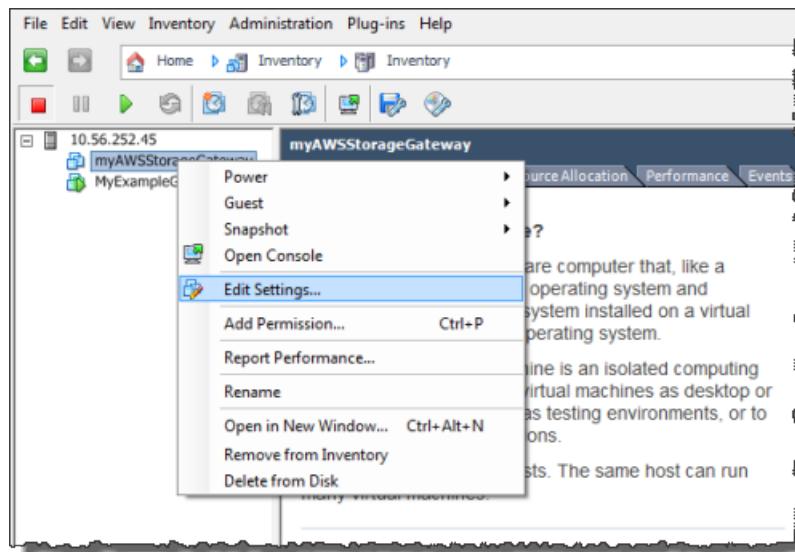
**Important**

Synchronizing the VM time with the host time is required for successful gateway activation.

### To synchronize VM time with host time

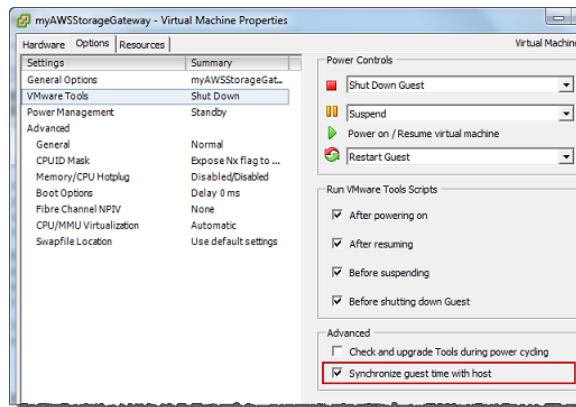
1. Configure your VM time.
  - a. In the vSphere client, open the context (right-click) menu for your gateway VM, and choose **Edit Settings**.

The **Virtual Machine Properties** dialog box opens.



- b. Choose the **Options** tab, and choose **VMware Tools** in the options list.
- c. Check the **Synchronize guest time with host** option, and then choose **OK**.

The VM synchronizes its time with the host.

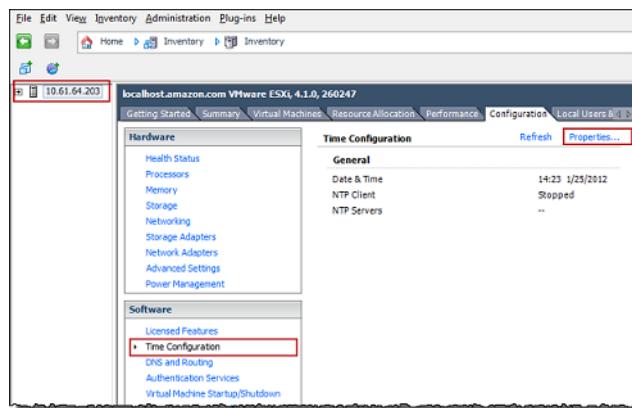


2. Configure the host time.

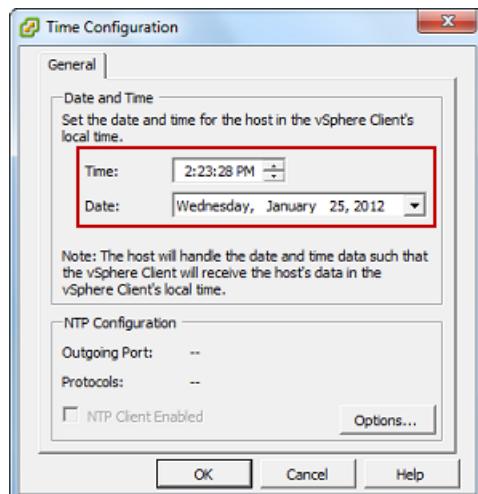
It is important to make sure that your host clock is set to the correct time. If you have not configured your host clock, perform the following steps to set and synchronize it with an NTP server.

- a. In the VMware vSphere client, select the vSphere host node in the left pane, and then choose the **Configuration** tab.
- b. Select **Time Configuration** in the **Software** panel, and then choose the **Properties** link.

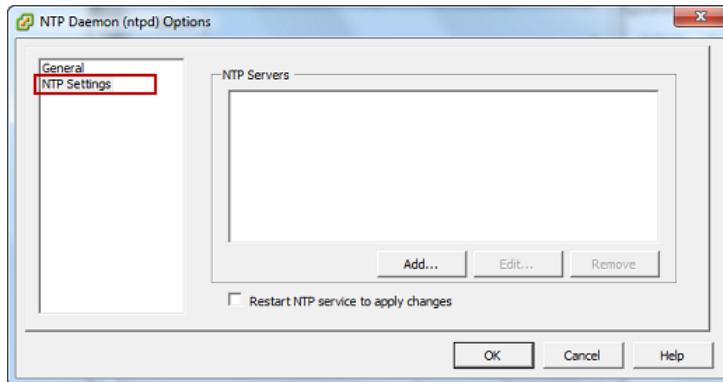
The **Time Configuration** dialog box appears.



- c. In the **Date and Time** panel, set the date and time.



- d. Configure the host to synchronize its time automatically to an NTP server.
  - i. Choose **Options** in the **Time Configuration** dialog box, and then in the **NTP Daemon (ntpd)** **Options** dialog box, choose **NTP Settings** in the left pane.



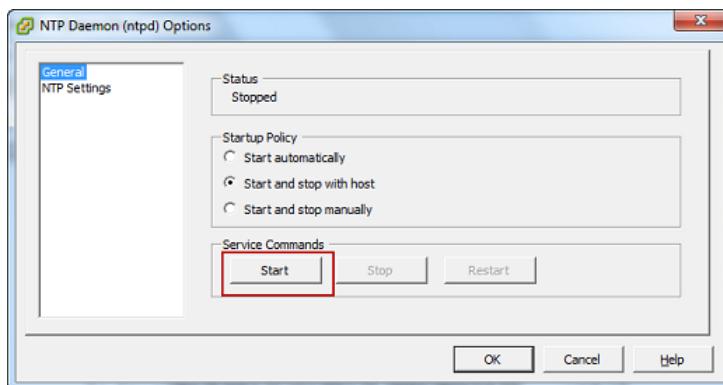
- ii. Choose **Add** to add a new NTP server.
- iii. In the **Add NTP Server** dialog box, type the IP address or the fully qualified domain name of an NTP server, and then choose **OK**.

You can use `pool.ntp.org` as shown in the following example.



- iv. In the **NTP Daemon (ntpd) Options** dialog box, choose **General** in the left pane.
- v. In the **Service Commands** pane, choose **Start** to start the service.

Note that if you change this NTP server reference or add another later, you will need to restart the service to use the new server.



- e. Choose **OK** to close the **NTP Daemon (ntpd) Options** dialog box.
- f. Choose **OK** to close the **Time Configuration** dialog box.

## Configuring the AWS Storage Gateway VM to Use Paravirtualized Disk Controllers

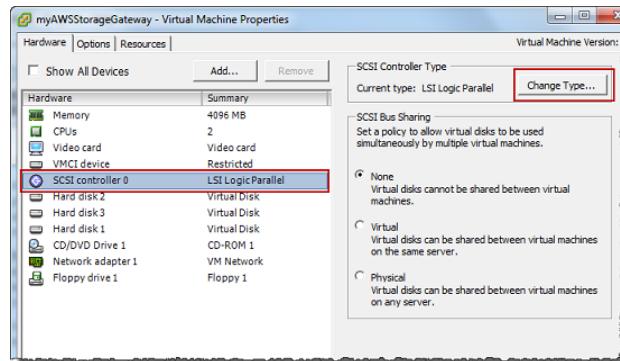
In this task, you set the iSCSI controller so that the VM uses paravirtualization. *Paravirtualization* is a mode where the gateway VM works with the host operating system so the console can identify the virtual disks that you add to your VM.

### Note

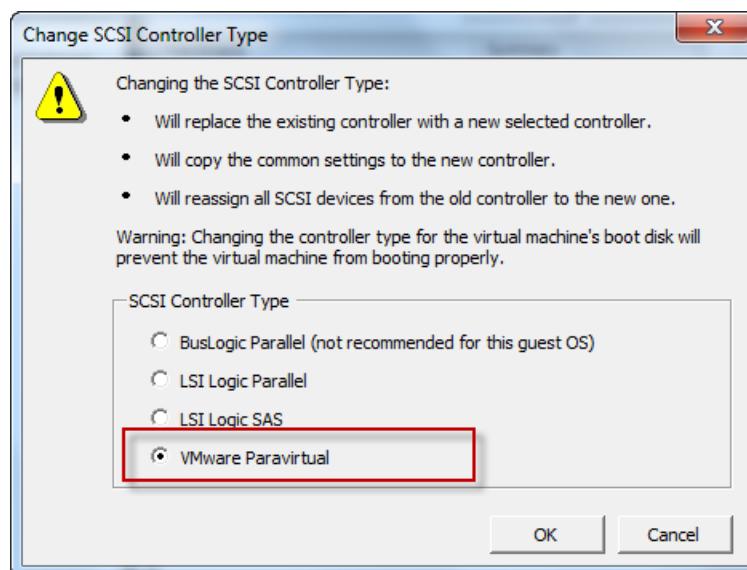
You must complete this step to avoid issues in identifying these disks when you configure them in the gateway console.

### To configure your VM to use paravirtualized controllers

1. In the VMware vSphere client, open the context (right-click) menu for your gateway VM, and then choose **Edit Settings**.
2. In the **Virtual Machine Properties** dialog box, choose the **Hardware** tab, select the **SCSI controller 0**, and then choose **Change Type**.



3. In the **Change SCSI Controller Type** dialog box, select the **VMware Paravirtual** SCSI controller type, and then choose **OK**.



## Using Storage Gateway with VMware High Availability

VMware High Availability (HA) is a component of vSphere that can provide protection from failures in the infrastructure layer supporting a gateway VM. VMware HA does this by using multiple hosts configured as a cluster so that if a host running a gateway VM fails, the gateway VM can be restarted automatically on another host within the cluster. For more information about VMware HA, see [VMware HA: Concepts and Best Practices](#) on the VMware website.

To use Storage Gateway with VMware HA, we recommend doing the following things:

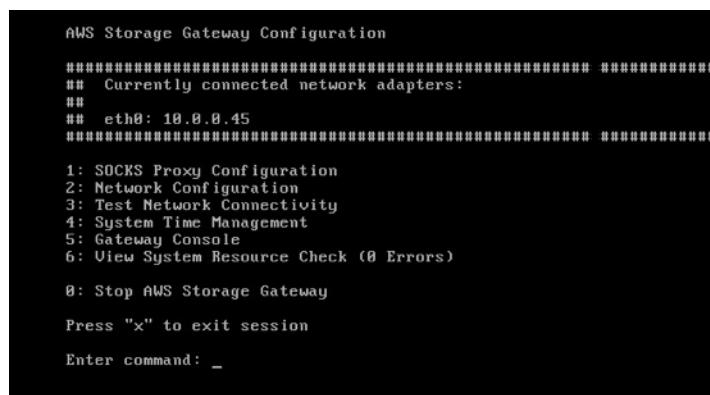
- Deploy the VMware ESX .ova downloadable package that contains the Storage Gateway VM on only one host in a cluster.
- When deploying the .ova package, select a data store that is not local to one host. Instead, use a data store that is accessible to all hosts in the cluster. If you select a data store that is local to a host and the host fails, then the data source might not be accessible to other hosts in the cluster and failover to another host might not succeed.
- To prevent your initiator from disconnecting from storage volume targets during failover, follow the recommended iSCSI settings for your operating system. In a failover event, it can take from a few seconds to several minutes for a gateway VM to start in a new host in the failover cluster. The recommended iSCSI timeouts for both Windows and Linux clients are greater than the typical time it takes for failover to occur. For more information on customizing Windows clients' timeout settings, see [Customizing Your Windows iSCSI Settings \(p. 424\)](#). For more information on customizing Linux clients' timeout settings, see [Customizing Your Linux iSCSI Settings \(p. 428\)](#).
- With clustering, if you deploy the .ova package to the cluster, select a host when you are prompted to do so. Alternately, you can deploy directly to a host in a cluster.

## Synchronizing Your Gateway VM Time

For a gateway deployed on VMware ESXi, setting the hypervisor host time and synchronizing the VM time to the host is sufficient to avoid time drift. For more information, see [Synchronizing VM Time with Host Time \(p. 392\)](#). For a gateway deployed on Microsoft Hyper-V, you should periodically check your VM's time using the procedure described following.

### To view and synchronize the time of a hypervisor gateway VM to a Network Time Protocol (NTP) server

1. Log in to your gateway's local console:
  - For more information on logging in to the VMware ESXi local console, see [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#).
  - For more information on logging in to the Microsoft Hyper-V local console, see [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#).
  - For more information on logging in to the local console for Linux Kernel-based Virtuan Machine (KVM), see [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#).
2. On the **Storage Gateway Configuration** main menu, enter **4** for **System Time Management**.



The screenshot shows a terminal window with the following text:

```
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. On the **System Time Management** menu, enter **1** for **View and Synchronize System Time**.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: _
```

4. If the result indicates that you should synchronize your VM's time to the NTP time, enter **y**. Otherwise, enter **n**.

If you enter **y** to synchronize, the synchronization might take a few moments.

The following screenshot shows a VM that doesn't require time synchronization.

```
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]: _
```

The following screenshot shows a VM that does require time synchronization.

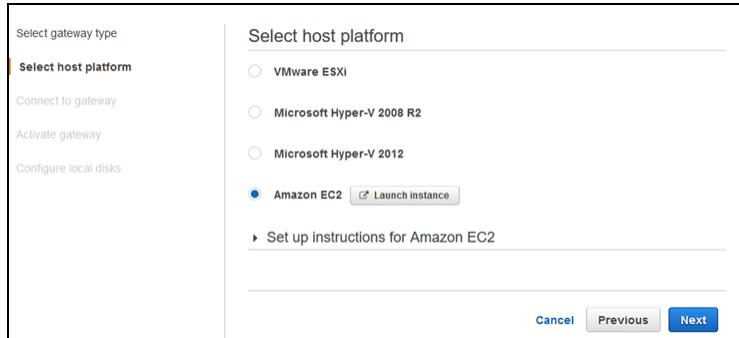
```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

# Deploying a Volume or Tape Gateway on an Amazon EC2 Host

You can deploy and activate a tape or volume gateway on an Amazon EC2 instance. The gateway Amazon Machine Image (AMI) is available as a community AMI.

## To deploy a gateway on an Amazon EC2 instance

1. On the **Choose host platform** page, choose **Amazon EC2**.
2. Choose **Launch instance** to launch a storage gateway EC2 AMI. You are redirected to the EC2 community AMI page, where you can choose an instance type.



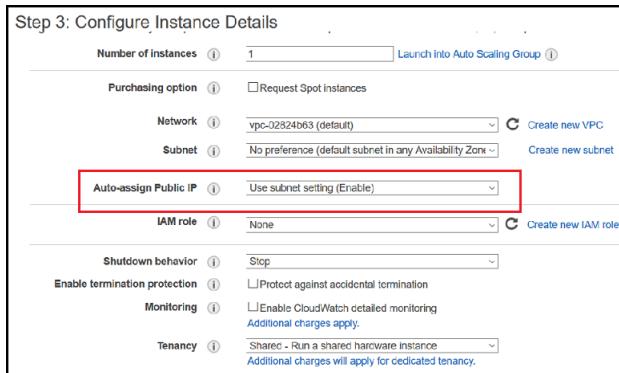
3. On the **Choose an Instance Type** page, choose the hardware configuration of your instance. Storage Gateway is supported on instance types that meet certain minimum requirements. We recommend starting with the m4xlarge instance type, which meets the minimum requirements for your gateway to function properly. For more information, see [Hardware requirements for on-premises VMs \(p. 12\)](#).

You can resize your instance after you launch, if necessary. For more information, see [Resizing Your Instance](#) in the *Amazon EC2 User Guide for Linux Instances*.

### Note

Certain instance types, particularly i3 EC2, use NVMe SSD disks. These can cause problems when you start or stop a gateway; for example, you can lose data from the cache. Monitor the CachePercentDirty Amazon CloudWatch metric, and only start or stop your system when that metric is 0. To learn more about monitoring metrics for your gateway, see [Storage Gateway Metrics and Dimensions](#) in the CloudWatch documentation. For more information, see the section called "Requirements for Amazon EC2 instance types" (p. 12).

4. Choose **Next: Configure Instance Details**.
5. On the **Configure Instance Details** page, choose a value for **Auto-assign Public IP**. If your instance should be accessible from the public internet, verify that **Auto-assign Public IP** is set to **Enable**. If your instance shouldn't be accessible from the internet, choose **Auto-assign Public IP** for **Disable**.



The screenshot shows the 'Step 3: Configure Instance Details' page. It includes fields for 'Number of instances' (1), 'Purchasing option' (Request Spot instances), 'Network' (vpc-02524b63 (default)), 'Subnet' (No preference (default subnet in any Availability Zone)), 'Auto-assign Public IP' (Use subnet setting (Enable) - highlighted with a red box), 'IAM role' (None), 'Shutdown behavior' (Stop), 'Enable termination protection' (Protect against accidental termination), 'Monitoring' (Enable CloudWatch detailed monitoring), and 'Tenancy' (Shared - Run a shared hardware instance). Buttons for 'Launch Into Auto Scaling Group' and 'Create new VPC' are also present.

6. On the **Configure Instance Details** page, choose the AWS Identity and Access Management (IAM) role that you want to use for your gateway.
7. Choose **Next: Add Storage**.
8. On the **Add Storage** page, choose **Add New Volume** to add storage to your tape or volume gateway instance. You need at least one Amazon EBS volume to configure for cache storage.

The following table recommends sizes for local disk storage for your deployed gateway.

Gateway Type	Cache (Minimum)	Cache (Maximum)	Upload Buffer (Minimum)	Upload Buffer (Maximum)	Other Required Local Disks
File gateway	150 GiB	64 TiB	—	—	—
Cached volume gateway	150 GiB	64 TiB	150 GiB	2 TiB	—
Stored volume gateway	—	—	150 GiB	2 TiB	1 or more for stored volume or volumes
Tape gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

#### Note

You can configure one or more local drives for your cache and upload buffer, up to the maximum capacity.

When adding cache or upload buffer to an existing gateway, it's important to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

9. On the **Step 5: Add Tags** page, you can add an optional tag to your instance. Then choose **Next: Configure Security Group**.
10. On the **Configure Security Group** page, add firewall rules to specific traffic to reach your instance. You can create a new security group or choose an existing security group.

#### Important

Besides the Storage Gateway activation and Secure Shell (SSH) access ports, NFS clients require access to additional ports. For detailed information, see [Network and firewall requirements \(p. 13\)](#).

11. Choose **Review and Launch** to review your configuration.
12. On the **Review Instance Launch** page, choose **Launch**.

13. In the **Select an existing key pair or create a new key pair** dialog box, choose **Choose an existing key pair**, and choose the key pair that you created when getting set up. When you are ready, select the acknowledgment box, and then choose **Launch Instances**.  
  
A confirmation page tells you that your instance is launching.
14. Choose **View Instances** to close the confirmation page and return to the console. On the **Instances** screen, you can view the status of your instance. It takes a short time for an instance to launch. When you launch an instance, its initial state is **Pending**. After the instance starts, its state changes to **running**, and it receives a public DNS name.
15. Choose your instance, note the public IP address in the **Description** tag, and return to the [Connect to gateway \(p. 43\)](#) page on the Storage Gateway console to continue your gateway setup.

You can determine the AMI ID to use for launching a tape or volume gateway by using the Storage Gateway console or by querying the AWS Systems Manager parameter store.

#### To determine the AMI ID

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **Create gateway**, choose your gateway type, and then choose **Next**.
3. On the **Choose host platform** page, choose **Amazon EC2**.
4. Choose **Launch instance** to launch a Storage Gateway EC2 AMI. You are redirected to the EC2 community AMI page, where you can see the AMI ID for your AWS Region in the URL.

Or you can query the Systems Manager parameter store. You can use the AWS CLI or Storage Gateway API to query the Systems Manager public parameter under the namespace `/aws/service/storagegateway/ami/GatewayType/latest`. For example, using the following CLI command returns the ID of the current AMI in the current AWS Region.

```
aws --region aws-region ssm get-parameter --name /aws/service/storagegateway/ami/GatewayType/latest
```

Allowed values for *GatewayType* include **CACHED**, **FILE\_S3**, **STORED**, and **VTL**.

The CLI command returns output similar to the following for VTL *GatewayType*.

