AWS Storage Gateway

Amazon S3 File Gateway User Guide

API Version 2013-06-30

AWS Storage Gateway: Amazon S3 File Gateway User Guide

Table of Contents

..... viii
What is Amazon S3 File Gateway 1
Amazon S3 File Gateway 1
How Storage Gateway works 3
Amazon S3 File Gateways 3
Getting Started 5
Sign up for Amazon Web Services 5
Create an IAM user 5
Requirements 6
Required prerequisites 6
Hardware and storage requirements 7
Network and firewall requirements 8
Supported hypervisors and host requirements 16
Supported NFS clients for a File Gateway 16
Supported SMB clients for a File Gateway 17
Supported file system operations 17
Accessing AWS Storage Gateway 17
Supported AWS Regions 17
Using the hardware appliance 18
Ordering Information 18
Supported AWS Regions 18
Setting up your hardware appliance 18
Rack-mounting and connecting the hardware appliance to power 19
Hardware appliance dimensions 20
Configuring network parameters 22
Activating your hardware appliance 24
Launching a gateway 26
Configuring an IP address for the gateway 26
Configuring your gateway 27
Removing a gateway 27
Deleting your hardware appliance 28
Creating Your Gateway 29
Overview - Gateway Activation 29
Set up gateway 29
Connect to AWS 29
Review and activate 29
Overview - Gateway Configuration 29
Overview - Storage Resources 30
Create an S3 File Gateway 30
Set up an Amazon S3 File Gateway 30
Connect your Amazon S3 File Gateway to AWS 31
Review settings and activate your Amazon S3 File Gateway 31
Configure your Amazon S3 File Gateway 32
Activating a gateway in a VPC 33
Creating a VPC endpoint for Storage Gateway 33
Create a file share 35
Create an NFS file share 36
Create an SMB file share 40
Creating an SMB file share 41
Mount and use your file share 47
Mount your NFS file share on your client 47
Mount your SMB file share on your client 48
Working with file shares on a bucket with pre-exisiting objects 51
Test your S3 File Gateway 51

Where do I go from here? ... 52
Cleaning up resources you don't need ... 52
Managing your Amazon S3 File Gateway ... 53
Adding a file share ... 53
Granting access to an S3 bucket ... 53
Cross-service confused deputy prevention ... 55
Using a file share for cross-account access ... 56
Deleting a file share ... 57
Editing settings for your NFS file share ... 58
Editing metadata defaults for your NFS file share ... 60
Editing access settings for your NFS file share ... 61
Editing SMB settings for a gateway ... 61
Setting a security level for your gateway ... 62
Using Active Directory to authenticate users ... 62
Providing guest access to your file share ... 64
Configure Local Groups for your gateway ... 64
Setting file share visibility ... 64
Editing settings for your SMB file share ... 65
Refresh Amazon S3 bucket objects ... 67
Configure an automated cache refresh schedule using the Storage Gateway console ... 67
Configure an automated cache refresh schedule using AWS Lambda with an Amazon CloudWatch rule ... 68
Perform a manual cache refresh using the Storage Gateway console ... 70
Perform a manual cache refresh using the Storage Gateway API ... 70
Using S3 Object Lock with an Amazon S3 File Gateway ... 70
Understanding file share status ... 71
File share best practices ... 71
Working with multiple file shares and Amazon S3 buckets ... 72
Allowing specific NFS clients to mount your file share ... 72
Monitoring your File Gateway ... 73
Getting File Gateway health logs ... 73
Configuring a CloudWatch log group for your gateway ... 74
Using Amazon CloudWatch metrics ... 75
Getting notified about file operations ... 76
Getting file upload notification ... 77
Getting working file set upload notification ... 78
Getting refresh cache notification ... 80
Understanding gateway metrics ... 81
Understanding file share metrics ... 84
Understanding File Gateway audit logs ... 86
Maintaining your gateway ... 90
Shutting down your gateway VM ... 90
Managing local disks ... 90
Deciding the amount of local disk storage ... 90
Sizing cache storage ... 91
Configuring cache storage ... 91
Using ephemeral storage with EC2 gateways ... 91
Managing Bandwidth ... 92
Edit bandwidth-rate-limit schedule ... 93
Using the AWS SDK for Java ... 94
Using the AWS SDK for .NET ... 95
Using the AWS Tools for Windows PowerShell ... 97
Managing Gateway Updates ... 98
Performing Maintenance Tasks on the Local Console ... 98
Performing tasks on the VM local console (File Gateway) ... 99
Performing tasks on the EC2 local console (File Gateway) ... 109
Accessing the Gateway Local Console ... 114