```
{  
    "Parameter": {  
        "Version": 9,  
        "Type": "String",  
        "Name": "/aws/service/storagegateway/ami/VTL/latest",  
        "Value": "ami-1234567890dd12222"  
    }  
}
```

## Deploying a file gateway on an Amazon EC2 host

You can deploy and activate a file gateway on an Amazon Elastic Compute Cloud (Amazon EC2) instance. The file gateway Amazon Machine Image (AMI) is available as a community AMI.

#### To deploy a gateway on an Amazon EC2 instance

1. On the **Select host platform** page, choose **Amazon EC2**.

2. Choose **Launch instance** to launch a storage gateway EC2 AMI. You are redirected to the Amazon EC2 console where you can choose an instance type.
3. On the **Step 2: Choose an Instance Type** page, choose the hardware configuration of your instance. Storage Gateway is supported on instance types that meet certain minimum requirements. We recommend starting with the m4.xlarge instance type, which meets the minimum requirements for your gateway to function properly. For more information, see [Hardware requirements for on-premises VMs \(p. 12\)](#).

You can resize your instance after you launch, if necessary. For more information, see [Resizing your instance](#) in the *Amazon EC2 User Guide for Linux Instances*.

**Note**

Certain instance types, particularly i3 EC2, use NVMe SSD disks. These can cause problems when you start or stop file gateway; for example, you can lose data from the cache. Monitor the CachePercentDirty Amazon CloudWatch metric, and only start or stop your system when that parameter is 0. To learn more about monitoring metrics for your gateway, see [Storage Gateway metrics and dimensions](#) in the CloudWatch documentation. For more information about Amazon EC2 instance type requirements, see the section called ["Requirements for Amazon EC2 instance types" \(p. 12\)](#).

4. Choose **Next: Configure Instance Details**.
5. On the **Step 3: Configure Instance Details** page, choose a value for **Auto-assign Public IP**. If your instance should be accessible from the public internet, verify that **Auto-assign Public IP** is set to **Enable**. If your instance shouldn't be accessible from the internet, choose **Auto-assign Public IP** for **Disable**.
6. For **IAM role**, choose the AWS Identity and Access Management (IAM) role that you want to use for your gateway.
7. Choose **Next: Add Storage**.
8. On the **Step 4: Add Storage** page, choose **Add New Volume** to add storage to your file gateway instance. You need at least one additional Amazon EBS volume to configure for cache storage.

The following table recommends sizes for local disk storage for your deployed gateway.

Gateway Type	Cache (Minimum)	Cache (Maximum)	Upload Buffer (Minimum)	Upload Buffer (Maximum)	Other Required Local Disks
File gateway	150 GiB	64 TiB	—	—	—
Cached volume gateway	150 GiB	64 TiB	150 GiB	2 TiB	—
Stored volume gateway	—	—	150 GiB	2 TiB	1 or more for stored volume or volumes
Tape gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

**Note**

You can configure one or more local drives for your cache and upload buffer, up to the maximum capacity.

When adding cache or upload buffer to an existing gateway, it's important to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

9. On the **Step 5: Add Tags** page, you can add an optional tag to your instance. Then choose **Next: Configure Security Group**.
10. On the **Step 6: Configure Security Group** page, add firewall rules to specific traffic to reach your instance. You can create a new security group or choose an existing security group.

**Important**

Besides the Storage Gateway activation and Secure Shell (SSH) access ports, NFS clients require access to additional ports. For detailed information, see [Network and firewall requirements \(p. 13\)](#).

11. Choose **Review and Launch** to review your configuration.
  12. On the **Step 7: Review Instance Launch** page, choose **Launch**.
  13. In the **Select an existing key pair or create a new key pair** dialog box, choose **Choose an existing key pair**, and then select the key pair that you created when getting set up. When you are ready, choose the acknowledgment box, and then choose **Launch Instances**.
- A confirmation page tells you that your instance is launching.
14. Choose **View Instances** to close the confirmation page and return to the console. On the **Instances** screen, you can view the status of your instance. It takes a short time for an instance to launch. When you launch an instance, its initial state is **pending**. After the instance starts, its state changes to **running**, and it receives a public DNS name.
  15. Select your instance, note the public IP address in the **Description** tag, and return to the [Connect to gateway \(p. 43\)](#) page on the Storage Gateway console to continue your gateway setup.

You can determine the AMI ID to use for launching a file gateway by using the Storage Gateway console or by querying the AWS Systems Manager parameter store.

### To determine the AMI ID

1. Sign in to the AWS Management Console and open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose **Create gateway**, choose **File gateway**, and then choose **Next**.
3. On the **Choose host platform** page, choose **Amazon EC2**.
4. Choose **Launch instance** to launch a Storage Gateway EC2 AMI. You are redirected to the EC2 community AMI page, where you can see the AMI ID for your AWS Region in the URL.

Or you can query the Systems Manager parameter store. You can use the AWS CLI or Storage Gateway API to query the Systems Manager public parameter under the namespace `/aws/service/storagegateway/ami/FILE_S3/latest`. For example, using the following CLI command returns the ID of the current AMI in the current AWS Region.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/FILE_S3/latest
```

The CLI command returns output similar to the following.

```
{  
    "Parameter": {  
        "Type": "String",  
        "LastModifiedDate": 1561054105.083,  
        "Version": 4,  
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/FILE_S3/latest",  
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",  
        "Value": "ami-123c45dd67d891000"  
    }  
}
```

}

# Volume Gateway

## Topics

- [Removing Disks from Your Gateway \(p. 404\)](#)
- [Adding and Removing Amazon EBS Volumes for Your Gateway Hosted on Amazon EC2 \(p. 406\)](#)

## Removing Disks from Your Gateway

Although we don't recommend removing the underlying disks from your gateway, you might want to remove a disk from your gateway, for example if you have a failed disk.

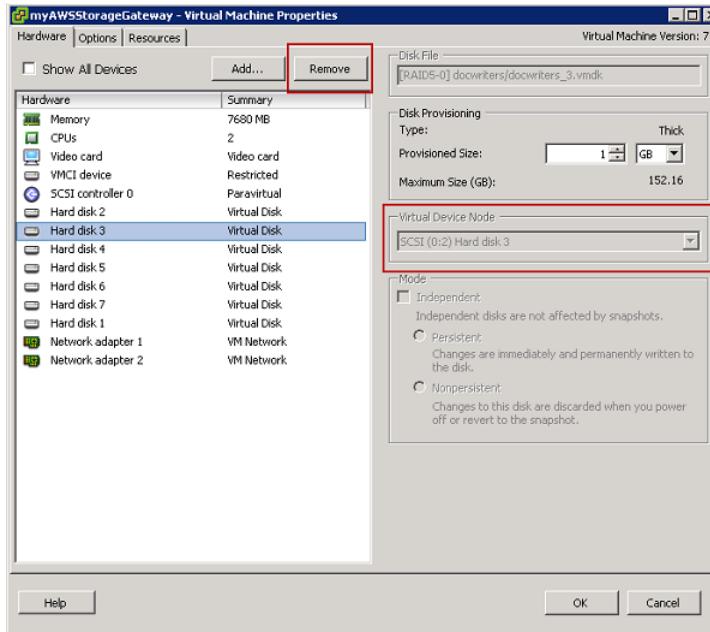
### Removing a Disk from a Gateway Hosted on VMware ESXi

You can use the following procedure to remove a disk from your gateway hosted on VMware hypervisor.

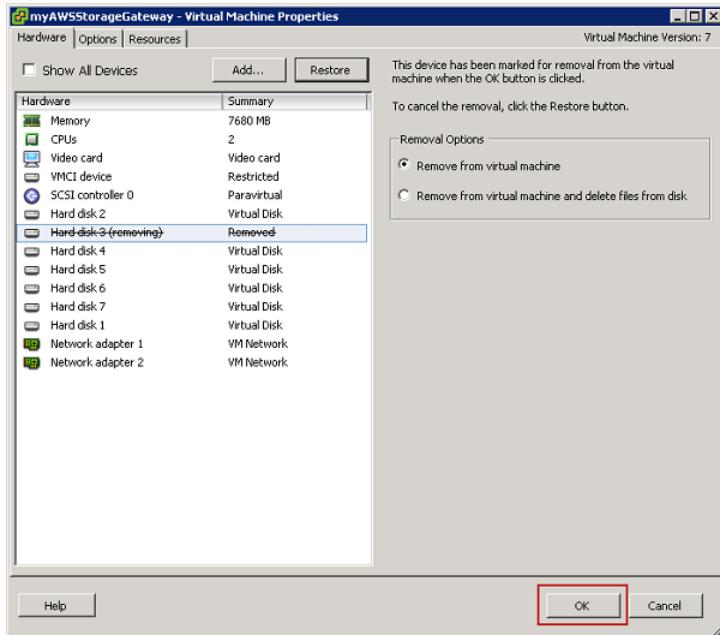
#### To remove a disk allocated for the upload buffer (VMware ESXi)

1. In the vSphere client, open the context (right-click) menu, choose the name of your gateway VM, and then choose **Edit Settings**.
2. On the **Hardware** tab of the **Virtual Machine Properties** dialog box, select the disk allocated as upload buffer space, and then choose **Remove**.

Verify that the **Virtual Device Node** value in the **Virtual Machine Properties** dialog box has the same value that you noted previously. Doing this helps ensure that you remove the correct disk.



3. Choose an option in the **Removal Options** panel, and then choose **OK** to complete the process of removing the disk.



## Removing a Disk from a Gateway Hosted on Microsoft Hyper-V

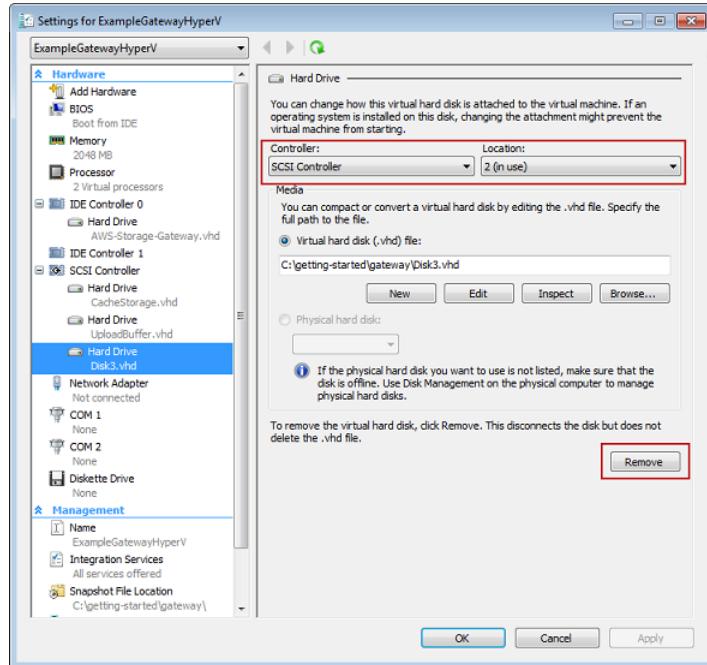
Using the following procedure, you can remove a disk from your gateway hosted on a Microsoft Hyper-V hypervisor.

### To remove an underlying disk allocated for the upload buffer (Microsoft Hyper-V)

1. In the Microsoft Hyper-V Manager, open the context (right-click) menu, choose the name of your gateway VM, and then choose **Settings**.
2. In the **Hardware** list of the **Settings** dialog box, select the disk to remove, and then choose **Remove**.

The disks you add to a gateway appear under the **SCSI Controller** entry in the **Hardware** list. Verify that the **Controller** and **Location** value are the same value that you noted previously. Doing this helps ensure that you remove the correct disk.

The first SCSI controller displayed in the Microsoft Hyper-V Manager is controller 0.



- Choose **OK** to apply the change.

## Removing a Disk from a Gateway Hosted on Linux KVM

To detach a disk from your gateway hosted on Linux Kernel-based Virtual Machine (KVM) hypervisor, you can use a `virsh` command similar to the one following.

```
$ virsh detach-disk domain_name /device/path
```

For more details about managing KVM disks, see documentation of your Linux distribution.

## Adding and Removing Amazon EBS Volumes for Your Gateway Hosted on Amazon EC2

When you initially configured your gateway to run as an Amazon EC2 instance, you allocated Amazon EBS volumes for use as an upload buffer and cache storage. Over time, as your applications needs change, you can allocate additional Amazon EBS volumes for this use. You can also reduce the storage you allocated by removing previously allocated Amazon EBS volumes. For more information about Amazon EBS, see [Amazon Elastic Block Store \(Amazon EBS\)](#) in the *Amazon EC2 User Guide for Linux Instances*.

Before you add more storage to the gateway, you should review how to size your upload buffer and cache storage based on your application needs for a gateway. To do so, see [Determining the size of upload buffer to allocate \(p. 255\)](#) and [Determining the size of cache storage to allocate \(p. 256\)](#).

There are quotas on the maximum storage you can allocate as an upload buffer and cache storage. You can attach as many Amazon EBS volumes to your instance as you want, but you can only configure these volumes as upload buffer and cache storage space up to these storage quotas. For more information, see [AWS Storage Gateway quotas \(p. 444\)](#).

## To add an Amazon EBS volume and configure it for your gateway

1. Create an Amazon EBS volume. For instructions, see [Creating or Restoring an Amazon EBS Volume in the Amazon EC2 User Guide for Linux Instances](#).
2. Attach the Amazon EBS volume to your Amazon EC2 instance. For instructions, see [Attaching an Amazon EBS Volume to an Instance in the Amazon EC2 User Guide for Linux Instances](#).
3. Configure the Amazon EBS volume you added as either an upload buffer or cache storage. For instructions, see [Managing local disks for your Storage Gateway \(p. 254\)](#).

There are times you might find you don't need the amount of storage you allocated for the upload buffer.

## To remove an Amazon EBS volume

### Warning

These steps apply only for Amazon EBS volumes allocated as upload buffer space. If you remove an Amazon EBS volume that is allocated as cache storage from a gateway, virtual tapes on the gateway will have the IRRECOVERABLE status, and you risk data loss. For more information on the IRRECOVERABLE status, see [Understanding Tape Status Information in a VTL \(p. 206\)](#).

1. Shut down the gateway by following the approach described in the [Shutting Down Your Gateway VM \(p. 253\)](#) section.
2. Detach the Amazon EBS volume from your Amazon EC2 instance. For instructions, see [Detaching an Amazon EBS Volume from an Instance in the Amazon EC2 User Guide for Linux Instances](#).
3. Delete the Amazon EBS volume. For instructions, see [Deleting an Amazon EBS Volume in the Amazon EC2 User Guide for Linux Instances](#).
4. Start the gateway by following the approach described in the [Shutting Down Your Gateway VM \(p. 253\)](#) section.

# Tape Gateway

### Topics

- [Working with VTL Devices \(p. 407\)](#)
- [Working With Tapes \(p. 411\)](#)

## Working with VTL Devices

Your tape gateway setup provides the following SCSI devices, which you select when activating your gateway.

### Topics

- [Selecting a Medium Changer After Gateway Activation \(p. 408\)](#)
- [Updating the Device Driver for Your Medium Changer \(p. 409\)](#)
- [Displaying Barcodes for Tapes in Microsoft System Center DPM \(p. 411\)](#)

For medium changers, AWS Storage Gateway works with the following:

- AWS-Gateway-VTL – This device is provided with the gateway.
- STK-L700 – This device emulation is provided with the gateway.

When activating your tape gateway, you select your backup application from the list and storage gateway uses the appropriate medium changer. If your backup application is not listed, you choose **Other** and then choose the medium changer that works with backup application.

The type of medium changer you choose depends on the backup application you plan to use. The following table lists third-party backup applications that have been tested and found to be compatible with tape gateways. This table includes the medium changer type recommended for each backup application.

Backup Application	Medium Changer Type
Arcserve Backup	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL or STK-L700
Commvault V11	STK-L700
Dell EMC NetWorker 19.5	AWS-Gateway-VTL
IBM Spectrum Protect v8.1.10	IBM-03584L32-0402
Micro Focus (HPE) Data Protector 9.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 or 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/Network 6.4 or 7.1	STK-L700
Quest NetVault Backup 12.4 or 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014 or 15 or 16 or 20.x	AWS-Gateway-VTL
Veritas Backup Exec 2012  <b>Note</b> Veritas has ended support for Backup Exec 2012.	STK-L700
Veritas NetBackup Version 7.x or 8.x	AWS-Gateway-VTL

### Important

We highly recommend that you choose the medium changer that's listed for your backup application. Other medium changers might not function properly. You can choose a different medium changer after the gateway is activated. For more information, see [Selecting a Medium Changer After Gateway Activation \(p. 408\)](#).

For tape drives, Storage Gateway works with the following:

- IBM-ULT3580-TD5—This device emulation is provided with the gateway.

## Selecting a Medium Changer After Gateway Activation

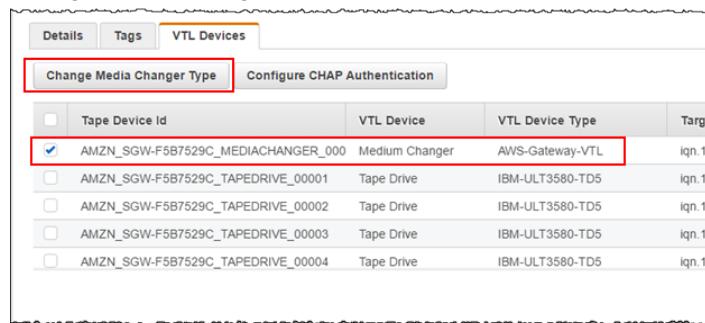
After your gateway is activated, you can choose to select a different medium changer type.

### Important

If your tape gateway uses the Symantec Backup Exec 2014 or NetBackup 7.x backup software, you must select the AWS-Gateway-VTL device type. For more information on how to change the medium changer after gateway activation for these applications, see [Best Practices for using Veritas Backup products \(NetBackup, Backup Exec\) with the Amazon Web Services Storage Tape Gateway-VTL in Symantec Support](#).

### To select a different medium changer type after gateway activation

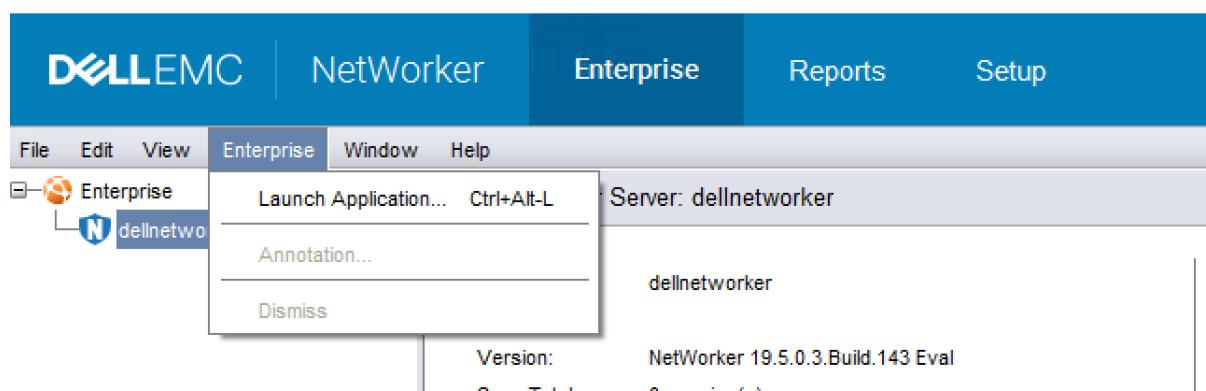
1. Stop any related jobs that are running in your backup software.
2. On the Windows server, open the iSCSI initiator properties window.
3. Choose the **Targets** tab to display the discovered targets.
4. On the Discovered targets pane, choose the medium changer you want to change, choose **Disconnect**, and then choose **OK**.
5. On the Storage Gateway console, choose **Gateways** from the navigation pane, and then choose the gateway whose medium changer you want to change.
6. Choose the **VTL Devices** tab, select the medium changer you want to change, and then choose **Change Media Changer**.



7. In the Change Media Changer Type dialog box that appears, select the media changer you want from the drop-down list box and then choose **Save**.

## Updating the Device Driver for Your Medium Changer

1. Open Device Manager on your Windows server, and expand the **Medium Changer devices** tree.
2. Open the context (right-click) menu for **Unknown Medium Changer**, and choose **Update Driver Software** to open the **Update Driver Software-unknown Medium Changer** window.
3. NetWorker Management Console V19.5.0.3 - localhost



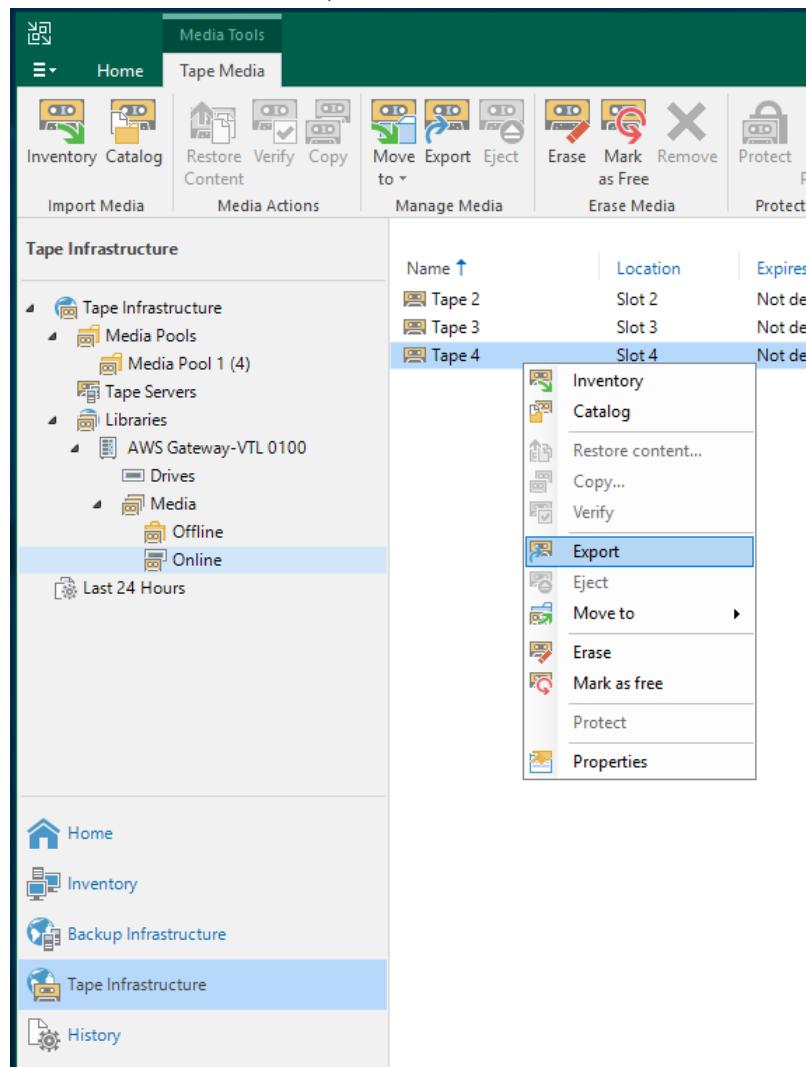
In the **How do you want to search for driver software?** section, choose **Browse my computer for driver software**.