Configuring Network Adapters for Your Gateway ... 118
Deleting Your Gateway and Removing Resources ... 124
Deleting Your Gateway by Using the Storage Gateway Console ... 124
Removing Resources from a Gateway Deployed On-Premises ... 125
Removing Resources from a Gateway Deployed on an Amazon EC2 Instance ... 125
Replacing your existing File Gateway with a new instance ... 127
Method 1: Migrate cache disk and Gateway ID to replacement instance ... 128
Method 2: Replacement instance with empty cache disk and new Gateway ID ... 129
Performance ... 131
Performance guidance for File Gateways ... 131
S3 File Gateway performance on Linux clients ... 131
File Gateway performance on Windows clients ... 132
Optimizing Gateway Performance ... 133
Add Resources to Your Gateway ... 134
Add Resources to Your Application Environment ... 135
Using VMware High Availability with Storage Gateway ... 135
Configure Your vSphere VMware HA Cluster ... 136
Download the .ova Image for Your Gateway Type ... 137
Deploy the Gateway ... 137
(Optional) Add Override Options for Other VMs on Your Cluster ... 137
Activate Your Gateway ... 138
Test Your VMware High Availability Configuration ... 138
Security ... 139
Data protection ... 139
Data encryption ... 140
Authentication and access control ... 141
Authentication ... 141
Access control ... 142
Overview of managing access ... 143
Using identity-based policies (IAM policies) ... 146
Using tags to control access to resources ... 152
Using ACLs for SMB file share access ... 154
Storage Gateway API permissions reference ... 156
Using service-linked roles ... 162
Logging and monitoring ... 164
Storage Gateway information in CloudTrail ... 164
Understanding Storage Gateway log file entries ... 165
Compliance validation ... 166
Resilience ... 167
Infrastructure security ... 167
AWS Security Best Practices ... 167
Troubleshooting and best practices ... 169
Troubleshooting: on-premises gateway issues ... 169
Enabling AWS Support to help troubleshoot your gateway ... 171
Troubleshooting: Microsoft Hyper-V setup issues ... 172
Troubleshooting: Amazon EC2 gateway issues ... 175
Gateway activation hasn't occurred after a few moments ... 176
Can't find the EC2 gateway instance in the instance list ... 176
Enabling AWS Support to help troubleshoot the gateway ... 176
Troubleshooting: hardware appliance issues ... 177
How to determine service IP address ... 177
How to perform a factory reset ... 177
How to obtain Dell iDRAC support ... 178
How to find the hardware appliance serial number ... 178
How to get hardware appliance support ... 178
Troubleshooting: File Gateway issues ... 179
Error: InaccessibleStorageClass ... 179

Error: S3AccessDenied ... 179
Error: InvalidObjectState ... 180
Error: ObjectMissing ... 180
Notification: Reboot ... 180
Notification: HardReboot ... 181
Notification: HealthCheckFailure ... 181
Notification: AvailabilityMonitorTest ... 181
Error: RoleTrustRelationshipInvalid ... 181
Troubleshooting with CloudWatch metrics ... 181
Troubleshooting: file share issues ... 183
File share is stuck in CREATING status ... 184
Can't create a file share ... 184
SMB file shares don't allow multiple different access methods ... 184
Multiple file shares can't write to the mapped S3 bucket ... 184
Notification for deleted log group when using audit logs ... 184
Can't upload files into S3 bucket ... 185
Can't change default encryption to SSE-KMS ... 185
Changes made directly in an S3 bucket with object versioning enabled may affect what you see in your file share ... 185
When writing to an S3 bucket with object versioning enabled, the File Gateway may create multiple versions of an S3 object ... 186
Changes to an S3 bucket are not reflected in Storage Gateway ... 187
ACL permissions aren't working as expected ... 187
Gateway performance declined after a recursive operation ... 187
High Availability Health Notifications ... 188
Troubleshooting: high availability issues ... 188
Health notifications ... 188
Metrics ... 189
Best practices: recovering data ... 189
Recovering from an unexpected VM shutdown ... 189
Recovering data from a malfunctioning cache disk ... 190
Recovering data from an inaccessible data center ... 190
Additional Resources ... 191
Host setup ... 191
Configuring VMware for Storage Gateway ... 191
Synchronizing Your Gateway VM Time ... 195
File Gateway on EC2 host ... 196
Getting Activation Key ... 198
AWS CLI ... 199
Linux (bash/zsh) ... 199
Microsoft Windows PowerShell ... 199
Using AWS Direct Connect with Storage Gateway ... 200
Port Requirements ... 200
Connecting to Your Gateway ... 205
Getting an IP Address from an Amazon EC2 Host ... 205
Understanding Resources and Resource IDs ... 206
Working with Resource IDs ... 206
Tagging Your Resources ... 207
Working with tags ... 207
See also ... 208
Open-source components ... 208
Open-source components for Storage Gateway ... 209
Open-source components for Amazon S3 File Gateway ... 209
Quotas ... 209
Quotas for file shares ... 209
Recommended local disk sizes for your gateway ... 210
Using storage classes ... 210

Using storage classes with a File Gateway 211
Using the GLACIER storage class with File Gateway 213
Using Kubernetes CSI drivers 213
SMB CSI drivers 214
NFS CSI drivers 217
API Reference 220
Required Request Headers 220
Signing Requests 222
Example Signature Calculation 222
Error Responses 223
Exceptions 224
Operation Error Codes 225
Error Responses 237
Operations 239
Document history 240
Earlier updates 246

Amazon FSx File Gateway documentation has been moved to What is Amazon FSx File Gateway?

Volume Gateway documentation has been moved to What is Volume Gateway?

Tape Gateway documentation has been moved to What is Tape Gateway?

What is Amazon S3 File 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 AWS Cloud for scalable and cost-effective storage that helps maintain data security. AWS Storage Gateway offers file-based, volume-based, and tape-based storage solutions.

Topics

- Amazon S3 File Gateway (p. 1)

Amazon S3 File Gateway

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. With a S3 File Gateway, you can do the following:

- You can store and retrieve files directly using the NFS version 3 or 4.1 protocol.
- You can store and retrieve files directly using the SMB file system version, 2 and 3 protocol.
- You can access your data directly in Amazon S3 from any AWS Cloud application or service.
- You can manage your S3 data using lifecycle policies, cross-region replication, and versioning. You can think of a S3 File Gateway as a file system mount on Amazon S3.

A S3 File Gateway simplifies file storage in Amazon S3, integrates to existing applications through industry-standard file system protocols, and provides a cost-effective alternative to on-premises storage. It also provides low-latency access to data through transparent local caching. A S3 File Gateway manages data transfer to and from AWS, buffers applications from network congestion, optimizes and streams data in parallel, and manages bandwidth consumption. S3 File Gateway integrate with AWS services, for example with the following:

- Common access management using AWS Identity and Access Management (IAM)
- Encryption using AWS Key Management Service (AWS KMS)
- Monitoring using Amazon CloudWatch (CloudWatch)
- Audit using AWS CloudTrail (CloudTrail)
- Operations using the AWS Management Console and AWS Command Line Interface (AWS CLI)
- Billing and cost management

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:

- provides instructions on how to create and use a S3 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.

- 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

- Amazon S3 File Gateways (p. 3)

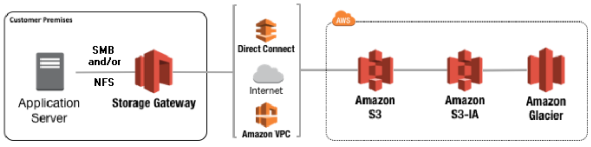
Amazon S3 File Gateways

To use an S3 File Gateway, you start by downloading a VM image for the gateway. You then activate the gateway from the AWS Management Console or through the Storage Gateway API. You can also create an S3 File Gateway using an Amazon EC2 image.

After the S3 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 S3 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 AWS Cloud. The following diagram provides an overview of file storage deployment for Storage Gateway.



S3 File Gateway converts files to S3 objects when uploading files to Amazon S3. The interaction between file operations performed against files shares on S3 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

File operation	S3 object impact	Storage class implication
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 S3 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 S3 File Gateway by an NFS or SMB client after it has been uploaded to Amazon S3, the S3 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 S3 File Gateway uploads larger files, it might need to upload smaller chunks of the file before the client is done writing to the S3 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.

Getting Started

This section provides instructions for getting started with Amazon S3 File 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 sections.