4. Choose **Let me pick from a list of device drivers on my computer**.

**Note**

We recommend using the Sony TSL-A500C Autoloader driver with the Veeam Backup & Replication 11A and Microsoft System Center Data Protection Manager backup software. This Sony driver has been tested with these types of backup software up to and including Windows Server 2019.

5. In the **Select the device driver you want to install for this hardware** section, clear the **Show compatible hardware** check box, choose **Sony** in the **Manufacturer** list, choose **Sony - TSL-A500C Autoloader** in the **Model** list, and then choose **Next**.



6. In the warning box that appears, choose **Yes**. If the driver is successfully installed, close the **Update drive software** window.

## Displaying Barcodes for Tapes in Microsoft System Center DPM

If you use the media changer driver for Sony TSL-A500C Autoloader, Microsoft System Center Data Protection Manager doesn't automatically display barcodes for virtual tapes created in Storage Gateway. To display barcodes correctly for your tapes, change the media changer driver to Sun/StorageTek Library.

### To display barcodes

1. Ensure that all backup jobs have completed and that there are no tasks pending or in progress.
2. Eject and move the tapes to offline storage (GLACIER or DEEP\_ARCHIVE) and exit the DPM Administrator console. For information about how to eject a tape in DPM, see [Archiving a Tape by Using DPM \(p. 122\)](#).
3. In **Administrative Tools**, choose **Services** and open the context (right-click) menu for **DPM Service** in the **Detail** pane, and then choose **Properties**.
4. On the **General** tab, ensure that the **Startup type** is set to **Automatic** and choose **Stop** to stop the DPM service.
5. Get the StorageTek drivers from [Microsoft Update Catalog](#) on the Microsoft website.

#### Note

Take note of the different drivers for the different sizes.

For **Size 18K**, choose **x86 drivers**.

For **Size 19K**, choose **x64 drivers**.

6. On your Windows server, open Device Manager, and expand the **Medium Changer Devices** tree.
7. Open the context (right-click) menu for **Unknown Medium Changer**, and choose **Update Driver Software** to open the **Update Driver Software-unknown Medium Changer** window.
8. Browse to the path of the new driver location and install. The driver appears as **Sun/StorageTek Library**. The tape drives remain as an IBM ULT3580-TD5 SCSI sequential device.
9. Reboot the DPM server.
10. In the Storage Gateway console, create new tapes.
11. Open the DPM Administrator console, choose **Management**, then choose **Rescan for new tape libraries**. You should see the **Sun/StorageTek library**.
12. Choose the library and choose **Inventory**.
13. Choose **Add Tapes** to add the new tapes into DPM. The new tapes should now display their barcodes.

## Working With Tapes

Storage Gateway provides one virtual tape library (VTL) for each tape gateway you activate. Initially, the library contains no tapes, but you can create tapes whenever you need to. Your application can read and write to any tapes available on your tape gateway. A tape's status must be AVAILABLE for you to write to the tape. These tapes are backed by Amazon Simple Storage Service (Amazon S3)—that is, when you write to these tapes, the tape gateway stores data in Amazon S3. For more information, see [Understanding Tape Status Information in a VTL \(p. 206\)](#).

### Topics

- [Archiving Tapes \(p. 412\)](#)
- [Canceling Tape Archival \(p. 413\)](#)

The tape library shows tapes in your tape gateway. The library shows the tape barcode, status, and size, amount of the tape used, and the gateway the tape is associated with.

	Barcode	Status	Used	Size	Created	Archived	Gateway	Pool
	SHDAB56413	Retrieved	0%	100 GiB	3/19/2019, 1:55:29 PM	-	sajhus-tgw-da	Deep Archive
	SHDB6B72CD	Retrieved	0%	100 GiB	3/25/2019, 4:06:45 PM	-	sajhus-tgw-da	Deep Archive
	SHDX4172E7	Available	-	100 GiB	3/25/2019, 4:35:43 PM	-	sajhus-tgw-da	Glacier Pool
	SHDY4872EE	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive
	SHDY4972EF	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive
	SHDY4A72EC	Available	-	100 GiB	3/25/2019, 4:41:51 PM	-	sajhus-tgw-da	Deep Archive

When you have a large number of tapes in the library, the console supports searching for tapes by barcode, by status, or by both. When you search by barcode, you can filter by status and gateway.

### To search by barcode, status, and gateway

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose **Tapes**, and then type a value in the search box. The value can be the barcode, status, or gateway. By default, Storage Gateway searches for all virtual tapes. However, you can also filter your search by status.

If you filter for status, tapes that match your criteria appear in the library in the Storage Gateway console.

If you filter for gateway, tapes that are associated with that gateway appear in the library in the Storage Gateway console.

#### Note

By default, Storage Gateway displays all tapes regardless of status.

## Archiving Tapes

You can archive the virtual tapes that are in your tape gateway. When you archive a tape, Storage Gateway moves the tape to the archive.

To archive a tape, you use your backup software. Tape archival process consists of three stages, seen as the tape statuses **IN TRANSIT TO VTS**, **ARCHIVING**, and **ARCHIVED**:

- To archive a tape, use the command provided by your backup application. When the archival process begins the tape status changes to **IN TRANSIT TO VTS** and the tape is no longer accessible to your backup application. In this stage, your tape gateway is uploading data to AWS. If needed, you can cancel the archival in progress. For more information about canceling archival, see [Canceling Tape Archival \(p. 413\)](#).

#### Note

The steps for archiving a tape depend on your backup application. For detailed instructions, see the documentation for your backup application.

- After the data upload to AWS completes, the tape status changes to **ARCHIVING** and Storage Gateway begins moving the tape to the archive. You cannot cancel the archival process at this point.
- After the tape is moved to the archive, its status changes to **ARCHIVED** and you can retrieve the tape to any of your gateways. For more information about tape retrieval, see [Retrieving Archived Tapes \(p. 203\)](#).

The steps involved in archiving a tape depend on your backup software. For instructions on how to archive a tape by using Symantec NetBackup software, see [Archiving the Tape \(p. 146\)](#).

## Canceling Tape Archival

After you start archiving a tape, you might decide you need your tape back. For example, you might want to cancel the archival process, get the tape back because the archival process is taking too long, or read data from the tape. A tape that is being archived goes through three statuses, as shown following:

- IN TRANSIT TO VTS: Your tape gateway is uploading data to AWS.
- ARCHIVING: Data upload is complete and the tape gateway is moving the tape to the archive.
- ARCHIVED: The tape is moved and the archive and is available for retrieval.

You can cancel archival only when the tape's status is IN TRANSIT TO VTS. Depending on factors such as upload bandwidth and the amount of data being uploaded, this status might or might not be visible in the Storage Gateway console. To cancel a tape archival, use the [CancelRetrieval](#) action in the API reference.

## Getting an Activation Key for Your Gateway

To get an activation key for your gateway, you make a web request to the gateway VM and it returns a redirect that contains the activation key. This activation key is passed as one of the parameters to the `ActivateGateway` API action to specify the configuration of your gateway. The request you make to the gateway VM contains the AWS Region in which activation occurs.

The URL returned by the redirect in the response contains a query string parameter called `activationkey`. This query string parameter is your activation key. The format of the query string looks like the following: `http://gateway_ip_address?activationRegion=activation_region`.

### Topics

- [Linux command line interface \(CLI\) \(p. 413\)](#)
- [Microsoft Windows PowerShell \(p. 413\)](#)

## Linux command line interface (CLI)

The following example shows you how to use the Linux CLI to get the activation key.

```
curl 'ec2_instance_ip_address?activationRegion=activation_region&no_redirect'
```

## Microsoft Windows PowerShell

The following example shows you how to use Microsoft Windows PowerShell to fetch the HTTP response, parse HTTP headers, and get the activation key.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion
    )
}
```

```
PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
        $activationKeyParam = $request.Headers.Location | Select-String -Pattern "activationKey=([A-Z0-9-]+)"
        $activationKeyParam.Matches.Value.Split("=")[1]
    }
}
```

## Connecting iSCSI Initiators

When managing your gateway, you work with volumes or virtual tape library (VTL) devices that are exposed as Internet Small Computer System Interface (iSCSI) targets. For volume gateways, the iSCSI targets are volumes. For tape gateways, the targets are VTL devices. As part of this work, you do such tasks as connecting to those targets, customizing iSCSI settings, connecting from a Red Hat Linux client, and configuring Challenge-Handshake Authentication Protocol (CHAP).

### Topics

- [Connecting to Your Volumes to a Windows Client \(p. 415\)](#)
- [Connecting Your VTL Devices to a Windows client \(p. 418\)](#)
- [Connecting Your Volumes or VTL Devices to a Linux Client \(p. 422\)](#)
- [Customizing iSCSI Settings \(p. 424\)](#)
- [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#)

The iSCSI standard is an Internet Protocol (IP)-based storage networking standard for initiating and managing connections between IP-based storage devices and clients. The following list defines some of the terms that are used to describe the iSCSI connection and the components involved.

#### iSCSI initiator

The client component of an iSCSI network. The initiator sends requests to the iSCSI target. Initiators can be implemented in software or hardware. Storage Gateway only supports software initiators.

#### iSCSI target

The server component of the iSCSI network that receives and responds to requests from initiators. Each of your volumes is exposed as an iSCSI target. Connect only one iSCSI initiator to each iSCSI target.

#### Microsoft iSCSI initiator

The software program on Microsoft Windows computers that enables you to connect a client computer (that is, the computer running the application whose data you want to write to the gateway) to an external iSCSI-based array (that is, the gateway). The connection is made using the host computer's Ethernet network adapter card. The Microsoft iSCSI initiator has been validated with Storage Gateway on Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019. The initiator is built into these operating systems.

#### Red Hat iSCSI initiator

The `iscsi-initiator-utils` Resource Package Manager (RPM) package provides you with an iSCSI initiator implemented in software for Red Hat Linux. The package includes a server daemon for the iSCSI protocol.

Each type of gateway can connect to iSCSI devices, and you can customize those connections, as described following.

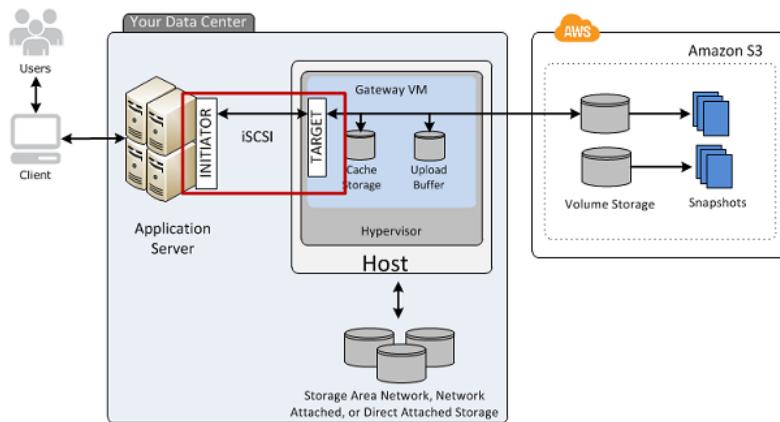
## Connecting to Your Volumes to a Windows Client

A volume gateway exposes volumes you have created for the gateway as iSCSI targets. For more information, see [Connecting Your Volumes to Your Client \(p. 75\)](#).

**Note**

To connect to your volume target, your gateway must have an upload buffer configured. If an upload buffer is not configured for your gateway, then the status of your volumes is displayed as UPLOAD BUFFER NOT CONFIGURED. To configure an upload buffer for a gateway in a stored volumes setup, see [To add and configure upload buffer or cache storage \(p. 257\)](#). To configure an upload buffer for a gateway in a cached volumes setup, see [To add and configure upload buffer or cache storage \(p. 257\)](#).

The following diagram highlights the iSCSI target in the larger picture of the Storage Gateway architecture. For more information, see [How Storage Gateway works \(architecture\) \(p. 3\)](#).



You can connect to your volume from either a Windows or Red Hat Linux client. You can optionally configure CHAP for either client type.

Your gateway exposes your volume as an iSCSI target with a name you specify, prepended by `iqn.1997-05.com.amazon:`. For example, if you specify a target name of `myvolume`, then the iSCSI target you use to connect to the volume is `iqn.1997-05.com.amazon:myvolume`. For more information about how to configure your applications to mount volumes over iSCSI, see [Connecting to Your Volumes to a Windows Client \(p. 415\)](#).

To	See
Connect to your volume from Windows.	<a href="#">Connecting Your Volumes to Your Client (p. 75)</a> in the Getting Started section
Connect to your volume from Red Hat Linux.	<a href="#">Connecting to a Microsoft Windows Client (p. 96)</a>
Configure CHAP authentication for Windows and Red Hat Linux.	<a href="#">Configuring CHAP Authentication for Your iSCSI Targets (p. 430)</a>

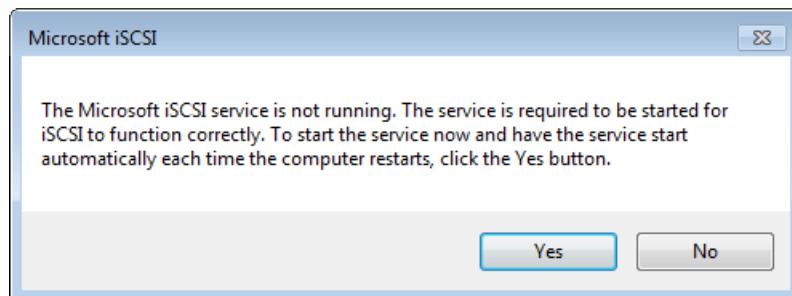
### To connect your Windows client to a storage volume

1. On the **Start** menu of your Windows client computer, enter `iscsicpl.exe` in the **Search Programs and files** box, locate the iSCSI initiator program, and then run it.

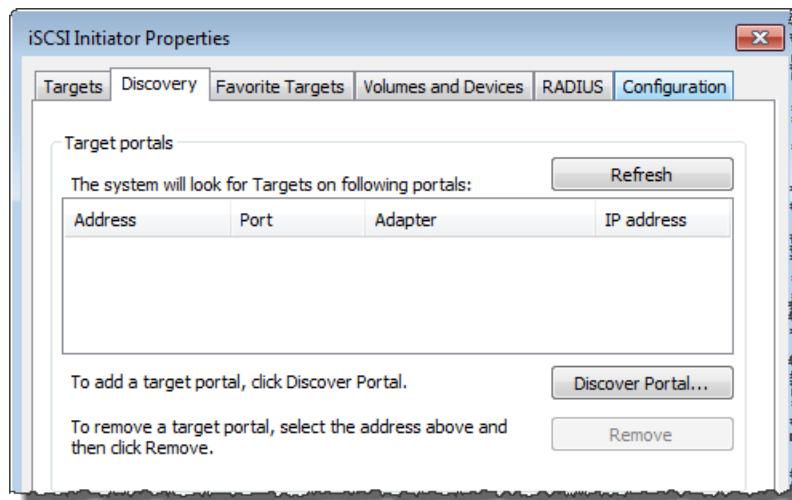
**Note**

You must have administrator rights on the client computer to run the iSCSI initiator.

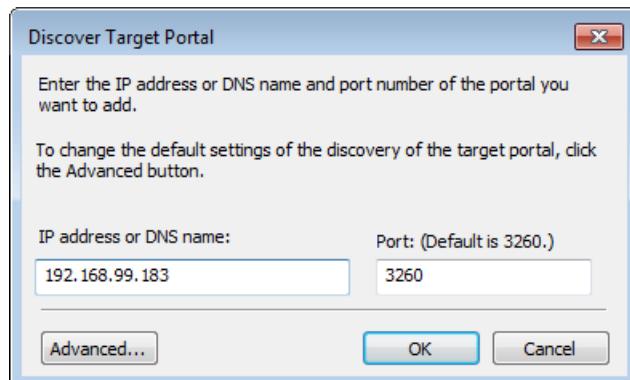
2. If prompted, choose **Yes** to start the Microsoft iSCSI initiator service.



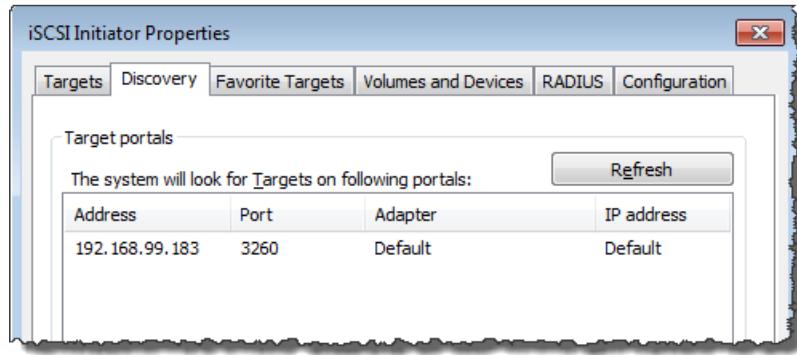
3. In the **iSCSI Initiator Properties** dialog box, choose the **Discovery** tab, and then choose **Discover Portal**.



4. In the **Discover Target Portal** dialog box, enter the IP address of your iSCSI target for **IP address or DNS name**, and then choose **OK**. To get the IP address of your gateway, check the **Gateway** tab on the Storage Gateway console. If you deployed your gateway on an Amazon EC2 instance, you can find the public IP or DNS address in the **Description** tab on the Amazon EC2 console.



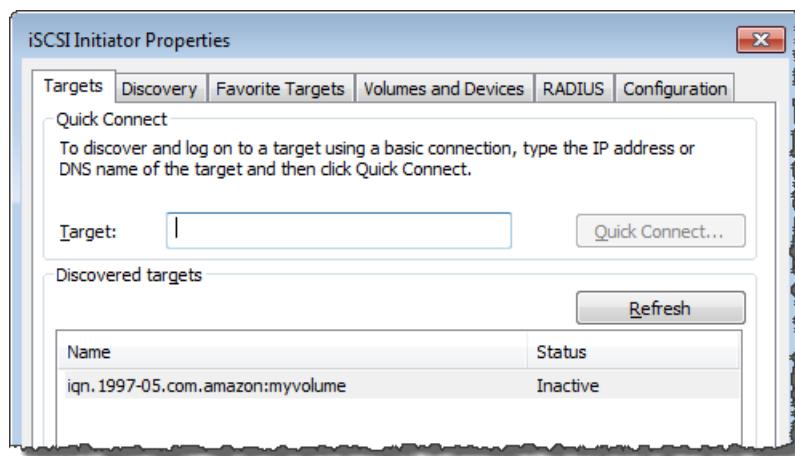
The IP address now appears in the **Target portals** list on the **Discovery** tab.



5. Connect the new target portal to the storage volume target on the gateway:

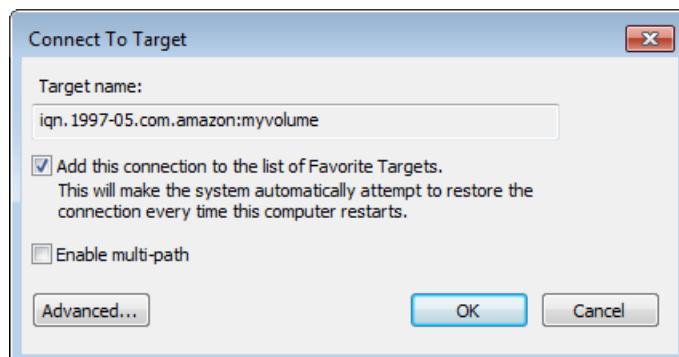
- a. Choose the **Targets** tab.

The new target portal is shown with an inactive status. The target name shown should be the same as the name that you specified for your storage volume in step 1.

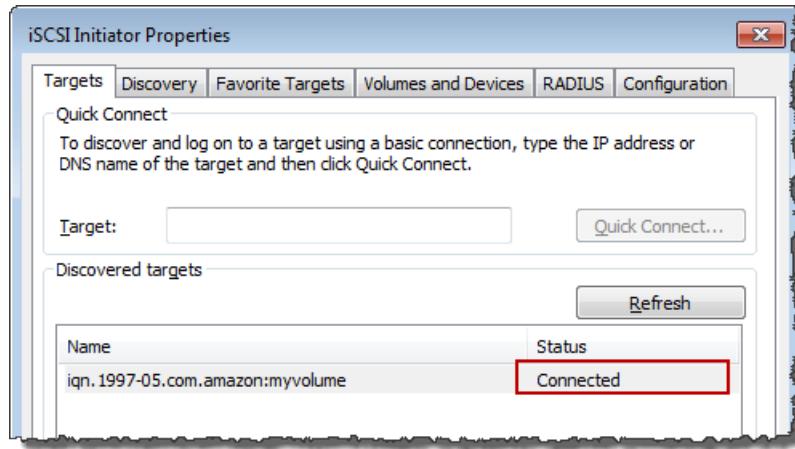


- b. Select the target, and then choose **Connect**.

If the target name is not populated already, enter the name of the target as shown in step 1. In the **Connect to Target** dialog box, select **Add this connection to the list of Favorite Targets**, and then choose **OK**.



- c. In the **Targets** tab, ensure that the target **Status** has the value **Connected**, indicating the target is connected, and then choose **OK**.



You can now initialize and format this storage volume for Windows so that you can begin saving data on it. You do this by using the Windows Disk Management tool.

**Note**

Although it is not required for this exercise, we highly recommend that you customize your iSCSI settings for a real-world application as discussed in [Customizing Your Windows iSCSI Settings \(p. 424\)](#).

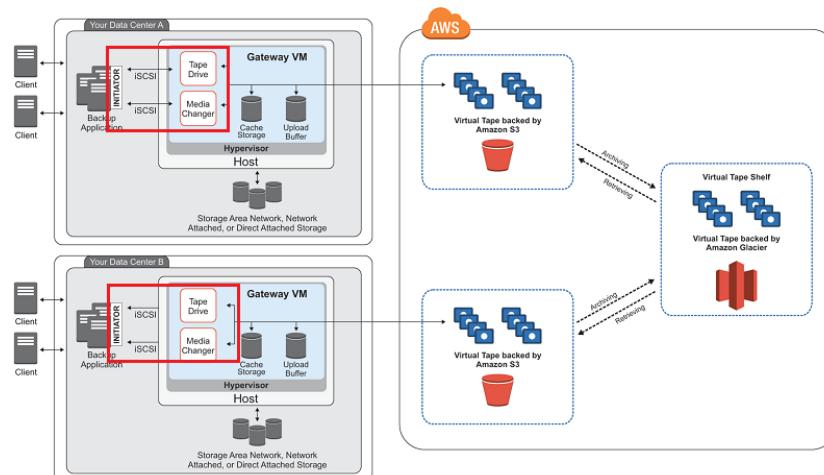
## Connecting Your VTL Devices to a Windows client

A tape gateway exposes several tape drives and a media changer, referred to collectively as VTL devices, as iSCSI targets. For more information, see [Requirements \(p. 11\)](#).

**Note**

You connect only one application to each iSCSI target.

The following diagram highlights the iSCSI target in the larger picture of the Storage Gateway architecture. For more information on Storage Gateway architecture, see [Tape gateways \(p. 7\)](#).



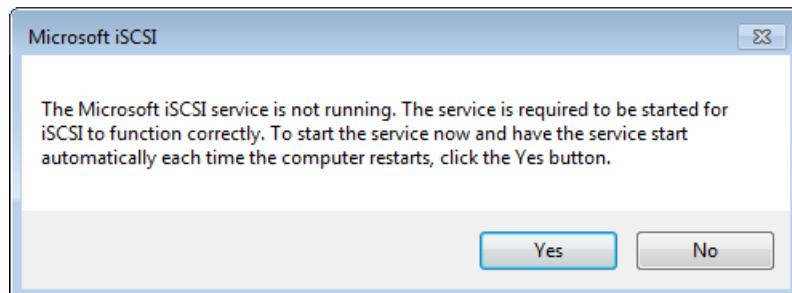
### To connect your Windows client to the VTL devices

1. On the **Start** menu of your Windows client computer, enter **iscsicpl.exe** in the **Search Programs and files** box, locate the iSCSI initiator program, and then run it.

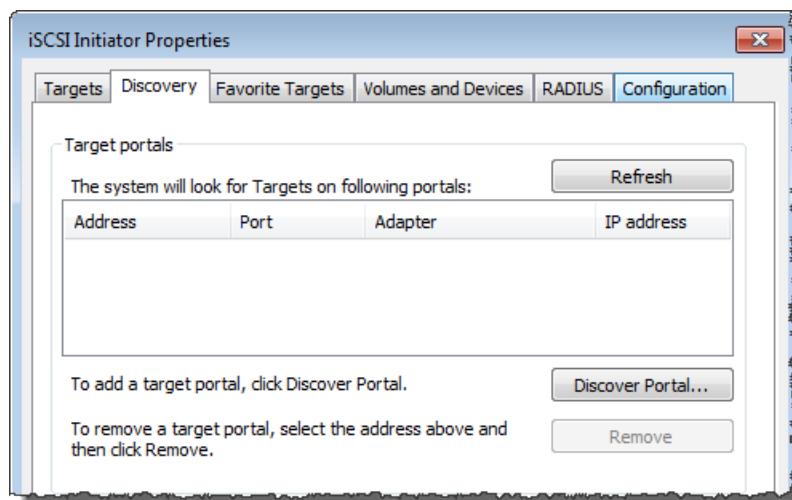
**Note**

You must have administrator rights on the client computer to run the iSCSI initiator.

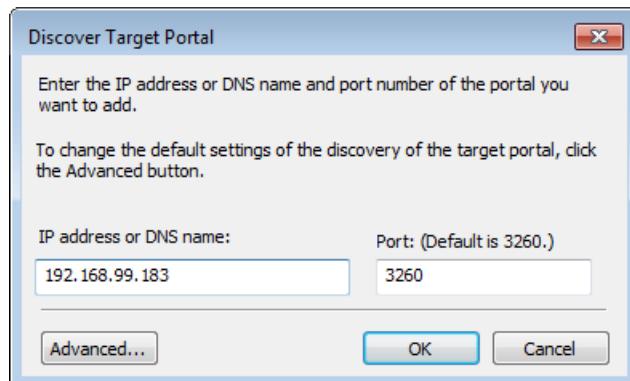
2. If prompted, choose **Yes** to start the Microsoft iSCSI initiator service.



3. In the **iSCSI Initiator Properties** dialog box, choose the **Discovery** tab, and then choose **Discover Portal**.

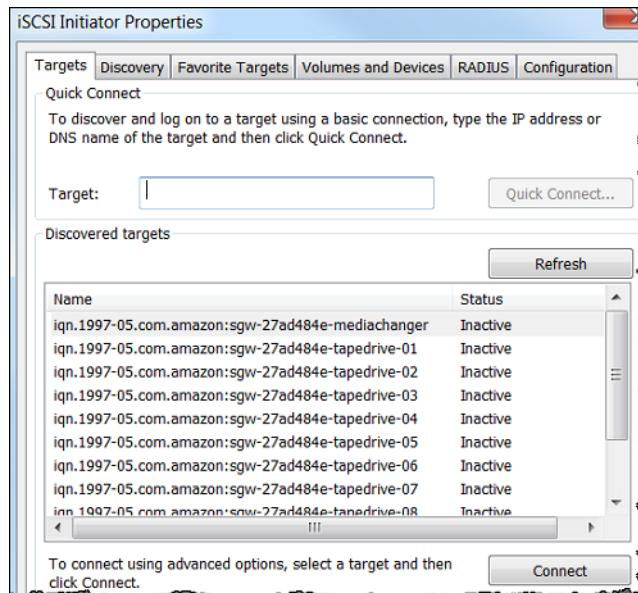


4. In the **Discover Target Portal** dialog box, enter the IP address of your tape gateway for **IP address or DNS name**, and then choose **OK**. To get the IP address of your gateway, check the **Gateway** tab on the Storage Gateway console. If you deployed your gateway on an Amazon EC2 instance, you can find the public IP or DNS address in the **Description** tab on the Amazon EC2 console.



5. Choose the **Targets** tab, and then choose **Refresh**. All 10 tape drives and the media changer appear in the **Discovered targets** box. The status for the targets is **Inactive**.

The following screenshot shows the discovered targets.

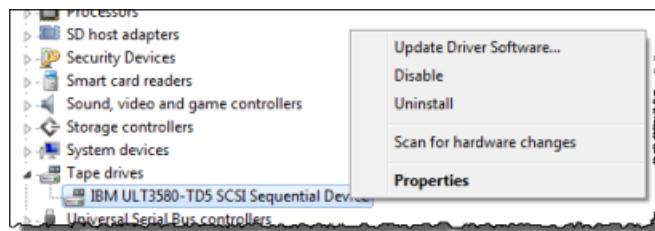


6. Select the first device and choose **Connect**. You connect the devices one at a time.
7. In the **Connect to Target** dialog box, choose **OK**.
8. Repeat steps 6 and 7 for each of the devices to connect all of them, and then choose **OK** in the **iSCSI Initiator Properties** dialog box.

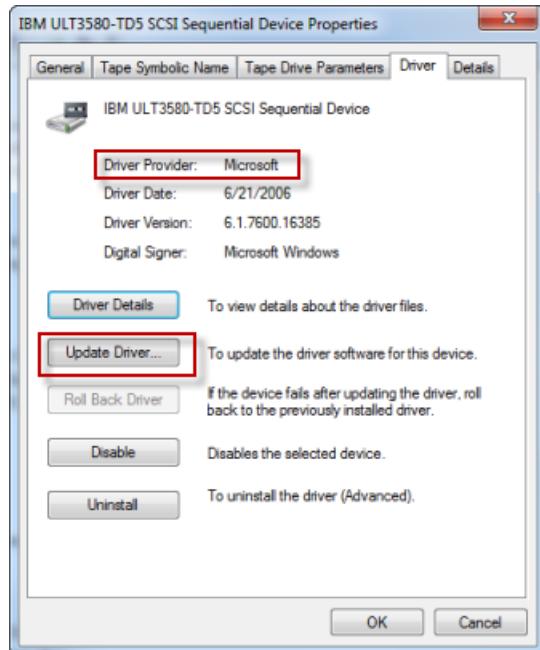
On a Windows client, the driver provider for the tape drive must be Microsoft. Use the following procedure to verify the driver provider, and update the driver and provider if necessary.

#### To verify the driver provider and (if necessary) update the provider and driver on a Windows client

1. On your Windows client, start Device Manager.
2. Expand **Tape drives**, choose the context (right-click) menu for a tape drive, and choose **Properties**.

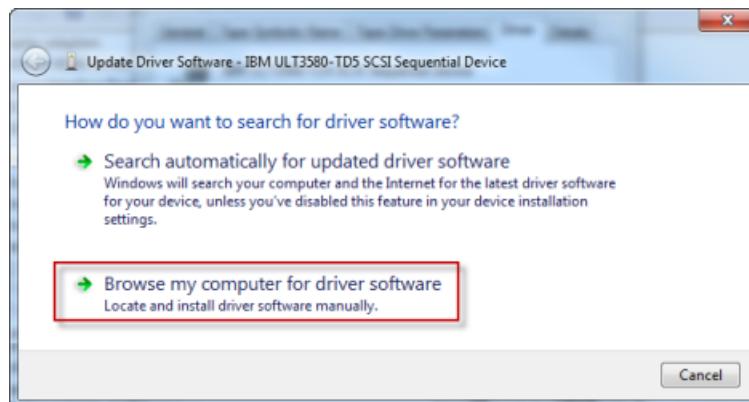


3. In the **Driver** tab of the **Device Properties** dialog box, verify that **Driver Provider** is **Microsoft**.

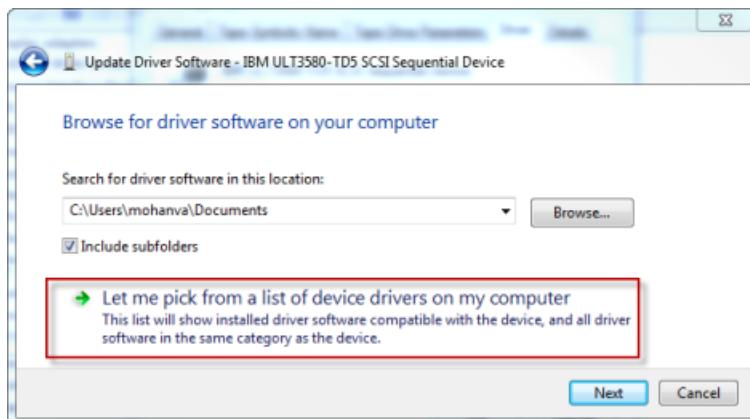


4. If **Driver Provider** is not **Microsoft**, set the value as follows:

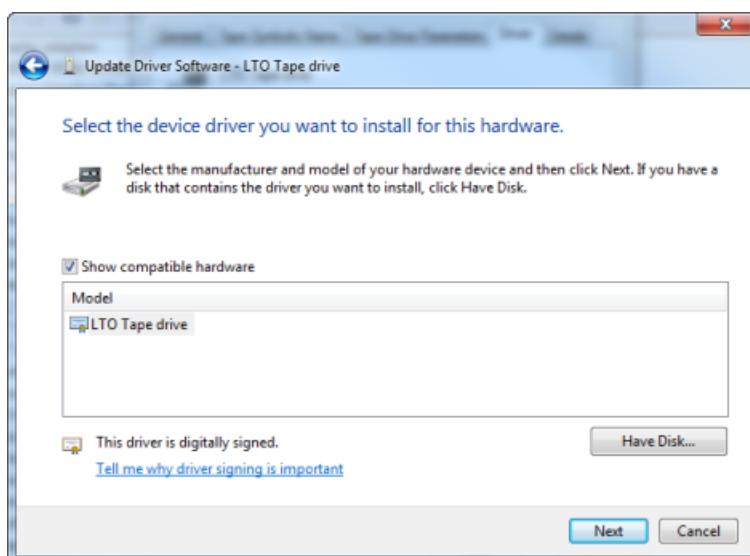
- Choose **Update Driver**.
- In the **Update Driver Software** dialog box, choose **Browse my computer for driver software**.



- In the **Update Driver Software** dialog box, choose **Let me pick from a list of device drivers on my computer**.



- d. Select **LTO Tape drive** and choose **Next**.



- e. Choose **Close** to close the **Update Driver Software** window, and verify that the **Driver Provider** value is now set to **Microsoft**.  
5. Repeat steps 4.1 through 4.5 to update all the tape drives.

## Connecting Your Volumes or VTL Devices to a Linux Client

When using Red Hat Enterprise Linux (RHEL), you use the `iscsi-initiator-utils` RPM package to connect to your gateway iSCSI targets (volumes or VTL devices).

### To connect a Linux client to the iSCSI targets

1. Install the `iscsi-initiator-utils` RPM package, if it isn't already installed on your client.

You can use the following command to install the package.

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

2. Ensure that the iSCSI daemon is running.

- a. Verify that the iSCSI daemon is running using one of the following commands.

For RHEL 5 or 6, use the following command.

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

For RHEL 7, use the following command.