Topics

- Sign up for Amazon Web Services (p. 5)
- Create an IAM user (p. 5)
- File Gateway setup requirements (p. 6)
- Accessing AWS Storage Gateway (p. 17)
- Supported AWS Regions (p. 17)

Sign up for Amazon Web Services

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS 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.

Create an IAM user

After you create your AWS account, use the following steps to create an AWS Identity and Access Management (IAM) user for yourself. Then you add that user to a group that has administrative permissions.

To create an administrator user for yourself and add the user to an administrators group (console)

1. Sign in to the IAM console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   Note
   We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.
2. In the navigation pane, choose **Users** and then choose **Add users**.
3. For **User name**, enter **`Administrator`**.
4. Select the check box next to **AWS Management Console access**. Then select **Custom password**, and then enter your new password in the text box.

5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to **User must create a new password at next sign-in** to allow the new user to reset their password after they sign in.
6. Choose **Next: Permissions**.
7. Under **Set permissions**, choose **Add user to group**.
8. Choose **Create group**.
9. In the **Create group** dialog box, for **Group name** enter **`Administrators`**.
10. Choose **Filter policies**, and then select **AWS managed - job function** to filter the table contents.
11. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.

    Note
    You must activate IAM user and role access to Billing before you can use the `AdministratorAccess` permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.
12. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
13. Choose **Next: Tags**.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the *IAM User Guide*.
15. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

File Gateway setup requirements

Unless otherwise noted, the following requirements are common to all File Gateway types in AWS Storage Gateway. Your setup must meet the requirements in this section. Review the requirements that apply to your gateway setup before you deploy your gateway.

Topics

- Required prerequisites (p. 6)
- Hardware and storage requirements (p. 7)
- Network and firewall requirements (p. 8)
- Supported hypervisors and host requirements (p. 16)
- Supported NFS clients for a File Gateway (p. 16)
- Supported SMB clients for a File Gateway (p. 17)
- Supported file system operations for a File Gateway (p. 17)

Required prerequisites

Before you use an Amazon S3 File Gateway (S3 File Gateway), you must meet the following requirements:

- Configure Microsoft Active Directory (AD).
- Ensure that there is sufficient network bandwidth between the gateway and AWS. A minimum of 100 Mbps is required to successfully download, activate, and update the gateway.

- Configure your private networking, VPN, or AWS Direct Connect between your Amazon Virtual Private Cloud (Amazon VPC) and the on-premises environment where you are deploying your gateway.
- Make sure your gateway can resolve the name of your Active Directory Domain Controller. You can use DHCP in your Active Directory domain to handle resolution, or specify a DNS server manually from the Network Configuration settings menu in the gateway local console.

Hardware and storage requirements

The following sections provide information about the minimum required 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. 131).

Hardware requirements for on-premises VMs

When deploying your gateway on-premises, ensure that the underlying hardware on which you deploy the gateway virtual machine (VM) can dedicate the following minimum resources:

- Four virtual processors assigned to the VM
- 16 GiB of reserved RAM for File Gateways
- 80 GiB of disk space for installation of VM image and system data

For more information, see Optimizing Gateway Performance (p. 133). For information about how your hardware affects the performance of the gateway VM, see Quotas for file shares (p. 209).

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 choose 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, the data that still resides in the cache and has not yet written to Amazon Simple Storage Service (Amazon S3) can be lost. Before you stop the instance that hosts the gateway, make sure that the `CachePercentDirty` CloudWatch metric is `0`. For information about ephemeral storage, see Using ephemeral storage with EC2 gateways (p. 91). For information about monitoring metrics for your Storage Gateway, see Monitoring your File Gateway (p. 73).
  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 startup. For information about how to increase the volume size, see Modifying an EBS volume using elastic volumes (console).

Storage requirements

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

Gateway type	Cache (minimum)	Cache (maximum)			
File Gateway	150 GiB	64 TiB			

Note
You can configure one or more local drives for your cache, up to the maximum capacity. When adding cache 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 a cache.

For information about gateway quotas, see Quotas for file shares (p. 209).

Network and firewall requirements

Your gateway requires access to the internet, local networks, Domain Name Service (DNS) servers, firewalls, routers, and so on.

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.

Following, you can find information about required ports and how to allow access through firewalls and routers.

Note
In some cases, you might deploy your 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*.

Topics

- Port requirements (p. 8)
- Networking and firewall requirements for the Storage Gateway Hardware Appliance (p. 12)
- Allowing AWS Storage Gateway access through firewalls and routers (p. 14)
- Configuring security groups for your Amazon EC2 gateway instance (p. 15)

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. 200).

Common ports for all gateway types

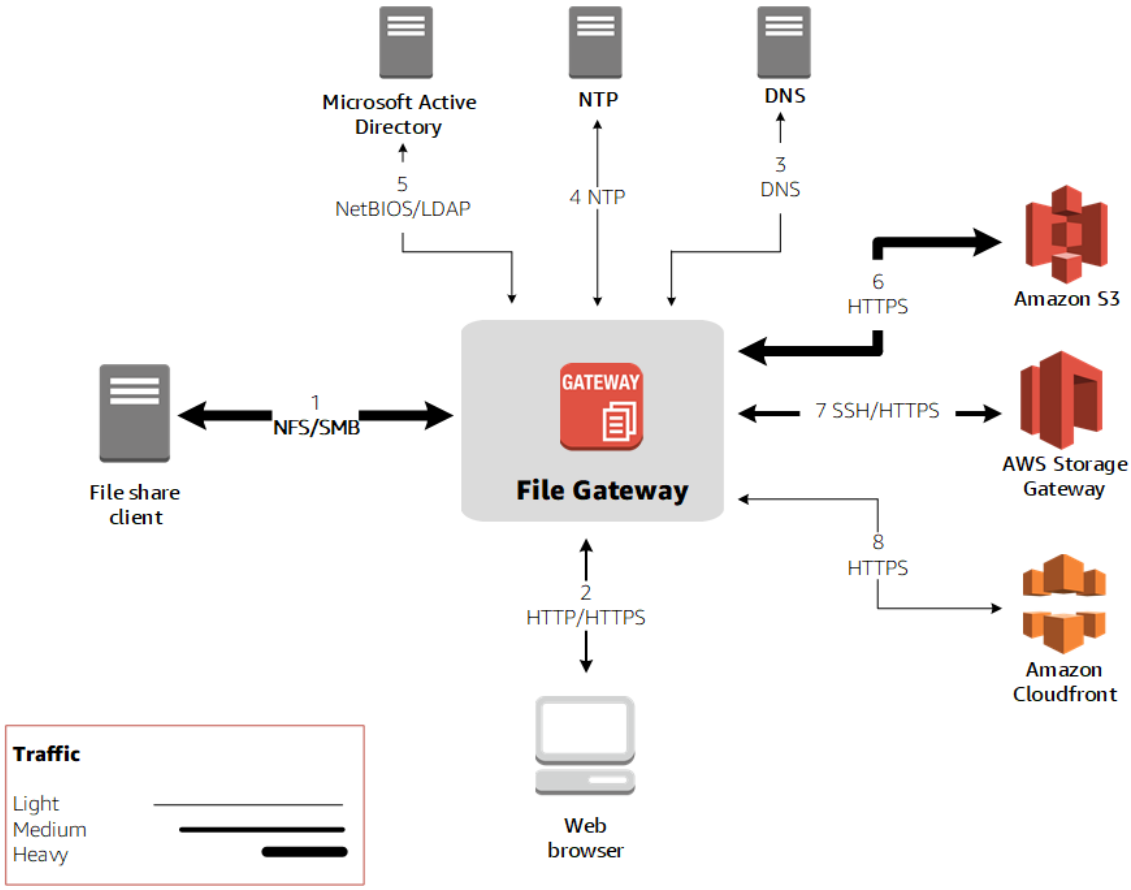
The following ports are common to all gateway types and are required by all gateway types.

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 Allowing AWS Storage Gateway access through firewalls and routers (p. 14).
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 the Storage Gateway appliance. 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 console, the host from which you connect to the console must

Protocol	Port	Direction	Source	Destination	How used
					have access to your gateway's port 80.
UDP/UDP	53 (DNS)	Outbound	Storage Gateway	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.
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 an S3 File Gateway.



Note
For specific port requirements, see Port Requirements (p. 200).

For S3 File Gateway, you only need to use Microsoft Active Directory when you want to allow domain users to access a 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 AD in the Amazon Web Services Cloud. For most AWS Managed Microsoft AD deployments, you need to configure the Dynamic Host Configuration Protocol (DHCP) service for your VPC. For information about creating a DHCP options set, see Create a DHCP options set in the *AWS Directory Service Administration Guide*.

In addition to the common ports, Amazon S3 File Gateway requires 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

Protocol	Port	Direction	Source	Destination	How used
					the port mapper that your gateway exposes. **Note** 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. **Note** This port is needed only for NFSv3.