```
sudo service iscsid status
```

- b. If the status command doesn't return a status of *running*, start the daemon using one of the following commands.

For RHEL 5 or 6, use the following command.

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

For RHEL 7, use the following command. For RHEL 7, you usually don't need to explicitly start the `iscsid` service.

```
sudo service iscsid start
```

3. To discover the volume or VTL device targets defined for a gateway, use the following discovery command.

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

Substitute your gateway's IP address for the `[GATEWAY_IP]` variable in the preceding command. You can find the gateway IP in the **iSCSI Target Info** properties of a volume on the Storage Gateway console.

The output of the discovery command will look like the following example output.

For volume gateways: `[GATEWAY_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume`

For tape gateways: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

Your iSCSI qualified name (IQN) will be different than what is shown preceding, because IQN values are unique to an organization. The name of the target is the name that you specified when you created the volume. You can also find this target name in the **iSCSI Target Info** properties pane when you select a volume on the Storage Gateway console.

4. To connect to a target, use the following command.

Note that you need to specify the correct `[GATEWAY_IP]` and IQN in the connect command.

**Warning**

For gateways that are deployed on an Amazon EC2 instance, accessing the gateway over a public internet connection is not supported. The Elastic IP address of the Amazon EC2 instance cannot be used as the target address.

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

5. To verify that the volume is attached to the client machine (the initiator), use the following command.

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

The output of the command will look like the following example output.

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

*For volume gateways only:* We highly recommend that after you set up your initiator, you customize your iSCSI settings as discussed in [Customizing Your Linux iSCSI Settings \(p. 428\)](#).

## Customizing iSCSI Settings

After you set up your initiator, we highly recommend that you customize your iSCSI settings to prevent the initiator from disconnecting from targets.

By increasing the iSCSI timeout values as shown in the following steps, you make your application better at dealing with write operations that take a long time and other transient issues such as network interruptions.

### Note

Before making changes to the registry, you should make a backup copy of the registry. For information on making a backup copy and other best practices to follow when working with the registry, see [Registry best practices](#) in the *Microsoft TechNet Library*.

### Topics

- [Customizing Your Windows iSCSI Settings \(p. 424\)](#)
- [Customizing Your Linux iSCSI Settings \(p. 428\)](#)
- [Customizing Your Linux Disk Timeout Settings for Volume Gateways \(p. 429\)](#)

## Customizing Your Windows iSCSI Settings

When using a Windows client, you use the Microsoft iSCSI initiator to connect to your gateway volume. For instructions on how to connect to your volumes, see [Connecting Your Volumes to Your Client \(p. 75\)](#).

For a tape gateway setup, connecting to your VTL devices by using a Microsoft iSCSI initiator is a two-step process:

1. Connect your tape gateway devices to your Windows client.
2. If you are using a backup application, configure the application to use the devices.

The Getting Started example setup provides instructions for both these steps. It uses the Symantec NetBackup backup application. For more information, see [Connecting Your VTL Devices \(p. 96\)](#) and [Configuring NetBackup Storage Devices \(p. 137\)](#).

### To customize your Windows iSCSI settings

1. Increase the maximum time for which requests are queued.
  - a. Start Registry Editor (`Regedit.exe`).
  - b. Navigate to the globally unique identifier (GUID) key for the device class that contains iSCSI controller settings, shown following.

**Warning**

Make sure that you are working in the **CurrentControlSet** subkey and not another control set, such as **ControlSet001** or **ControlSet002**.

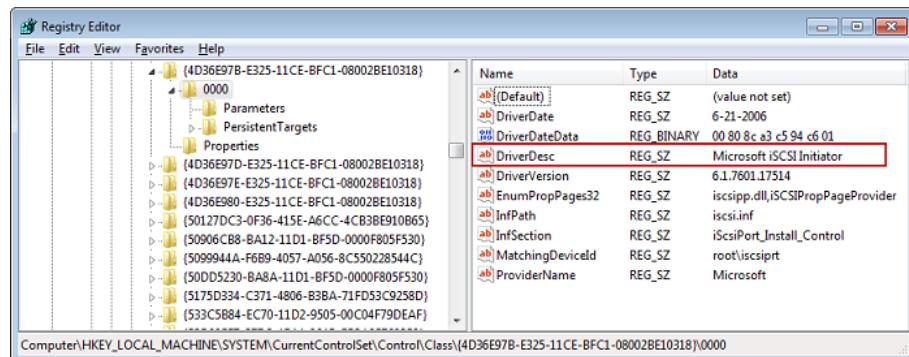
HKEY\_Local\_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}

- c. Find the subkey for the Microsoft iSCSI initiator, shown following as [*<Instance Number>*].

The key is represented by a four-digit number, such as 0000.

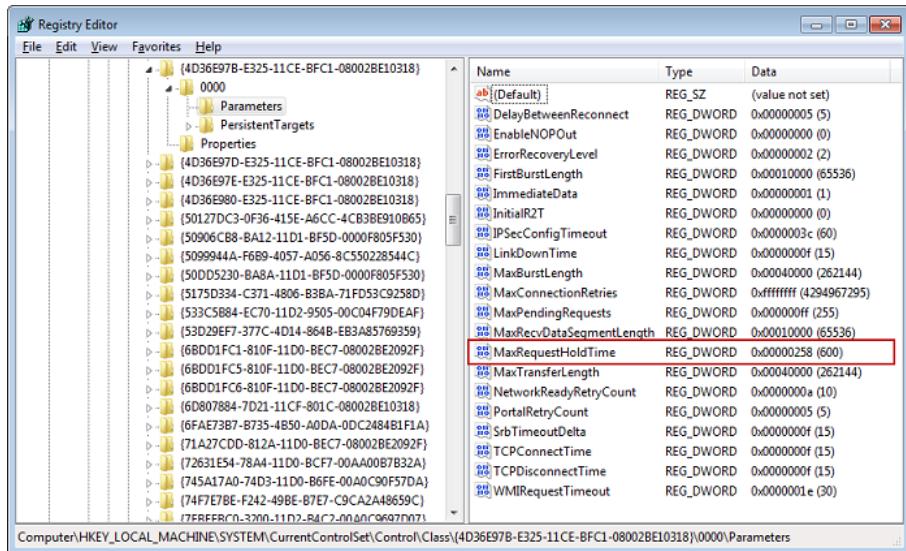
HKEY\_Local\_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[*<Instance Number>*]

Depending on what is installed on your computer, the Microsoft iSCSI initiator might not be the subkey 0000. You can ensure that you have selected the correct subkey by verifying that the string **DriverDesc** has the value **Microsoft iSCSI Initiator**, as shown in the following example.

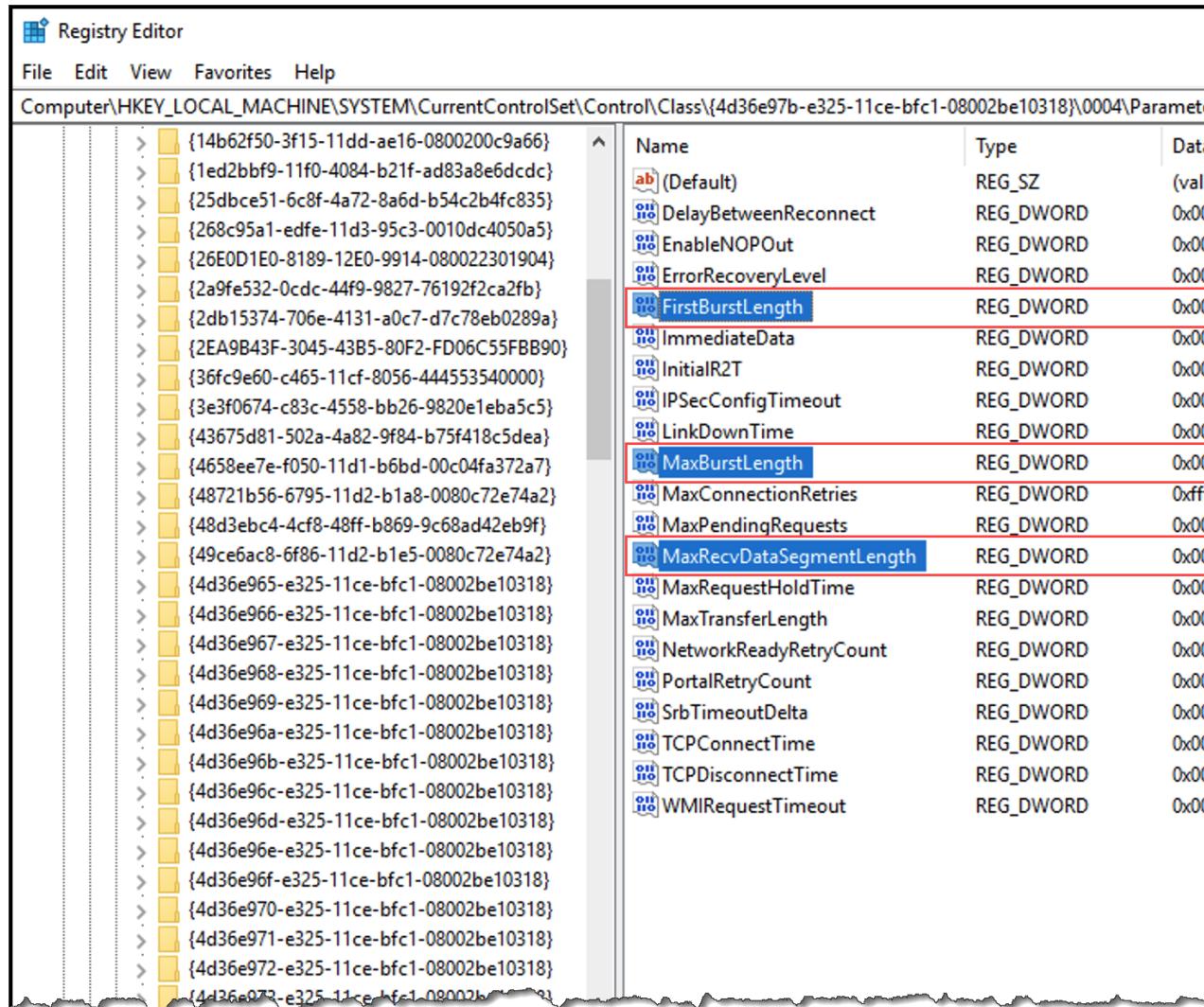


- d. To show the iSCSI settings, choose the **Parameters** subkey.  
e. Open the context (right-click) menu for the **MaxRequestHoldTime** DWORD (32-bit) value, choose **Modify**, and then change the value to **600**.

This value represents a hold time of 600 seconds. The example following shows the **MaxRequestHoldTime** DWORD value with a value of 600.



2. You can increase the maximum amount of data that can be sent in iSCSI packets by modifying the following parameters:
  - **FirstBurstLength** controls the maximum amount of data that can be transmitted in an unsolicited write request. Set this value to **262144** if the original value is smaller.
  - **MaxBurstLength** is similar to **FirstBurstLength**, but it sets the maximum amount of data that can be transmitted in solicited write sequences. Set this value to **1048576** if the original value is smaller.
  - **MaxRecvDataSegmentLength** controls the maximum data segment size that is associated with a single protocol data unit (PDU). Set this value to **262144** if the original value is smaller.

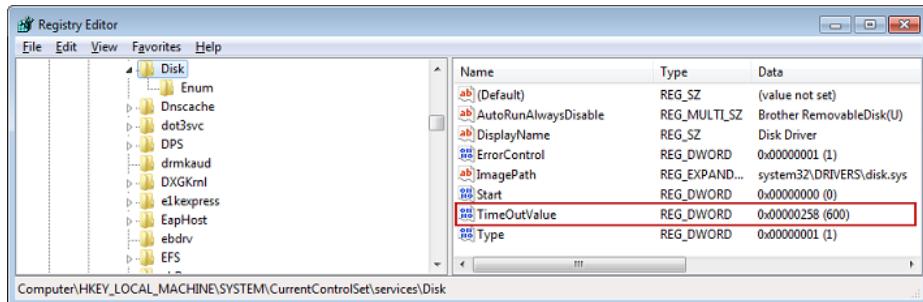


#### Note

Different backup software can be optimized to work best using different iSCSI settings. To verify which values for these parameters will provide the best performance, see the documentation for your backup software.

3. Increase the disk timeout value, as shown following:
    - a. Start Registry Editor (`Regedit.exe`), if you haven't already.
    - b. Navigate to the **Disk** subkey in the **Services** subkey of the **CurrentControlSet**, shown following.
- HKEY\_Local\_Machine\SYSTEM\CurrentControlSet\Services\Disk
- c. Open the context (right-click) menu for the **TimeOutValue** DWORD (32-bit) value, choose **Modify**, and then change the value to **600**.

This value represents a timeout of 600 seconds. The example following shows the **TimeOutValue** DWORD value with a value of 600.



- To ensure that the new configuration values take effect, restart your system.

Before restarting, you must make sure that the results of all write operations to volumes are flushed. To do this, take any mapped storage volume disks offline before restarting.

## Customizing Your Linux iSCSI Settings

After setting up the initiator for your gateway, we highly recommend that you customize your iSCSI settings to prevent the initiator from disconnecting from targets. By increasing the iSCSI timeout values as shown following, you make your application better at dealing with write operations that take a long time and other transient issues such as network interruptions.

### Note

Commands might be slightly different for other types of Linux. The following examples are based on Red Hat Linux.

### To customize your Linux iSCSI settings

- Increase the maximum time for which requests are queued.

- Open the /etc/iscsi/iscsid.conf file and find the following lines.

```
node.session.timeout.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeout.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeout.noop_out_timeout = [noop_out_timeout_value]
```

- Set the *[replacement\_timeout\_value]* value to **600**.

Set the *[noop\_out\_interval\_value]* value to **60**.

Set the *[noop\_out\_timeout\_value]* value to **600**.

All three values are in seconds.

### Note

The iscsid.conf settings must be made before discovering the gateway. If you have already discovered your gateway or logged in to the target, or both, you can delete the entry from the discovery database using the following command. Then you can rediscover or log in again to pick up the new configuration.

```
iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
```

- Increase the maximum values for the amount of data that can be transmitted in each response.

- Open the /etc/iscsi/iscsid.conf file and find the following lines.

```
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. We recommend the following values to achieve better performance. Your backup software might be optimized to use different values, so see your backup software documentation for best results.

Set the *[replacement\_first\_burst\_length\_value]* value to **262144** if the original value is smaller.

Set the *[replacement\_max\_burst\_length\_value]* value to **1048576** if the original value is smaller.

Set the *[replacement\_segment\_length\_value]* value to **262144** if the original value is smaller.

**Note**

Different backup software can be optimized to work best using different iSCSI settings. To verify which values for these parameters will provide the best performance, see the documentation for your backup software.

3. Restart your system to ensure that the new configuration values take effect.

Before restarting, make sure that the results of all write operations to your tapes are flushed. To do this, unmount tapes before restarting.

## Customizing Your Linux Disk Timeout Settings for Volume Gateways

If you are using a volume gateway, you can customize the following Linux disk timeout settings in addition to the iSCSI settings described in the preceding section.

### To customize your Linux disk timeout settings

1. Increase the disk timeout value in the rules file.

- a. If you are using the RHEL 5 initiator, open the `/etc/udev/rules.d/50-udev.rules` file, and find the following line.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

This rules file does not exist in RHEL 6 or 7 initiators, so you must create it using the following rule.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

To modify the timeout value in RHEL 6, use the following command, and then add the lines of code shown preceding.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

To modify the timeout value in RHEL 7, use the following command, and then add the lines of code shown preceding.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

- b. Set the [**timeout**] value to **600**.

This value represents a timeout of 600 seconds.

2. Restart your system to ensure that the new configuration values take effect.

Before restarting, make sure that the results of all write operations to your volumes are flushed. To do this, unmount storage volumes before restarting.

3. You can test the configuration by using the following command.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

This command shows the udev rules that are applied to the iSCSI device.

## Configuring CHAP Authentication for Your iSCSI Targets

Storage Gateway supports authentication between your gateway and iSCSI initiators by using Challenge-Handshake Authentication Protocol (CHAP). CHAP provides protection against playback attacks by periodically verifying the identity of an iSCSI initiator as authenticated to access a volume and VTL device target.

**Note**

CHAP configuration is optional but highly recommended.

To set up CHAP, you must configure it both on the Storage Gateway console and in the iSCSI initiator software that you use to connect to the target. Storage Gateway uses mutual CHAP, which is when the initiator authenticates the target and the target authenticates the initiator.

### To set up mutual CHAP for your targets

1. Configure CHAP on the Storage Gateway console, as discussed in [To configure CHAP for a volume target on the Storage Gateway console \(p. 430\)](#).
2. In your client initiator software, complete the CHAP configuration:
  - To configure mutual CHAP on a Windows client, see [To configure mutual CHAP on a Windows client \(p. 432\)](#).
  - To configure mutual CHAP on a Red Hat Linux client, see [To configure mutual CHAP on a Red Hat Linux client \(p. 435\)](#).

### To configure CHAP for a volume target on the Storage Gateway console

In this procedure, you specify two secret keys that are used to read and write to a volume. These same keys are used in the procedure to configure the client initiator.

1. On the Storage Gateway console, choose **Volumes** in the navigation pane.
2. For **Actions**, choose **Configure CHAP Authentication**.
3. Provide the requested information in the **Configure CHAP Authentication** dialog box.
  - a. For **Initiator Name**, enter the name of your iSCSI initiator. This name is an Amazon iSCSI qualified name (IQN) that is prepended by `iqn.1997-05.com.amazon:` followed by the target name. The following is an example.

`iqn.1997-05.com.amazon:your-volume-name`

You can find the initiator name by using your iSCSI initiator software. For example, for Windows clients, the name is the value on the **Configuration** tab of the iSCSI initiator. For more information, see [To configure mutual CHAP on a Windows client \(p. 432\)](#).

**Note**

To change an initiator name, you must first disable CHAP, change the initiator name in your iSCSI initiator software, and then enable CHAP with the new name.

- b. For **Secret used to Authenticate Initiator**, enter the secret requested.

This secret must be a minimum of 12 characters and a maximum of 16 characters long. This value is the secret key that the initiator (that is, the Windows client) must know to participate in CHAP with the target.

- c. For **Secret used to Authenticate Target (Mutual CHAP)**, enter the secret requested.

This secret must be a minimum of 12 characters and a maximum of 16 characters long. This value is the secret key that the target must know to participate in CHAP with the initiator.

**Note**

The secret used to authenticate the target must be different than the secret to authenticate the initiator.

- d. Choose **Save**.

4. Choose the **Details** tab and confirm that **iSCSI CHAP authentication** is set to **true**.



## To configure CHAP for a VTL device target on the Storage Gateway console

In this procedure, you specify two secret keys that are used to read and write to a virtual tape. These same keys are used in the procedure to configure the client initiator.

1. In the navigation pane, choose **Gateways**.
2. Choose your gateway, and then choose the **VTL Devices** tab to display all your VTL devices.
3. Choose the device that you want to configure CHAP for.
4. Provide the requested information in the **Configure CHAP Authentication** dialog box.
  - a. For **Initiator Name**, enter the name of your iSCSI initiator. This name is an Amazon iSCSI qualified name (IQN) that is prepended by `iqn.1997-05.com.amazon:` followed by the target name. The following is an example.

`iqn.1997-05.com.amazon:your-tape-device-name`

You can find the initiator name by using your iSCSI initiator software. For example, for Windows clients, the name is the value on the **Configuration** tab of the iSCSI initiator. For more information, see [To configure mutual CHAP on a Windows client \(p. 432\)](#).

**Note**

To change an initiator name, you must first disable CHAP, change the initiator name in your iSCSI initiator software, and then enable CHAP with the new name.

- b. For **Secret used to Authenticate Initiator**, enter the secret requested.

This secret must be a minimum of 12 characters and a maximum of 16 characters long. This value is the secret key that the initiator (that is, the Windows client) must know to participate in CHAP with the target.

- c. For **Secret used to Authenticate Target (Mutual CHAP)**, enter the secret requested.

This secret must be a minimum of 12 characters and a maximum of 16 characters long. This value is the secret key that the target must know to participate in CHAP with the initiator.

**Note**

The secret used to authenticate the target must be different than the secret to authenticate the initiator.

- d. Choose **Save**.

5. On the **VTL Devices** tab, confirm that the iSCSI CHAP authentication field is set to **true**.

### To configure mutual CHAP on a Windows client

In this procedure, you configure CHAP in the Microsoft iSCSI initiator using the same keys that you used to configure CHAP for the volume on the console.

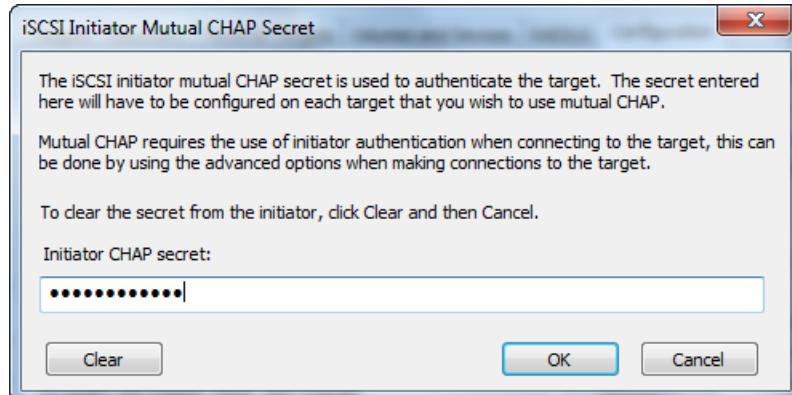
1. If the iSCSI initiator is not already started, on the **Start** menu of your Windows client computer, choose **Run**, enter **iscsicpl.exe**, and then choose **OK** to run the program.
2. Configure mutual CHAP configuration for the initiator (that is, the Windows client):
  - a. Choose the **Configuration** tab.

**Note**

The **Initiator Name** value is unique to your initiator and company. The name shown preceding is the value that you used in the **Configure CHAP Authentication** dialog box of the Storage Gateway console.

The name shown in the example image is for demonstration purposes only.

- b. Choose **CHAP**.
- c. In the **iSCSI Initiator Mutual Chap Secret** dialog box, enter the mutual CHAP secret value.

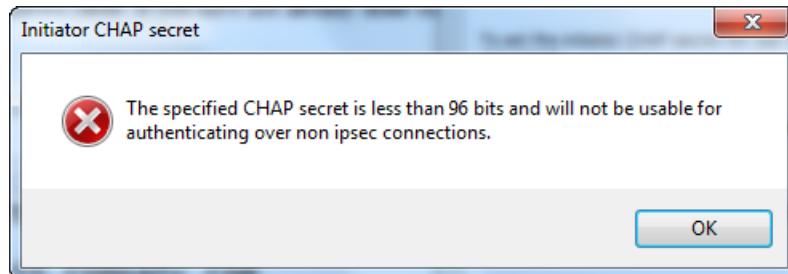


In this dialog box, you enter the secret that the initiator (the Windows client) uses to authenticate the target (the storage volume). This secret allows the target to read and write to

the initiator. This secret is the same as the secret entered into the **Secret used to Authenticate Target (Mutual CHAP)** box in the **Configure CHAP Authentication** dialog box. For more information, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).

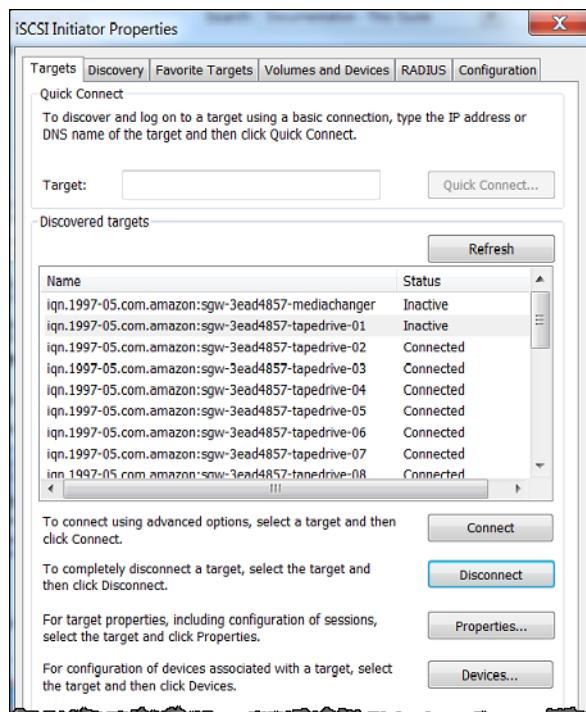
- d. If the key that you entered is fewer than 12 characters or more than 16 characters long, an **Initiator CHAP secret** error dialog box appears.

Choose **OK**, and then enter the key again.

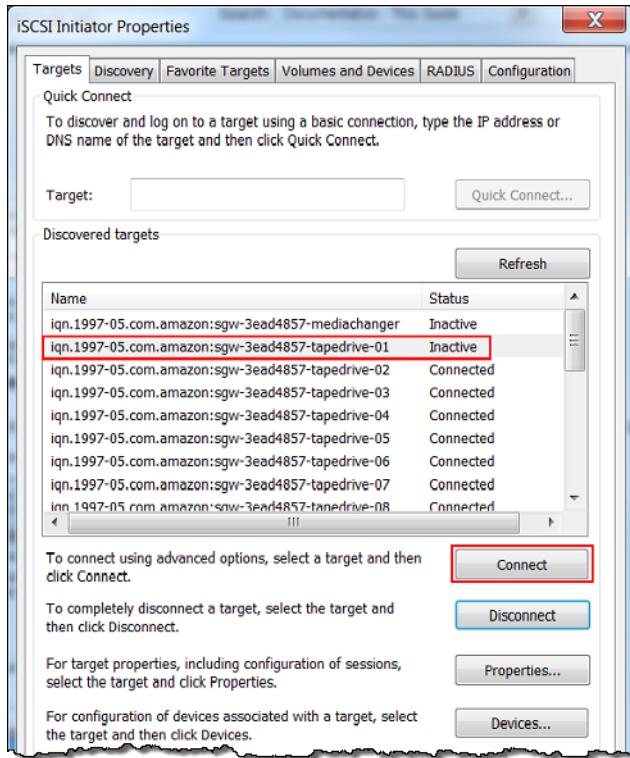


3. Configure the target with the initiator's secret to complete the mutual CHAP configuration.

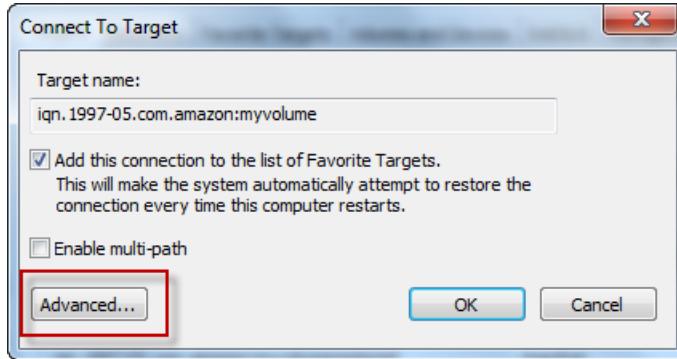
- a. Choose the **Targets** tab.



- b. If the target that you want to configure for CHAP is currently connected, disconnect the target by selecting it and choosing **Disconnect**.
- c. Select the target that you want to configure for CHAP, and then choose **Connect**.



- d. In the **Connect to Target** dialog box, choose **Advanced**.

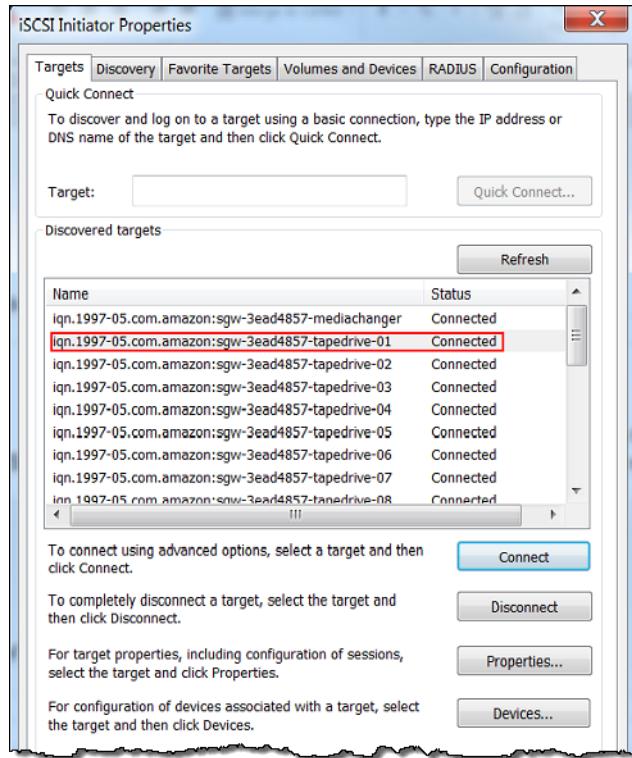


- e. In the **Advanced Settings** dialog box, configure CHAP.

- Select **Enable CHAP log on**.
- Enter the secret that is required to authenticate the initiator. This secret is the same as the secret entered into the **Secret used to Authenticate Initiator** box in the **Configure CHAP Authentication** dialog box. For more information, see [Configuring CHAP Authentication for Your iSCSI Targets \(p. 430\)](#).
- Select **Perform mutual authentication**.
- To apply the changes, choose **OK**.

- f. In the **Connect to Target** dialog box, choose **OK**.

4. If you provided the correct secret key, the target shows a status of **Connected**.



### To configure mutual CHAP on a Red Hat Linux client

In this procedure, you configure CHAP in the Linux iSCSI initiator using the same keys that you used to configure CHAP for the volume on the Storage Gateway console.

1. Ensure that the iSCSI daemon is running and that you have already connected to a target. If you have not completed these two tasks, see [Connecting to a Microsoft Windows Client \(p. 96\)](#).
2. Disconnect and remove any existing configuration for the target for which you are about to configure CHAP.
  - a. To find the target name and ensure it is a defined configuration, list the saved configurations using the following command.

```
sudo /sbin/iscsiadm --mode node
```

- b. Disconnect from the target.

The following command disconnects from the target named **myvolume** that is defined in the Amazon iSCSI qualified name (IQN). Change the target name and IQN as required for your situation.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
iqn.1997-05.com.amazon:myvolume
```

- c. Remove the configuration for the target.

The following command removes the configuration for the **myvolume** target.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname
iqn.1997-05.com.amazon:myvolume
```

3. Edit the iSCSI configuration file to enable CHAP.

- Get the name of the initiator (that is, the client you are using).

The following command gets the initiator name from the `/etc/iscsi/initiatorname.iscsi` file.

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

The output from this command looks like this:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

- Open the `/etc/iscsi/iscsid.conf` file.
- Uncomment the following lines in the file and specify the correct values for `username`, `password`, `username_in`, and `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
```

For guidance on what values to specify, see the following table.

Configuration Setting	Value
<code>username</code>	The initiator name that you found in a previous step in this procedure. The value starts with <code>iqn</code> . For example, <code>iqn.1994-05.com.redhat:8e89b27b5b8</code> is a valid <code>username</code> value.
<code>password</code>	The secret key used to authenticate the initiator (the client you are using) when it communicates with the volume.
<code>username_in</code>	The IQN of the target volume. The value starts with <code>iqn</code> and ends with the target name. For example, <code>iqn.1997-05.com.amazon:myvolume</code> is a valid <code>username_in</code> value.
<code>password_in</code>	The secret key used to authenticate the target (the volume) when it communicates to the initiator.

- Save the changes in the configuration file, and then close the file.
- Discover and log in to the target. To do so, follow the steps in [Connecting to a Microsoft Windows Client \(p. 96\)](#).

# Using AWS Direct Connect with Storage Gateway

AWS Direct Connect links your internal network to the Amazon Web Services Cloud. By using AWS Direct Connect with Storage Gateway, you can create a connection for high-throughput workload needs, providing a dedicated network connection between your on-premises gateway and AWS.

Storage Gateway uses public endpoints. With an AWS Direct Connect connection in place, you can create a public virtual interface to allow traffic to be routed to the Storage Gateway endpoints. The public virtual interface bypasses internet service providers in your network path. The Storage Gateway service public endpoint can be in the same AWS Region as the AWS Direct Connect location, or it can be in a different AWS Region.

The following illustration shows an example of how AWS Direct Connect works with Storage Gateway.

The following procedure assumes that you have created a functioning gateway.

## To use AWS Direct Connect with Storage Gateway

1. Create and establish an AWS Direct Connect connection between your on-premises data center and your Storage Gateway endpoint. For more information about how to create a connection, see [Getting Started with](#) in the *AWS Direct Connect User Guide*.
2. Connect your on-premises Storage Gateway appliance to the AWS Direct Connect router.
3. Create a public virtual interface, and configure your on-premises router accordingly. For more information, see [Creating a Virtual Interface](#) in the *AWS Direct Connect User Guide*.

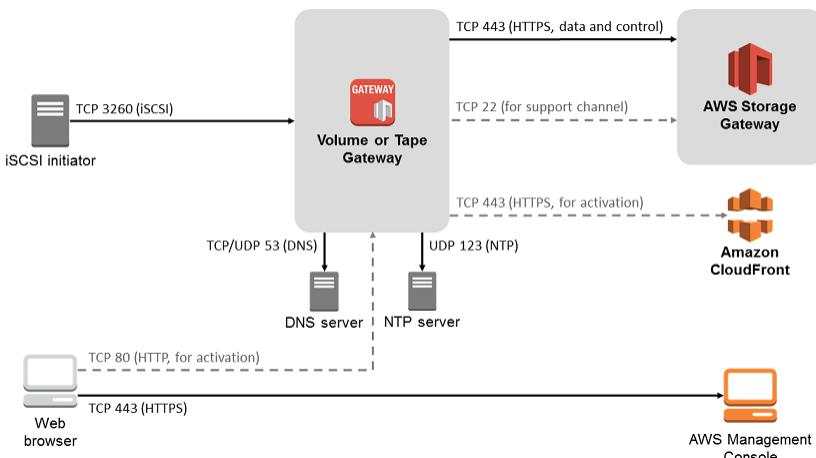
For details about AWS Direct Connect, see [What is AWS Direct Connect?](#) in the *AWS Direct Connect User Guide*.

# Port Requirements

Storage Gateway requires the following ports for its operation. Some ports are common to and required by all gateway types. Other ports are required by specific gateway types. In this section, you can find an illustration and a list of the required ports for tape and volume gateways.

## Volume Gateways and Tape Gateways

The following illustration shows all of the ports you need to open for volume and tape gateway operation.



The following ports are common to and required by all gateway types.

<b>From</b>	<b>To</b>	<b>Protocol</b>	<b>Port</b>	<b>How Used</b>	
Storage Gateway VM	AWS	Transmission Control Protocol (TCP)	443 (HTTPS)	For communication from an Storage Gateway VM to an AWS service endpoint. For information about service endpoints, see <a href="#">Allowing AWS Storage Gateway access through firewalls and routers (p. 20)</a> .	
Your web browser	Storage Gateway VM	TCP	80 (HTTP)	<p>By local systems to obtain the Storage Gateway activation key. Port 80 is used only during activation of a Storage Gateway appliance.</p> <p>A Storage Gateway VM doesn't require port 80 to be publicly accessible. The required level of access to port 80 depends on your network configuration. If you activate your gateway from the Storage Gateway Management Console, the host from which you connect to the console must</p>	

From	To	Protocol	Port	How Used	
				have access to your gateway's port 80.	
Storage Gateway VM	Domain Name Service (DNS) server	User Datagram Protocol (UDP)/UDP	53 (DNS)	For communication between a Storage Gateway VM and the DNS server.	
Storage Gateway VM	AWS	TCP	22 (Support channel)	Allows AWS Support to access your gateway to help you with troubleshooting gateway issues. You don't need this port open for the normal operation of your gateway, but it is required for troubleshooting.	
Storage Gateway VM	Network Time Protocol (NTP) server	UDP	123 (NTP)	Used by local systems to synchronize VM time to the host time. A Storage Gateway VM is configured to use the following NTP servers: <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>	
Storage Gateway Hardware Appliance	Hypertext Transfer Protocol (HTTP) proxy	TCP	8080 (HTTP)	Required briefly for activation.	

In addition to the common ports, volume and tape gateways also require the following ports.

From	To	Protocol	Port	How Used	
iSCSI initiators	Storage Gateway VM	TCP	3260 (iSCSI)	By local systems to connect to iSCSI targets exposed by a gateway.	

## Connecting to Your Gateway

After you choose a host and deploy your gateway VM, you connect and activate your gateway. To do this, you need the IP address of your gateway VM. You get the IP address from your gateway's local console. You log in to the local console and get the IP address from the top of the console page.

For gateways deployed on-premises, you can also get the IP address from your hypervisor. For Amazon EC2 gateways, you can also get the IP address of your Amazon EC2 instance from the Amazon EC2 Management Console. To find how to get your gateway's IP address, see one of the following:

- VMware host: [Accessing the Gateway Local Console with VMware ESXi \(p. 312\)](#)
- HyperV host: [Access the Gateway Local Console with Microsoft Hyper-V \(p. 313\)](#)
- Linux Kernel-based Virtual Machine (KVM) host: [Accessing the Gateway Local Console with Linux KVM \(p. 310\)](#)
- EC2 host: [Getting an IP Address from an Amazon EC2 Host \(p. 440\)](#)

When you locate the IP address, take note of it. Then return to the Storage Gateway console and type the IP address into the console.

## Getting an IP Address from an Amazon EC2 Host

To get the IP address of the Amazon EC2 instance your gateway is deployed on, log in to the EC2 instance's local console. Then get the IP address from the top of the console page. For instructions, see [Logging In to Your Amazon EC2 Gateway Local Console \(p. 304\)](#).

You can also get the IP address from the Amazon EC2 Management Console. We recommend using the public IP address for activation. To get the public IP address, use procedure 1. If you choose to use the elastic IP address instead, see procedure 2.

### Procedure 1: To connect to your gateway using the public IP address

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then select the EC2 instance that your gateway is deployed on.
3. Choose the **Description** tab at the bottom, and then note the public IP. You use this IP address to connect to the gateway. Return to the Storage Gateway console and type in the IP address.

If you want to use the elastic IP address for activation, use the procedure following.

### Procedure 2: To connect to your gateway using the elastic IP address

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, choose **Instances**, and then select the EC2 instance that your gateway is deployed on.

3. Choose the **Description** tab at the bottom, and then note the **Elastic IP** value. You use this elastic IP address to connect to the gateway. Return to the Storage Gateway console and type in the elastic IP address.
4. After your gateway is activated, choose the gateway that you just activated, and then choose the **VTL devices** tab in the bottom panel.
5. Get the names of all your VTL devices.
6. For each target, run the following command to configure the target.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. For each target, run the following command to log in.

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

Your gateway is now connected using the elastic IP address of the EC2 instance.

## Understanding Storage Gateway Resources and Resource IDs

In Storage Gateway, the primary resource is a *gateway* but other resource types include: *volume*, *virtual tape*, *iSCSI target*, and *vtl device*. These are referred to as *subresources* and they don't exist unless they are associated with a gateway.

These resources and subresources have unique Amazon Resource Names (ARNs) associated with them as shown in the following table.

Resource Type	ARN Format
Gateway ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i>
File Share ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :share/ <i>share-id</i>
Volume ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
Tape ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :tape/ <i>tapebarcode</i>
Target ARN (iSCSI target)	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSITarget</i>
VTL Device ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /device/ <i>vtldevice</i>

Storage Gateway also supports the use of EC2 instances and EBS volumes and snapshots. These resources are Amazon EC2 resources that are used in Storage Gateway.

## Working with Resource IDs

When you create a resource, Storage Gateway assigns the resource a unique resource ID. This resource ID is part of the resource ARN. A resource ID takes the form of a resource identifier, followed by a hyphen, and a unique combination of eight letters and numbers. For example, a gateway ID is of the

form sgw-12A3456B where sgw is the resource identifier for gateways. A volume ID takes the form vol-3344CCDD where vol is the resource identifier for volumes.

For virtual tapes, you can prepend up to a four character prefix to the barcode ID to help you organize your tapes.

Storage Gateway resource IDs are in uppercase. However, when you use these resource IDs with the Amazon EC2 API, Amazon EC2 expects resource IDs in lowercase. You must change your resource ID to lowercase to use it with the EC2 API. For example, in Storage Gateway the ID for a volume might be vol-1122AABB. When you use this ID with the EC2 API, you must change it to vol-1122aabb. Otherwise, the EC2 API might not behave as expected.

**Important**

IDs for Storage Gateway volumes and Amazon EBS snapshots created from gateway volumes are changing to a longer format. Starting in December 2016, all new volumes and snapshots will be created with a 17-character string. Starting in April 2016, you will be able to use these longer IDs so you can test your systems with the new format. For more information, see [Longer EC2 and EBS Resource IDs](#).

For example, a volume ARN with the longer volume ID format will look like this:

arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG.

A snapshot ID with the longer ID format will look like this: snap-78e226633445566ee.

For more information, see [Announcement: Heads-up – Longer AWS Storage Gateway volume and snapshot IDs coming in 2016](#).

## Tagging Storage Gateway Resources

In Storage Gateway, you can use tags to manage your resources. Tags let you add metadata to your resources and categorize your resources to make them easier to manage. Each tag consists of a key-value pair, which you define. You can add tags to gateways, volumes, and virtual tapes. You can search and filter these resources based on the tags you add.

As an example, you can use tags to identify Storage Gateway resources used by each department in your organization. You might tag gateways and volumes used by your accounting department like this: (key=department and value=accounting). You can then filter with this tag to identify all gateways and volumes used by your accounting department and use the information to determine cost. For more information, see [Using Cost Allocation Tags](#) and [Working with Tag Editor](#).

If you archive a virtual tape that is tagged, the tape maintains its tags in the archive. Similarly, if you retrieve a tape from the archive to another gateway, the tags are maintained in the new gateway.

Tags don't have any semantic meaning but rather are interpreted as strings of characters.

The following restrictions apply to tags:

- Tag keys and values are case-sensitive.
- The maximum number of tags for each resource is 50.
- Tag keys cannot begin with aws :. This prefix is reserved for AWS use.
- Valid characters for the key property are UTF-8 letters and numbers, space, and special characters + - = . \_ : / and @.

## Working with Tags

You can work with tags by using the Storage Gateway console, the Storage Gateway API, or the [Storage Gateway Command Line Interface \(CLI\)](#). The following procedures show you how to add, edit, and delete a tag on the console.

### To add a tag

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. In the navigation pane, choose the resource you want to tag.

For example, to tag a gateway, choose **Gateways**, and then choose the gateway you want to tag from the list of gateways.

3. Choose **Tags**, and then choose **Add/edit tags**.
4. In the **Add/edit tags** dialog box, choose **Create tag**.
5. Type a key for **Key** and a value for **Value**. For example, you can type **Department** for the key and **Accounting** for the value.

**Note**

You can leave the **Value** box blank.

6. Choose **Create Tag** to add more tags. You can add multiple tags to a resource.
7. When you're done adding tags, choose **Save**.

### To edit a tag

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose the resource whose tag you want to edit.
3. Choose **Tags** to open the **Add/edit tags** dialog box.
4. Choose the pencil icon next to the tag you want edit, and then edit the tag.
5. When you're done editing the tag, choose **Save**.

### To delete a tag

1. Open the Storage Gateway console at <https://console.aws.amazon.com/storagegateway/home>.
2. Choose the resource whose tag you want to delete.
3. Choose **Tags**, and then choose **Add/edit tags** to open the **Add/edit tags** dialog box.
4. Choose the X icon next to the tag you want to delete, and then choose **Save**.

## Working with Open-Source Components for AWS Storage Gateway

In this section, you can find information about third party tools and licenses that we depend on to deliver Storage Gateway functionality.

The source code for certain open-source software components that are included with the AWS Storage Gateway software is available for download at the following locations:

- For gateways deployed on VMware ESXi, download [sources.tar](#)
- For gateways deployed on Microsoft Hyper-V, download [sources\\_hyperv.tar](#)
- For gateways deployed on Linux Kernel-based Virtual Machine (KVM), download [sources\\_KVM.tar](#)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). For the relevant licenses for all dependent third party tools, see [Third Party Licenses](#).

# AWS Storage Gateway quotas

In this topic, you can find information about volume and tape quotas, configuration, and performance limits for Storage Gateway.

## Topics

- [Quotas for volumes \(p. 444\)](#)
- [Quotas for tapes \(p. 444\)](#)
- [Recommended local disk sizes for your gateway \(p. 445\)](#)

## Quotas for volumes

The following table lists quotas for volumes.

Description	Cached volumes	Stored volumes
Maximum size of a volume  <b>Note</b> If you create a snapshot from a cached volume that is more than 16 TiB in size, you can restore it to a Storage Gateway volume but not to an Amazon Elastic Block Store (Amazon EBS) volume.	32 TiB	16 TiB
Maximum number of volumes per gateway	32	32
Total size of all volumes for a gateway	1,024 TiB	512 TiB

## Quotas for tapes

The following table lists quotas for tapes.

Description	Tape gateway
Minimum size of a virtual tape	100 GiB
Maximum size of a virtual tape	5 TiB
Maximum number of virtual tapes for a virtual tape library (VTL)	1,500
Total size of all tapes in a virtual tape library (VTL)	1 PiB
Maximum number of virtual tapes in archive	No limit
Total size of all tapes in a archive	No limit

## Recommended local disk sizes for your gateway

The following table recommends sizes for local disk storage for your deployed gateway.

Gateway Type	Cache (Minimum)	Cache (Maximum)	Upload Buffer (Minimum)	Upload Buffer (Maximum)	Other Required Local Disks
Cached volume gateway	150 GiB	64 TiB	150 GiB	2 TiB	—
Stored volume gateway	—	—	150 GiB	2 TiB	1 or more for stored volume or volumes
Tape gateway	150 GiB	64 TiB	150 GiB	2 TiB	—

### Note

You can configure one or more local drives for your cache and upload buffer, up to the maximum capacity.

When adding cache or upload buffer to an existing gateway, it's important to create new disks in your host (hypervisor or Amazon EC2 instance). Don't change the size of existing disks if the disks have been previously allocated as either a cache or upload buffer.

# API Reference for Storage Gateway

In addition to using the console, you can use the AWS Storage Gateway API to programmatically configure and manage your gateways. This section describes the AWS Storage Gateway operations, request signing for authentication and the error handling. For information about the regions and endpoints available for Storage Gateway, see [AWS Storage Gateway Endpoints and Quotas](#) in the [AWS General Reference](#).

## Note

You can also use the AWS SDKs when developing applications with AWS Storage Gateway. The AWS SDKs for Java, .NET, and PHP wrap the underlying AWS Storage Gateway API, simplifying your programming tasks. For information about downloading the SDK libraries, see [Sample Code Libraries](#).

## Topics

- [Storage Gateway Required Request Headers \(p. 446\)](#)
- [Signing Requests \(p. 447\)](#)
- [Error Responses \(p. 449\)](#)
- [Actions](#)

## Storage Gateway Required Request Headers

This section describes the required headers that you must send with every POST request to Storage Gateway. You include HTTP headers to identify key information about the request including the operation you want to invoke, the date of the request, and information that indicates the authorization of you as the sender of the request. Headers are case insensitive and the order of the headers is not important.

The following example shows headers that are used in the [ActivateGateway](#) operation.

```
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
```

The following are the headers that must include with your POST requests to Storage Gateway. Headers shown below that begin with "x-amz" are AWS-specific headers. All other headers listed are common header used in HTTP transactions.

Header	Description
Authorization	The authorization header contains several of pieces of information about the request that enable Storage Gateway to determine if the request is a valid action for the requester. The format of this header is as follows (line breaks added for readability):

Header	Description	
	<pre>Authorization: AWS4-HMAC-SHA456 Credentials=YourAccessKey/yyymmdd/region/storagegateway/ aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature=CalculatedSignature</pre> <p>In the preceding syntax, you specify <i>YourAccessKey</i>, the year, month, and day (<i>yyymmdd</i>), the <i>region</i>, and the <i>CalculatedSignature</i>. The format of the authorization header is dictated by the requirements of the AWS V4 Signing process. The details of signing are discussed in the topic <a href="#">Signing Requests (p. 447)</a>.</p>	
Content-Type	<p>Use application/x-amz-json-1.1 as the content type for all requests to Storage Gateway.</p> <table border="1"> <tr> <td>Content-Type: application/x-amz-json-1.1</td></tr> </table>	Content-Type: application/x-amz-json-1.1
Content-Type: application/x-amz-json-1.1		
Host	<p>Use the host header to specify the Storage Gateway endpoint where you send your request. For example, <code>storagegateway.us-east-2.amazonaws.com</code> is the endpoint for the US East (Ohio) region. For more information about the endpoints available for Storage Gateway, see <a href="#">AWS Storage Gateway Endpoints and Quotas</a> in the <i>AWS General Reference</i>.</p> <table border="1"> <tr> <td>Host: storagegateway.<i>region</i>.amazonaws.com</td></tr> </table>	Host: storagegateway. <i>region</i> .amazonaws.com
Host: storagegateway. <i>region</i> .amazonaws.com		
x-amz-date	<p>You must provide the time stamp in either the HTTP Date header or the AWS x-amz-date header. (Some HTTP client libraries don't let you set the Date header.) When an x-amz-date header is present, the Storage Gateway ignores any Date header during the request authentication. The x-amz-date format must be ISO8601 Basic in the <code>YYYYMMDD'T'HHMMSS'Z'</code> format. If both the Date and x-amz-date header are used, the format of the Date header does not have to be ISO8601.</p> <table border="1"> <tr> <td>x-amz-date: <i>YYYYMMDD 'T' HHMMSS 'Z'</i></td></tr> </table>	x-amz-date: <i>YYYYMMDD 'T' HHMMSS 'Z'</i>
x-amz-date: <i>YYYYMMDD 'T' HHMMSS 'Z'</i>		
x-amz-target	<p>This header specifies the version of the API and the operation that you are requesting. The target header values are formed by concatenating the API version with the API name and are in the following format.</p> <table border="1"> <tr> <td>x-amz-target: <i>StorageGateway_APIversion.operationName</i></td></tr> </table> <p>The <i>operationName</i> value (e.g. "ActivateGateway") can be found from the API list, <a href="#">API Reference for Storage Gateway (p. 446)</a>.</p>	x-amz-target: <i>StorageGateway_APIversion.operationName</i>
x-amz-target: <i>StorageGateway_APIversion.operationName</i>		

## Signing Requests

Storage Gateway requires that you authenticate every request you send by signing the request. To sign a request, you calculate a digital signature using a cryptographic hash function. A cryptographic hash is a

function that returns a unique hash value based on the input. The input to the hash function includes the text of your request and your secret access key. The hash function returns a hash value that you include in the request as your signature. The signature is part of the `Authorization` header of your request.

After receiving your request, Storage Gateway recalculates the signature using the same hash function and input that you used to sign the request. If the resulting signature matches the signature in the request, Storage Gateway processes the request. Otherwise, the request is rejected.

Storage Gateway supports authentication using [AWS Signature Version 4](#). The process for calculating a signature can be broken into three tasks:

- [Task 1: Create a Canonical Request](#)

Rearrange your HTTP request into a canonical format. Using a canonical form is necessary because Storage Gateway uses the same canonical form when it recalculates a signature to compare with the one you sent.

- [Task 2: Create a String to Sign](#)

Create a string that you will use as one of the input values to your cryptographic hash function. The string, called the *string to sign*, is a concatenation of the name of the hash algorithm, the request date, a *credential scope* string, and the canonicalized request from the previous task. The *credential scope* string itself is a concatenation of date, region, and service information.

- [Task 3: Create a Signature](#)

Create a signature for your request by using a cryptographic hash function that accepts two input strings: your *string to sign* and a *derived key*. The *derived key* is calculated by starting with your secret access key and using the *credential scope* string to create a series of Hash-based Message Authentication Codes (HMACs).

## Example Signature Calculation

The following example walks you through the details of creating a signature for [ListGateways](#). The example could be used as a reference to check your signature calculation method. Other reference calculations are included in the [Signature Version 4 Test Suite](#) of the Amazon Web Services Glossary.

The example assumes the following:

- The time stamp of the request is "Mon, 10 Sep 2012 00:00:00" GMT.
- The endpoint is the US East (Ohio) region.

The general request syntax (including the JSON body) is:

```
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
{}
```

The canonical form of the request calculated for [Task 1: Create a Canonical Request \(p. 448\)](#) is:

```
POST
/
```

```
content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T00000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

The last line of the canonical request is the hash of the request body. Also, note the empty third line in the canonical request. This is because there are no query parameters for this API (or any Storage Gateway APIs).

The *string to sign* for [Task 2: Create a String to Sign \(p. 448\)](#) is:

```
AWS4-HMAC-SHA256
20120910T00000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

The first line of the *string to sign* is the algorithm, the second line is the time stamp, the third line is the *credential scope*, and the last line is a hash of the canonical request from Task 1.

For [Task 3: Create a Signature \(p. 448\)](#), the *derived key* can be represented as:

```
derived key = HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-east-2"), "storagegateway"), "aws4_request")
```

If the secret access key, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, is used, then the calculated signature is:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

The final step is to construct the Authorization header. For the demonstration access key AKIAIOSFODNN7EXAMPLE, the header (with line breaks added for readability) is:

```
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
```

## Error Responses

### Topics

- [Exceptions \(p. 450\)](#)
- [Operation Error Codes \(p. 451\)](#)
- [Error Responses \(p. 463\)](#)

This section provides reference information about AWS Storage Gateway errors. These errors are represented by an error exception and an operation error code. For example, the error exception `InvalidSignatureException` is returned by any API response if there is a problem with the request signature. However, the operation error code `ActivationKeyInvalid` is returned only for the [ActivateGateway](#) API.

Depending on the type of error, Storage Gateway may return only just an exception, or it may return both an exception and an operation error code. Examples of error responses are shown in the [Error Responses \(p. 463\)](#).

## Exceptions

The following table lists AWS Storage Gateway API exceptions. When an AWS Storage Gateway operation returns an error response, the response body contains one of these exceptions. The `InternalServerError` and `InvalidGatewayRequestException` return one of the operation error codes [Operation Error Codes \(p. 451\)](#) message codes that give the specific operation error code.

Exception	Message	HTTP Status Code
<code>IncompleteSignatureException</code>	The specified signature is incomplete.	400 Bad Request
<code>InternalFailure</code>	The request processing has failed due to some unknown error, exception or failure.	500 Internal Server Error
<code>InternalServerError</code>	One of the operation error code messages <a href="#">Operation Error Codes (p. 451)</a> .	500 Internal Server Error
<code>InvalidAction</code>	The requested action or operation is invalid.	400 Bad Request
<code>InvalidClientTokenId</code>	The X.509 certificate or AWS Access Key ID provided does not exist in our records.	403 Forbidden
<code>InvalidGatewayRequestException</code>	One of the operation error code messages in <a href="#">Operation Error Codes (p. 451)</a> .	400 Bad Request
<code>InvalidSignatureException</code>	The request signature we calculated does not match the signature you provided. Check your AWS Access Key and signing method.	400 Bad Request
<code>MissingAction</code>	The request is missing an action or operation parameter.	400 Bad Request
<code>MissingAuthenticationToken</code>	The request must contain either a valid (registered) AWS Access Key ID or X.509 certificate.	403 Forbidden
<code>RequestExpired</code>	The request is past the expiration date or the request date (either with 15 minute padding), or the request date occurs more than 15 minutes in the future.	400 Bad Request
<code>SerializationException</code>	An error occurred during serialization. Check that your JSON payload is well-formed.	400 Bad Request
<code>ServiceUnavailable</code>	The request has failed due to a temporary failure of the server.	503 Service Unavailable

Exception	Message	HTTP Status Code
SubscriptionRequiredException	The AWS Access Key Id needs a subscription for the service.	400 Bad Request
ThrottlingException	Rate exceeded.	400 Bad Request
UnknownOperationException	An unknown operation was specified. Valid operations are listed in <a href="#">Operations in Storage Gateway (p. 465)</a> .	400 Bad Request
UnrecognizedClientException	The security token included in the request is invalid.	400 Bad Request
ValidationException	The value of an input parameter is bad or out of range.	400 Bad Request

## Operation Error Codes

The following table shows the mapping between AWS Storage Gateway operation error codes and APIs that can return the codes. All operation error codes are returned with one of two general exceptions—`InternalServerError` and `InvalidGatewayRequestException`—described in [Exceptions \(p. 450\)](#).

Operation Error Code	Message	Operations That Return this Error Code
ActivationKeyExpired	The specified activation key has expired.	<a href="#">ActivateGateway</a>
ActivationKeyInvalid	The specified activation key is invalid.	<a href="#">ActivateGateway</a>
ActivationKeyNotFound	The specified activation key was not found.	<a href="#">ActivateGateway</a>
BandwidthThrottleScheduleNotFound	The specified bandwidth throttle was not found.	<a href="#">DeleteBandwidthRateLimit</a>
CannotExportSnapshot	The specified snapshot cannot be exported.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
InitiatorNotFound	The specified initiator was not found.	<a href="#">DeleteChapCredentials</a>
DiskAlreadyAllocated	The specified disk is already allocated.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskDoesNotExist	The specified disk does not exist.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a>

Operation Error Code	Message	Operations That Return this Error Code
		<a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskSizeNotGigAligned	The specified disk is not gigabyte-aligned.	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeGreaterThanVolumeMaxSize	The specified disk size is greater than the maximum volume size.	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeLessThanVolumeSize	The specified disk size is less than the volume size.	<a href="#">CreateStorediSCSIVolume</a>
DuplicateCertificateInfo	The specified certificate information is a duplicate.	<a href="#">ActivateGateway</a>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
GatewayInternalError	A gateway internal error occurred.	<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> <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>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
GatewayNotConnected	The specified gateway is not connected.	<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> <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>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
GatewayNotFound	The specified gateway was not found.	<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> <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>

Operation Error Code	Message	Operations That Return this Error Code
		<a href="#">UpdateSnapshotSchedule</a>
GatewayProxyNetworkConnection	The specified gateway proxy network connection is busy.	<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> <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>

Operation Error Code	Message	Operations That Return this Error Code
InternalError	An internal error occurred.	<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> <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>

Operation Error Code	Message	Operations That Return this Error Code
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

Operation Error Code	Message	Operations That Return this Error Code
InvalidParameters	The specified request contains invalid parameters.	<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> <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>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
<code>LocalStorageLimitExceeded</code>	The local storage limit was exceeded.	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a>
<code>LunInvalid</code>	The specified LUN is invalid.	<a href="#">CreateStorediSCSIVolume</a>
<code>MaximumVolumeCountExceeded</code>	The maximum volume count was exceeded.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a>
<code>NetworkConfigurationChanged</code>	The gateway network configuration has changed.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
NotSupported	The specified operation is not supported.	<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> <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>

<b>Operation Error Code</b>	<b>Message</b>	<b>Operations That Return this Error Code</b>
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
OutdatedGateway	The specified gateway is out of date.	<a href="#">ActivateGateway</a>
SnapshotInProgressException	The specified snapshot is in progress.	<a href="#">DeleteVolume</a>
SnapshotIdInvalid	The specified snapshot is invalid.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
StagingAreaFull	The staging area is full.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetAlreadyExists	The specified target already exists.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetInvalid	The specified target is invalid.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">UpdateChapCredentials</a>
TargetNotFound	The specified target was not found.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">UpdateChapCredentials</a>

Operation Error Code	Message	Operations That Return this Error Code
UnsupportedOperationForGateway	The specified operation is not valid for the type of the 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>
VolumeAlreadyExists	The specified volume already exists.	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
VolumeIdInvalid	The specified volume is invalid.	<a href="#">DeleteVolume</a>
VolumeInUse	The specified volume is already in use.	<a href="#">DeleteVolume</a>
VolumeNotFound	The specified volume was not found.	<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	The specified volume is not ready.	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a>

## Error Responses

When there is an error, the response header information contains:

- Content-Type: application/x-amz-json-1.1

- An appropriate 4xx or 5xx HTTP status code

The body of an error response contains information about the error that occurred. The following sample error response shows the output syntax of response elements common to all error responses.

```
{  
    "__type": "String",  
    "message": "String",  
    "error":  
        { "errorCode": "String",  
          "errorDetails": "String"  
        }  
}
```

The following table explains the JSON error response fields shown in the preceding syntax.

**\_\_type**

One of the exceptions from [Exceptions \(p. 450\)](#).

*Type:* String

**error**

Contains API-specific error details. In general errors (i.e., not specific to any API), this error information is not shown.

*Type:* Collection

**errorCode**

One of the operation error codes .

*Type:* String

**errorDetails**

This field is not used in the current version of the API.

*Type:* String

**message**

One of the operation error code messages.

*Type:* String

## Error Response Examples

The following JSON body is returned if you use the `DescribeStorediSCSIVolumes` API and specify a gateway ARN request input that does not exist.

```
{  
    "__type": "InvalidGatewayRequestException",  
    "message": "The specified volume was not found.",  
    "error": {  
        "errorCode": "VolumeNotFound"  
    }  
}
```

The following JSON body is returned if Storage Gateway calculates a signature that does not match the signature sent with a request.

```
{  
    "__type": "InvalidSignatureException",  
    "message": "The request signature we calculated does not match the signature you  
provided."  
}
```

## Operations in Storage Gateway

For a list of Storage Gateway operations, see [Actions in the AWS Storage Gateway API Reference](#).

# Document history for AWS Tape and Volume Gateway

- **API version:** 2013-06-30
- **Latest documentation update:** November 24, 2020

The following table describes important changes in each release of the *AWS Storage Gateway User Guide* after April 2018. For notification about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
<a href="#">Support for Tape Gateway on Snowball Edge (p. 466)</a>	You can now host Tape Gateway on a specially configured Snowball Edge device that you order from AWS. This combination of technologies facilitates secure offline tape data migration. For more information, see <a href="#">Using Tape Gateway on AWS Snowball Edge</a> .	November 30, 2021
<a href="#">New Tapes interface (p. 466)</a>	The Tapes page in the AWS Storage Gateway console has been updated with new search and filtering features. All relevant procedures in this guide have been updated to describe the new functionality. For more information, see <a href="#">Managing Your Tape Gateway</a> .	September 23, 2021
<a href="#">S3 File Gateway topics removed from Tape and Volume Gateway guides (p. 466)</a>	To help make the user guides for Tape Gateway and Volume Gateway easier to follow for customers setting up their respective gateway types, some unnecessary topics have been removed.	July 21, 2021
<a href="#">Support for IBM Spectrum Protect 8.1.10 on Windows and Linux for tape gateway (p. 466)</a>	Tape gateways now support IBM Spectrum Protect version 8.1.10 running on Microsoft Windows Server and Linux. For more information, see <a href="#">Testing Your Setup by Using IBM Spectrum Protect</a> .	November 24, 2020
<a href="#">FedRAMP compliance (p. 466)</a>	Storage Gateway is now FedRAMP compliant. For more information, see <a href="#">Compliance validation for Storage Gateway</a> .	November 24, 2020

<a href="#">Schedule-based bandwidth throttling (p. 466)</a>	Storage Gateway now supports schedule-based bandwidth throttling for tape and volume gateways. For more information, see <a href="#">Scheduling bandwidth throttling using the Storage Gateway console</a> .	November 9, 2020
<a href="#">File upload notification for file gateway (p. 466)</a>	File gateway now provides file upload notification, which notifies you when a file has been fully uploaded to Amazon S3 by the file gateway. For more information, see <a href="#">Getting file upload notification</a> .	November 9, 2020
<a href="#">Cached volume and tape gateways local cache storage 4x increase (p. 466)</a>	Storage Gateway now supports a local cache of up to 64 TB for cached volume and tape gateways, improving performance for on-premises applications by providing low-latency access to larger working datasets. For more information, see <a href="#">Recommended local disk sizes for your gateway</a> .	November 9, 2020
<a href="#">Access-based enumeration for file gateway (p. 466)</a>	File gateway now provides access-based enumeration, which filters the enumeration of files and folders on an SMB file share based on the share's ACLs. For more information, see <a href="#">Creating an SMB file share</a> .	November 9, 2020
<a href="#">Gateway migration (p. 466)</a>	Storage Gateway now supports migrating cached volume gateways to new virtual machines. For more information, see <a href="#">Moving Cached Volumes to a New Cached Volume Gateway Virtual Machine</a> .	September 10, 2020
<a href="#">File gateway cold cache read performance 4x increase (p. 466)</a>	Storage Gateway has increased cold cache read performance 4x. For more information, see <a href="#">Performance guidance for file gateways</a> .	August 31, 2020

Support for tape retention lock and write-once-read-many (WORM) tape protection (p. 466)	Storage Gateway supports tape retention lock on virtual tapes and <i>write once read many</i> (WORM). Tape retention lock lets you specify the retention mode and period on archived virtual tapes, preventing them from being deleted for a fixed amount of time up to 100 years. It includes permission controls on who can delete tapes or modify retention settings. For more information, see <a href="#">Using Tape Retention Lock</a> . WORM-enabled virtual tapes help ensure that data on active tapes in your virtual tape library cannot be overwritten or erased. For more information, see <a href="#">Write Once, Read Many (WORM) Tape Protection</a> .	August 19, 2020
Order the hardware appliance through the console (p. 466)	You can now order the hardware appliance through the AWS Storage Gateway console. For more information, see <a href="#">Using the Storage Gateway Hardware Appliance</a> .	August 12, 2020
Support for Federal Information Processing Standard (FIPS) endpoints in new AWS Regions (p. 466)	You can now activate a gateway with FIPS endpoints in the US East (Ohio), US East (N. Virginia), US West (N. California), US West (Oregon), and Canada (Central) Regions. For more information, see <a href="#">AWS Storage Gateway endpoints and quotas</a> in the <a href="#">AWS General Reference</a> .	July 31, 2020
Gateway migration (p. 466)	Storage Gateway now supports migrating tape and stored volume gateways to new virtual machines. For more information, see <a href="#">Moving Your Data to a New Gateway</a> .	July 31, 2020

Support for multiple file shares attached to a single Amazon S3 bucket (p. 466)	File gateway now supports creating multiple file shares for a single S3 bucket and synchronizing the file gateway's local cache with a bucket based on frequency of directory access. You can limit the number of buckets necessary to manage the file shares that you create on your file gateway. You can define multiple S3 prefixes for an S3 bucket and map a single S3 prefix to a single gateway file share. You can also define gateway file share names to be independent of the bucket name to fit the on-premises file share naming convention. For more information, see <a href="#">Creating an NFS file share</a> or <a href="#">Creating an SMB file share</a> .	July 7, 2020
File gateway local cache storage 4x increase (p. 466)	Storage Gateway now supports a local cache of up to 64 TB for file gateway, improving performance for on-premises applications by providing low-latency access to larger working datasets. For more information, see <a href="#">Recommended local disk sizes for your gateway</a> in the <i>Storage Gateway User Guide</i> .	July 7, 2020
View Amazon CloudWatch alarms in the Storage Gateway console (p. 466)	You can now view CloudWatch alarms in the Storage Gateway console. For more information, see <a href="#">Understanding CloudWatch alarms</a> .	May 29, 2020
Support for Federal Information Processing Standard (FIPS) endpoints (p. 466)	You can now activate a gateway with FIPS endpoints in the AWS GovCloud (US) Regions. To choose a FIPS endpoint for a file gateway, see <a href="#">Choosing a service endpoint</a> . To choose a FIPS endpoint for a volume gateway, see <a href="#">Choosing a service endpoint</a> . To choose a FIPS endpoint for a tape gateway, see <a href="#">Choosing a service endpoint</a> .	May 22, 2020

New AWS Regions (p. 466)	Storage Gateway is now available in the Africa (Cape Town) and Europe (Milan) Regions. For more information, see <a href="#">AWS Storage Gateway endpoints and quotas</a> in the <a href="#">AWS General Reference</a> .	May 7, 2020
Support for S3 Intelligent-Tiering storage class (p. 466)	Storage Gateway now supports S3 Intelligent-Tiering storage class. The S3 Intelligent-Tiering storage class optimizes storage costs by automatically moving data to the most cost-effective storage access tier, without performance impact or operational overhead. For more information, see <a href="#">Storage class for automatically optimizing frequently and infrequently accessed objects</a> in the <a href="#">Amazon Simple Storage Service User Guide</a> .	April 30, 2020
Tape Gateway write and read performance 2x increase (p. 466)	Storage Gateway increases performance for reading from and writing to virtual tapes on tape gateway by 2x, enabling you to perform faster backup and recovery than before. For more information, see <a href="#">Performance Guidance for Tape Gateways</a> in the <a href="#">Storage Gateway User Guide</a> .	April 23, 2020
Support for automatic tape creation (p. 466)	Storage Gateway now provides the ability to automatically create new virtual tapes. Tape gateway automatically creates new virtual tapes to maintain the minimum number of available tapes you configure and then makes these new tapes available for import by the backup application, enabling your backup jobs to run without interruption. For more information, see <a href="#">Creating Tapes Automatically</a> in the <a href="#">Storage Gateway User Guide</a> .	April 23, 2020
New AWS Region (p. 466)	Storage Gateway is now available in the AWS GovCloud (US-East) Region. For more information, see <a href="#">AWS Storage Gateway Endpoints and Quotas</a> in the <a href="#">AWS General Reference</a> .	March 12, 2020

<a href="#">Support for Linux Kernel-based Virtual Machine (KVM) hypervisor (p. 466)</a>	Storage Gateway now provides the ability to deploy an on-premises gateway on the KVM virtualization platform. Gateways deployed on KVM have all the same functionality and features as the existing on-premises gateways. For more information, see <a href="#">Supported Hypervisors and Host Requirements</a> in the <i>Storage Gateway User Guide</i> .	February 4, 2020
<a href="#">Support for VMware vSphere High Availability (p. 466)</a>	Storage Gateway now provides support for high availability on VMware to help protect storage workloads against hardware, hypervisor, or network failures. For more information, see <a href="#">Using VMware vSphere High Availability with Storage Gateway</a> in the <i>Storage Gateway User Guide</i> . This release also includes performance improvements. For more information, see <a href="#">Performance</a> in the <i>Storage Gateway User Guide</i> .	November 20, 2019
<a href="#">New AWS Region for Tape gateway (p. 466)</a>	Tape gateway is now available in the South America (Sao Paulo) Region. For more information, see <a href="#">AWS Storage Gateway Endpoints and Quotas</a> in the <i>AWS General Reference</i> .	September 24, 2019
<a href="#">Support for IBM Spectrum Protect version 7.1.9 on Linux, and for tape gateways an increased maximum tape size to 5 TiB (p. 466)</a>	Tape gateways now support IBM Spectrum Protect (Tivoli Storage Manager) version 7.1.9 running on Linux, in addition to running on Microsoft Windows. For more information, see <a href="#">Testing Your Setup by Using IBM Spectrum Protect</a> in the <i>Storage Gateway User Guide</i> . Also, for tape gateways, the maximum size of a virtual tape is now increased from 2.5 TiB to 5 TiB. For more information, see <a href="#">Quotas for Tapes</a> in the <i>Storage Gateway User Guide</i> .	September 10, 2019

<a href="#">Support for Amazon CloudWatch Logs (p. 466)</a>	You can now configure file gateways with Amazon CloudWatch Log Groups to get notified about errors and the health of your gateway and its resources. For more information, see <a href="#">Getting Notified About Gateway Health and Errors With Amazon CloudWatch Log Groups</a> in the <i>Storage Gateway User Guide</i> .	September 4, 2019
<a href="#">New AWS Region (p. 466)</a>	Storage Gateway is now available in the Asia Pacific (Hong Kong) Region. For more information, see <a href="#">AWS Storage Gateway Endpoints and Quotas</a> in the <i>AWS General Reference</i> .	August 14, 2019
<a href="#">New AWS Region (p. 466)</a>	Storage Gateway is now available in the Middle East (Bahrain) Region. For more information, see <a href="#">AWS Storage Gateway Endpoints and Quotas</a> in the <i>AWS General Reference</i> .	July 29, 2019
<a href="#">Support for activating a gateway in a virtual private cloud (VPC) (p. 466)</a>	You can now activate a gateway in a VPC. You can create a private connection between your on-premises software appliance and cloud-based storage infrastructure. For more information, see <a href="#">Activating a Gateway in a Virtual Private Cloud</a> .	June 20, 2019
<a href="#">Support for moving virtual tapes from GLACIER to DEEP_ARCHIVE (p. 466)</a>	You can now move your virtual tapes that are archived in the GLACIER storage class to the DEEP_ARCHIVE storage class for cost effective and long-term data retention. For more information, see <a href="#">Moving a Tape from Glacier to Deep Archive</a> .	May 28, 2019
<a href="#">SMB file share support for Microsoft Windows ACLs (p. 466)</a>	For file gateways, you can now use Microsoft Windows access control lists (ACLs) to control access to Server Message Block (SMB) file shares. For more information, see <a href="#">Using Microsoft Windows ACLs to Control Access to an SMB File Share</a> .	May 8, 2019

<a href="#">Integration with Amazon S3 Glacier Deep Archive (p. 466)</a>	Tape gateway integrates with DEEP_ARCHIVE. You can now archive virtual tapes in Deep Archive for long-term data retention. For more information, see <a href="#">Archiving Virtual Tapes</a> .	March 27, 2019
<a href="#">Availability of Storage Gateway Hardware Appliance in Europe (p. 466)</a>	The Storage Gateway Hardware Appliance is now available in Europe. For more information, see <a href="#">AWS Storage Gateway Hardware Appliance Regions</a> in the <i>AWS General Reference</i> . In addition, you can now increase the useable storage on the Storage Gateway Hardware Appliance from 5 TB to 12 TB and replace the installed copper network card with a 10 Gigabit fiber optic network card. For more information, see <a href="#">Setting Up Your Hardware Appliance</a> .	February 25, 2019
<a href="#">Integration with AWS Backup (p. 466)</a>	Storage Gateway integrates with AWS Backup. You can now use AWS Backup to back up on-premises business applications that use Storage Gateway volumes for cloud-backed storage. For more information, see <a href="#">Backing Up Your Volumes</a> .	January 16, 2019
<a href="#">Support for Bacula Enterprise and IBM Spectrum Protect (p. 466)</a>	Tape gateways now support Bacula Enterprise and IBM Spectrum Protect. Storage Gateway also now supports newer versions of Veritas NetBackup, Veritas Backup Exec and Quest NetVault backup. You can now use these backup applications to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Using Your Backup Software to Test Your Gateway Setup</a> .	November 13, 2018

<a href="#">Support for Storage Gateway Hardware Appliance (p. 466)</a>	The Storage Gateway Hardware Appliance includes Storage Gateway software preinstalled on a third-party server. You can manage the appliance from the AWS Management Console. The appliance can host file, tape, and volume gateways. For more information, see <a href="#">Using the Storage Gateway Hardware Appliance</a> .	September 18, 2018
<a href="#">Compatibility with Microsoft System Center 2016 Data Protection Manager (DPM) (p. 466)</a>	Tape gateways are now compatible with Microsoft System Center 2016 Data Protection Manager (DPM). You can now use Microsoft DPM to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Microsoft System Center Data Protection Manager</a> .	July 18, 2018
<a href="#">Support for Server Message Block (SMB) protocol (p. 466)</a>	File gateways added support for the Server Message Block (SMB) protocol to file shares. For more information, see <a href="#">Creating a File Share</a> .	June 20, 2018
<a href="#">Support for file share, cached volumes, and virtual tape encryption (p. 466)</a>	You can now use AWS Key Management Service (AWS KMS) to encrypt data written to a file share, cached volume, or virtual tape. Currently, you can do this by using the AWS Storage Gateway API. For more information, see <a href="#">Data encryption using AWS KMS</a> .	June 12, 2018
<a href="#">Support for NovaStor DataCenter/Network (p. 466)</a>	Tape gateways now support NovaStor DataCenter/Network. You can now use NovaStor DataCenter/Network version 6.4 or 7.1 to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using NovaStor DataCenter/Network</a> .	May 24, 2018

## Earlier updates

The following table describes important changes in each release of the *AWS Storage Gateway User Guide* before May 2018.

Change	Description	Date Changed
Support for S3 One Zone_IA storage class	For file gateways, you can now choose S3 One Zone_IA as the default storage class for your file shares. Using this storage class, you can store your object data in a single Availability Zone in Amazon S3. For more information, see <a href="#">Creating a file share (p. 46)</a> .	April 4, 2018
New Region	Tape Gateway is now available in the Asia Pacific (Singapore) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	April 3, 2018
Support for refresh cache notification, requester pays, and canned ACLs for Amazon S3 buckets.	<p>With file gateways, you can now be notified when the gateway finishes refreshing the cache for your Amazon S3 bucket. For more information, see <a href="#">RefreshCache.html</a> in the <i>Storage Gateway API Reference</i>.</p> <p>File gateways now enable the requester or reader instead of the bucket owner to pay for access charges.</p> <p>File gateways now enable you to give full control to the owner of the S3 bucket that maps to the NFS file share.</p> <p>For more information, see <a href="#">Creating a file share (p. 46)</a>.</p>	March 1, 2018
Support for Dell EMC NetWorker V9.x	Tape gateways now support Dell EMC NetWorker V9.x. You can now use Dell EMC NetWorker V9.x to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Dell EMC NetWorker (p. 109)</a> .	February 27, 2018
New Region	Storage Gateway is now available in the Europe (Paris) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	December 18, 2017
Support for file upload notification and guessing of the MIME type	<p>File gateways now enable you to get notification when all files written to your NFS file share have been uploaded to Amazon S3. For more information, see <a href="#">NotifyWhenUploaded</a> in the <i>Storage Gateway API Reference</i>.</p> <p>File gateways now enable guessing of the MIME type for uploaded objects based on file extensions. For more information, see <a href="#">Creating a file share (p. 46)</a>.</p>	November 21, 2017
Support for VMware ESXi Hypervisor version 6.5	AWS Storage Gateway now supports VMware ESXi Hypervisor version 6.5. This is in addition to version 4.1, 5.0, 5.1, 5.5, and 6.0. For more information, see <a href="#">Supported hypervisors and host requirements (p. 22)</a> .	September 13, 2017
Compatibility with Commvault 11	Tape gateways are now compatible with Commvault 11. You can now use Commvault to back up your data	September 12, 2017

Change	Description	Date Changed
	to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Commvault (p. 105)</a> .	
File gateway support for Microsoft Hyper-V hypervisor	You can now deploy a file gateway on a Microsoft Hyper-V hypervisor. For information, see <a href="#">Supported hypervisors and host requirements (p. 22)</a> .	June 22, 2017
Support for three to five hour tape retrieval from archive	For a tape gateway, you can now retrieve your tapes from archive in three to five hours. You can also determine the amount of data written to your tape from your backup application or your virtual tape library (VTL). For more information, see <a href="#">Viewing Tape Usage (p. 204)</a> .	May 23, 2017
New Region	Storage Gateway is now available in the Asia Pacific (Mumbai) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	May 02, 2017
Updates to file share settings  Support for cache refresh for file shares	File gateways now add mount options to the file share settings. You can now set squash and read-only options for your file share. For more information, see <a href="#">Creating a file share (p. 46)</a> .  File gateways now can find objects in the Amazon S3 bucket that were added or removed since the gateway last listed the bucket's contents and cached the results. For more information, see <a href="#">RefreshCache</a> in the API Reference.	March 28, 2017
Support for cloning a volume	For cached volume gateways, AWS Storage Gateway now supports the ability to clone a volume from an existing volume. For more information, see <a href="#">Cloning a Volume (p. 179)</a> .	March 16, 2017
Support for file gateways on Amazon EC2	AWS Storage Gateway now provides the ability to deploy a file gateway in Amazon EC2. You can launch a file gateway in Amazon EC2 using the Storage Gateway Amazon Machine Image (AMI) now available as a community AMI. For information about how to create a file gateway and deploy it on an EC2 instance, see <a href="#">Creating a gateway (p. 40)</a> . For information about how to launch a file gateway AMI, see <a href="#">Deploying a file gateway on an Amazon EC2 host (p. 401)</a> .  In addition, file gateway now supports for HTTP proxy configuration. For more information, see <a href="#">Routing Your On-Premises Gateway Through a Proxy (p. 290)</a> .	February 08, 2017
Compatibility with Arcserve 17	Tape gateway is now compatible with Arcserve 17. You can now use Arcserve to back up your data to Amazon S3 and archive directly to S3 Glacier. For more information, see <a href="#">Testing Your Setup by Using Arcserve Backup r17.0 (p. 100)</a> .	January 17, 2017

<b>Change</b>	<b>Description</b>	<b>Date Changed</b>
New Region	Storage Gateway is now available in the EU (London) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	December 13, 2016
New Region	Storage Gateway is now available in the Canada (Central) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	December 08, 2016
Support for File gateway	In addition to volume gateways and tape gateway, Storage Gateway now provides File Gateway. File Gateway combines a service and virtual software appliance, enabling you to store and retrieve objects in Amazon S3 using industry-standard file protocols such as Network File System (NFS). The gateway provides access to objects in Amazon S3 as files on an NFS mount point.	November 29, 2016
Backup Exec 16	Tape gateway is now compatible with Backup Exec 16. You can now use Backup Exec 16 to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Veritas Backup Exec (p. 133)</a> .	November 7, 2016
Compatibility with Micro Focus (HPE) Data Protector 9.x	Tape gateway is now compatible with Micro Focus (HPE) Data Protector 9.x. You can now use HPE Data Protector to back up your data to Amazon S3 and archive directly to S3 Glacier. For more information, see <a href="#">Testing Your Setup by Using Micro Focus (HPE) Data Protector (p. 114)</a> .	November 2, 2016
New Region	Storage Gateway is now available in the US East (Ohio) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	October 17, 2016
Storage Gateway console redesign	The Storage Gateway Management Console has been redesigned to make it easier to configure, manage, and monitor your gateways, volumes, and virtual tapes. The user interface now provides views that can be filtered and provides direct links to integrated AWS services such as CloudWatch and Amazon EBS. For more information, see <a href="#">Sign Up for AWS Storage Gateway (p. 11)</a> .	August 30, 2016
Compatibility with Veeam Backup & Replication V9 Update 2 or later	Tape gateway is now compatible with Veeam Backup & Replication V9 Update 2 or later (that is, version 9.0.0.1715 or later). You can now use Veeam Backup Replication V9 Update 2 or later to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Veeam Backup &amp; Replication (p. 130)</a> .	August 15, 2016
Longer volume and snapshot IDs	Storage Gateway is introducing longer IDs for volumes and snapshots. You can enable the longer ID format for your volumes, snapshots, and other supported AWS resources. For more information, see <a href="#">Understanding Storage Gateway Resources and Resource IDs (p. 441)</a> .	April 25, 2016

Change	Description	Date Changed
New Region  Support for storage up to 512 TiB in size for stored volumes  Other gateway updates and enhancements to the Storage Gateway local console	<p>Tape gateway is now available in the Asia Pacific (Seoul) Region. For more information, see <a href="#">AWS Regions (p. 11)</a>.</p> <p>For stored volumes, you can now create up to 32 storage volumes up to 16 TiB in size each, for a maximum of 512 TiB of storage. For more information, see <a href="#">Stored volumes architecture (p. 6)</a> and <a href="#">AWS Storage Gateway quotas (p. 444)</a>.</p> <p>Total size of all tapes in a virtual tape library is increased to 1 PiB. For more information, see <a href="#">AWS Storage Gateway quotas (p. 444)</a>.</p> <p>You can now set the password for your VM local console on the Storage Gateway Console. For information, see <a href="#">Setting the Local Console Password from the Storage Gateway Console (p. 289)</a>.</p>	March 21, 2016
Compatibility with Dell EMC NetWorker 8.x	Tape gateway is now compatible with Dell EMC NetWorker 8.x. You can now use Dell EMC NetWorker to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Dell EMC NetWorker (p. 109)</a> .	February 29, 2016
Support for VMware ESXi Hypervisor version 6.0 and Red Hat Enterprise Linux 7 iSCSI initiator  Content restructure	<p>AWS Storage Gateway now supports the VMware ESXi Hypervisor version 6.0 and the Red Hat Enterprise Linux 7 iSCSI initiator. For more information, see <a href="#">Supported hypervisors and host requirements (p. 22)</a> and <a href="#">Supported iSCSI initiators (p. 23)</a>.</p> <p>This release includes this improvement: The documentation now includes a Managing Your Activated Gateway section that combines management tasks that are common to all gateway solutions. Following, you can find instructions on how you can manage your gateway after you have deployed and activated it. For more information, see <a href="#">Managing Your Gateway (p. 162)</a>.</p>	October 20, 2015

Change	Description	Date Changed
Support for storage up to 1,024 TiB in size for cached volumes	For cached volumes, you can now create up to 32 storage volumes at up to 32 TiB each for a maximum of 1,024 TiB of storage. For more information, see <a href="#">Cached volumes architecture (p. 4)</a> and <a href="#">AWS Storage Gateway quotas (p. 444)</a> .	September 16, 2015
Support for the VMXNET3 (10 GbE) network adapter type in VMware ESXi hypervisor	If your gateway is hosted on a VMware ESXi hypervisor, you can reconfigure the gateway to use the VMXNET3 adapter type. For more information, see <a href="#">Configuring Network Adapters for Your Gateway (p. 300)</a> .	
Performance enhancements	The maximum upload rate for Storage Gateway has increased to 120 MB a second, and the maximum download rate has increased to 20 MB a second.	
Miscellaneous enhancements and updates to the Storage Gateway local console	The Storage Gateway local console has been updated and enhanced with additional features to help you perform maintenance tasks. For more information, see <a href="#">Configuring Your Gateway Network (p. 293)</a> .	
Support for tagging	Storage Gateway now supports resource tagging. You can now add tags to gateways, volumes, and virtual tapes to make them easier to manage. For more information, see <a href="#">Tagging Storage Gateway Resources (p. 442)</a> .	September 2, 2015
Compatibility with Quest (formerly Dell) NetVault Backup 10.0	Tape gateway is now compatible with Quest NetVault Backup 10.0. You can now use Quest NetVault Backup 10.0 to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Quest NetVault Backup (p. 127)</a> .	June 22, 2015

Change	Description	Date Changed
<ul style="list-style-type: none"> <li>Support for 16 TiB storage volumes for stored volumes gateway setups</li> <li>Support for system resource checks on the Storage Gateway local console</li> <li>Support for the Red Hat Enterprise Linux 6 iSCSI initiator</li> </ul>	<p>Storage Gateway now supports 16 TiB storage volumes for stored volumes gateway setups. You can now create 12 16 TiB storage volumes for a maximum of 192 TiB of storage. For more information, see <a href="#">Stored volumes architecture (p. 6)</a>.</p> <p>You can now determine whether your system resources (virtual CPU cores, root volume size, and RAM) are sufficient for your gateway to function properly. For more information, see <a href="#">Viewing Your Gateway System Resource Status (p. 299)</a> or <a href="#">Viewing Your Gateway System Resource Status (p. 299)</a>.</p> <p>Storage Gateway now supports the Red Hat Enterprise Linux 6 iSCSI initiator. For more information, see <a href="#">Requirements (p. 11)</a>.</p> <p>This release includes the following Storage Gateway improvements and updates:</p> <ul style="list-style-type: none"> <li>From the Storage Gateway console, you can now see the date and time the last successful software update was applied to your gateway. For more information, see <a href="#">Managing Gateway Updates Using the AWS Storage Gateway Console (p. 263)</a>.</li> <li>Storage Gateway now provides an API you can use to list iSCSI initiators connected to your storage volumes. For more information, see <a href="#">ListVolumeInitiators</a> in the API reference.</li> </ul>	June 3, 2015
Support for Microsoft Hyper-V hypervisor versions 2012 and 2012 R2	Storage Gateway now supports Microsoft Hyper-V hypervisor versions 2012 and 2012 R2. This is in addition to support for Microsoft Hyper-V hypervisor version 2008 R2. For more information, see <a href="#">Supported hypervisors and host requirements (p. 22)</a> .	April 30, 2015
Compatibility with Symantec Backup Exec 15	Tape gateway is now compatible with Symantec Backup Exec 15. You can now use Symantec Backup Exec 15 to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Veritas Backup Exec (p. 133)</a> .	April 6, 2015
CHAP authentication support for storage volumes	Storage Gateway now supports configuring CHAP authentication for storage volumes. For more information, see <a href="#">Creating a volume (p. 72)</a> .	April 2, 2015

Change	Description	Date Changed
Support for VMware ESXi Hypervisor version 5.1 and 5.5	Storage Gateway now supports VMware ESXi Hypervisor versions 5.1 and 5.5. This is in addition to support for VMware ESXi Hypervisor versions 4.1 and 5.0. For more information, see <a href="#">Supported hypervisors and host requirements (p. 22)</a> .	March 30, 2015
Support for Windows CHKDSK utility	Storage Gateway now supports the Windows CHKDSK utility. You can use this utility to verify the integrity of your volumes and fix errors on the volumes. For more information, see <a href="#">Troubleshooting volume issues (p. 379)</a> .	March 04, 2015
Integration with AWS CloudTrail to capture API calls	<p>Storage Gateway is now integrated with AWS CloudTrail. AWS CloudTrail captures API calls made by or on behalf of Storage Gateway in your Amazon Web Services account and delivers the log files to an Amazon S3 bucket that you specify. For more information, see <a href="#">Logging and Monitoring in AWS Storage Gateway (p. 355)</a>.</p> <p>This release includes the following Storage Gateway improvement and update:</p> <ul style="list-style-type: none"> <li>Virtual tapes that have dirty data in cache storage (that is, that contain content that has not been uploaded to AWS) are now recovered when a gateway's cached drive changes. For more information, see <a href="#">Recovering a Virtual Tape From An Unrecoverable Gateway (p. 383)</a>.</li> </ul>	December 16, 2014
Compatibility with additional backup software and medium changer	<p>Tape gateway is now compatible with the following backup software:</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>You can now use these four backup software products with the Storage Gateway virtual tape library (VTL) to back up to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Using Your Backup Software to Test Your Gateway Setup (p. 99)</a>.</p> <p>Storage Gateway now provides an additional medium changer that works with the new backup software.</p> <p>This release includes miscellaneous AWS Storage Gateway improvements and updates.</p>	November 3, 2014

<b>Change</b>	<b>Description</b>	<b>Date Changed</b>
Europe (Frankfurt) Region	Storage Gateway is now available in the Europe (Frankfurt) Region. For detailed information, see <a href="#">AWS Regions (p. 11)</a> .	October 23, 2014
Content restructure	Created a Getting Started section that is common to all gateway solutions. Following, you can find instructions for you to download, deploy, and activate a gateway. After you deploy and activate a gateway, you can proceed to further instructions specific to stored volumes, cached volumes, and tape gateway setups. For more information, see <a href="#">Creating a Tape Gateway (p. 84)</a> .	May 19, 2014
Compatibility with Symantec Backup Exec 2012	Tape gateway is now compatible with Symantec Backup Exec 2012. You can now use Symantec Backup Exec 2012 to back up your data to Amazon S3 and archive directly to offline storage (GLACIER or DEEP_ARCHIVE). For more information, see <a href="#">Testing Your Setup by Using Veritas Backup Exec (p. 133)</a> .	April 28, 2014
Support for Windows Server Failover Clustering	<ul style="list-style-type: none"> <li>Storage Gateway now supports connecting multiple hosts to the same volume if the hosts coordinate access by using Windows Server Failover Clustering (WSFC). However, you can't connect multiple hosts to that same volume without using WSFC.</li> </ul>	January 31, 2014
Support for VMware ESX initiator	<ul style="list-style-type: none"> <li>Storage Gateway now enables you to manage storage connectivity directly through your ESX host. This provides an alternative to using initiators resident in the guest OS of your VMs.</li> </ul>	
Support for performing configuration tasks on Storage Gateway local console	<ul style="list-style-type: none"> <li>Storage Gateway now provides support for performing configuration tasks in the Storage Gateway local console. For information about performing configuration tasks on gateways deployed on-premises, see <a href="#">Performing Tasks on the VM Local Console (Volume and Tape Gateways) (p. 287)</a> or <a href="#">Performing Tasks on the VM Local Console (Volume and Tape Gateways) (p. 287)</a>. For information about performing configuration tasks on gateways deployed on an EC2 instance, see <a href="#">Performing Tasks on the Amazon EC2 Local Console (Volume and Tape Gateways) (p. 304)</a> or <a href="#">Performing Tasks on the Amazon EC2 Local Console (Volume and Tape Gateways) (p. 304)</a>.</li> </ul>	

Change	Description	Date Changed
Support for virtual tape library (VTL) and introduction of API version 2013-06-30	<p>Storage Gateway connects an on-premises software appliance with cloud-based storage to integrate your on-premises IT environment with the AWS storage infrastructure. In addition to volume gateways (cached volumes and stored volumes), Storage Gateway now supports gateway–virtual tape library (VTL). You can configure tape gateway with up to 10 virtual tape drives per gateway. Each virtual tape drive responds to the SCSI command set, so your existing on-premises backup applications will work without modification. For more information, see the following topics in the <i>AWS Storage Gateway User Guide</i>.</p> <ul style="list-style-type: none"> <li>• For an architectural overview, see <a href="#">Tape gateways (p. 7)</a>.</li> <li>• To get started with tape gateway, see <a href="#">Creating a Tape Gateway (p. 84)</a>.</li> </ul>	November 5, 2013
Support for Microsoft Hyper-V	<p>Storage Gateway now provides the ability to deploy an on-premises gateway on the Microsoft Hyper-V virtualization platform. Gateways deployed on Microsoft Hyper-V have all the same functionality and features as the existing on-premises storage gateway. To get started deploying a gateway with Microsoft Hyper-V, see <a href="#">Supported hypervisors and host requirements (p. 22)</a>.</p>	April 10, 2013
Support for deploying a gateway on Amazon EC2	<p>Storage Gateway now provides the ability to deploy a gateway in Amazon Elastic Compute Cloud (Amazon EC2). You can launch a gateway instance in Amazon EC2 using the Storage Gateway AMI available in <a href="#">AWS Marketplace</a>. To get started deploying a gateway using the Storage Gateway AMI, see <a href="#">Deploying a Volume or Tape Gateway on an Amazon EC2 Host (p. 399)</a>.</p>	January 15, 2013

Change	Description	Date Changed
Support for cached volumes and introduction of API Version 2012-06-30	<p>In this release, Storage Gateway introduces support for cached volumes. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their active data. You can create storage volumes up to 32 TiB in size and mount them as iSCSI devices from your on-premises application servers. Data written to your cached volumes is stored in Amazon Simple Storage Service (Amazon S3), with only a cache of recently written and recently read data stored locally on your on-premises storage hardware. Cached volumes allow you to utilize Amazon S3 for data where higher retrieval latencies are acceptable, such as for older, infrequently accessed data, while maintaining storage on-premises for data where low-latency access is required.</p> <p>In this release, Storage Gateway also introduces a new API version that, in addition to supporting the current operations, provides new operations to support cached volumes.</p> <p>For more information on the two Storage Gateway solutions, see <a href="#">How Storage Gateway works (architecture) (p. 3)</a>.</p> <p>You can also try a test setup. For instructions, see <a href="#">Creating a Tape Gateway (p. 84)</a>.</p>	October 29, 2012
API and IAM support	<p>In this release, Storage Gateway introduces API support as well as support for AWS Identity and Access Management(IAM).</p> <ul style="list-style-type: none"> <li>• <b>API support</b>—You can now programmatically configure and manage your Storage Gateway resources. For more information about the API, see <a href="#">API Reference for Storage Gateway (p. 446)</a> in the <i>AWS Storage Gateway User Guide</i>.</li> <li>• <b>IAM support</b> – AWS Identity and Access Management (IAM) enables you create users and manage user access to your Storage Gateway resources by means of IAM policies. For examples of IAM policies, see <a href="#">Authentication and Access Control for Storage Gateway (p. 336)</a>. For more information about IAM, see <a href="#">AWS Identity and Access Management (IAM)</a> detail page.</li> </ul>	May 9, 2012
Static IP support	You can now specify a static IP for your local gateway. For more information, see <a href="#">Configuring Your Gateway Network (p. 293)</a> .	March 5, 2012
New guide	This is the first release of <i>AWS Storage Gateway User Guide</i> .	January 24, 2012