Networking and firewall requirements for the Storage Gateway Hardware Appliance

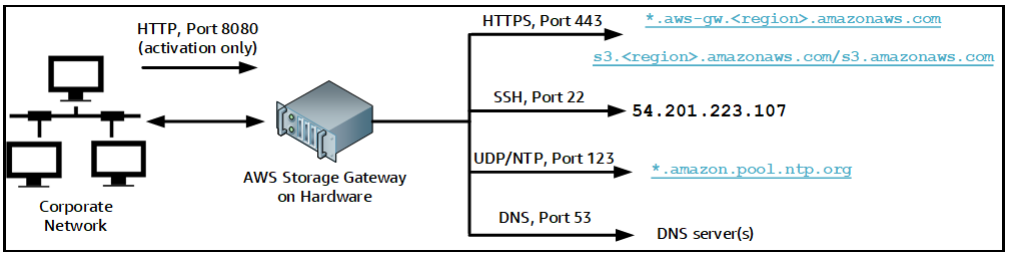
Each Storage Gateway Hardware Appliance requires the following network services:

- **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.

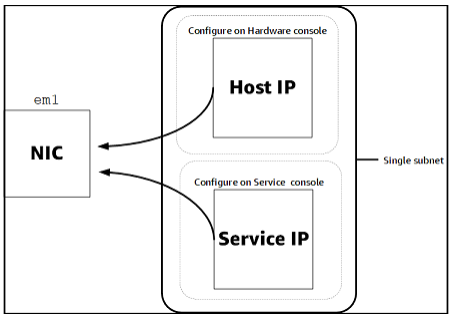
Protocol	Port	Direction	Source	Destination	How used
SSH	22	Outbound	Hardware appliance	`54.201.223.107`	Support channel
DNS	53	Outbound	Hardware appliance	DNS servers	Name resolution
UDP/NTP	123	Outbound	Hardware appliance	`*.amazon.pool.ntp.org`	Time synchronization
HTTPS	443	Outbound	Hardware appliance	`*.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. 22).

> **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. 19).

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 about activating and configuring a hardware appliance, see Using the Storage Gateway Hardware Appliance (p. 18).

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 Amazon S3 bucket that a file share maps to.

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

The following example is an Amazon 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 Regions where your gateway is activated, and where your S3 bucket is located.

The following are Amazon 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 that 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 that 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

In AWS Storage Gateway, 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. 176).

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. 200).

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 6.5, 6.7, or 7.0) – 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, 2016, 2019, or 2022) – 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. For information about how to deploy a gateway on Amazon EC2, see Deploying a File Gateway on an Amazon EC2 host (p. 196).
- Storage Gateway Hardware Appliance – Storage Gateway provides a physical hardware appliance as an 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. 189).
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

  Note
  We recommend setting the `rsize` and `wsize` mount options to 64KB to improve performance when mounting NFS file shares on 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 v3.x dialects.

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 Amazon 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 Amazon S3. Directories are managed as folder objects in S3, using the same syntax as in the Amazon S3 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.

Accessing AWS Storage Gateway

You can use the AWS Storage Gateway 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.

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. 220).

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 the AWS Developer Center.

For information about pricing, see AWS Storage Gateway pricing.

Supported AWS Regions

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

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 AWS 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.

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

Topics

- Ordering Information (p. 18)
- Supported AWS Regions (p. 18)
- Setting up your hardware appliance (p. 18)
- Rack-mounting your hardware appliance and connecting it to power (p. 19)
- Configuring network parameters (p. 22)
- Activating your hardware appliance (p. 24)
- Launching a gateway (p. 26)
- Configuring an IP address for the gateway (p. 26)
- Configuring your gateway (p. 27)
- Removing a gateway from the hardware appliance (p. 27)
- Deleting your hardware appliance (p. 28)

Ordering Information

The AWS Storage Gateway hardware appliance is available exclusively through resellers. Please contact your preferred reseller for purchasing information and to request a quote. Customers in the US and Canada can also purchase the appliance directly from CDW.

Supported AWS Regions

For a list of supported AWS Regions where the Storage Gateway Hardware Appliance is available for activation and use, 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 AWS 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.

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. 19).
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. 22).
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. 24).
4. Install the Storage Gateway on your hardware appliance. For more information, see Configuring your gateway (p. 27).

   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).

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 AWS 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

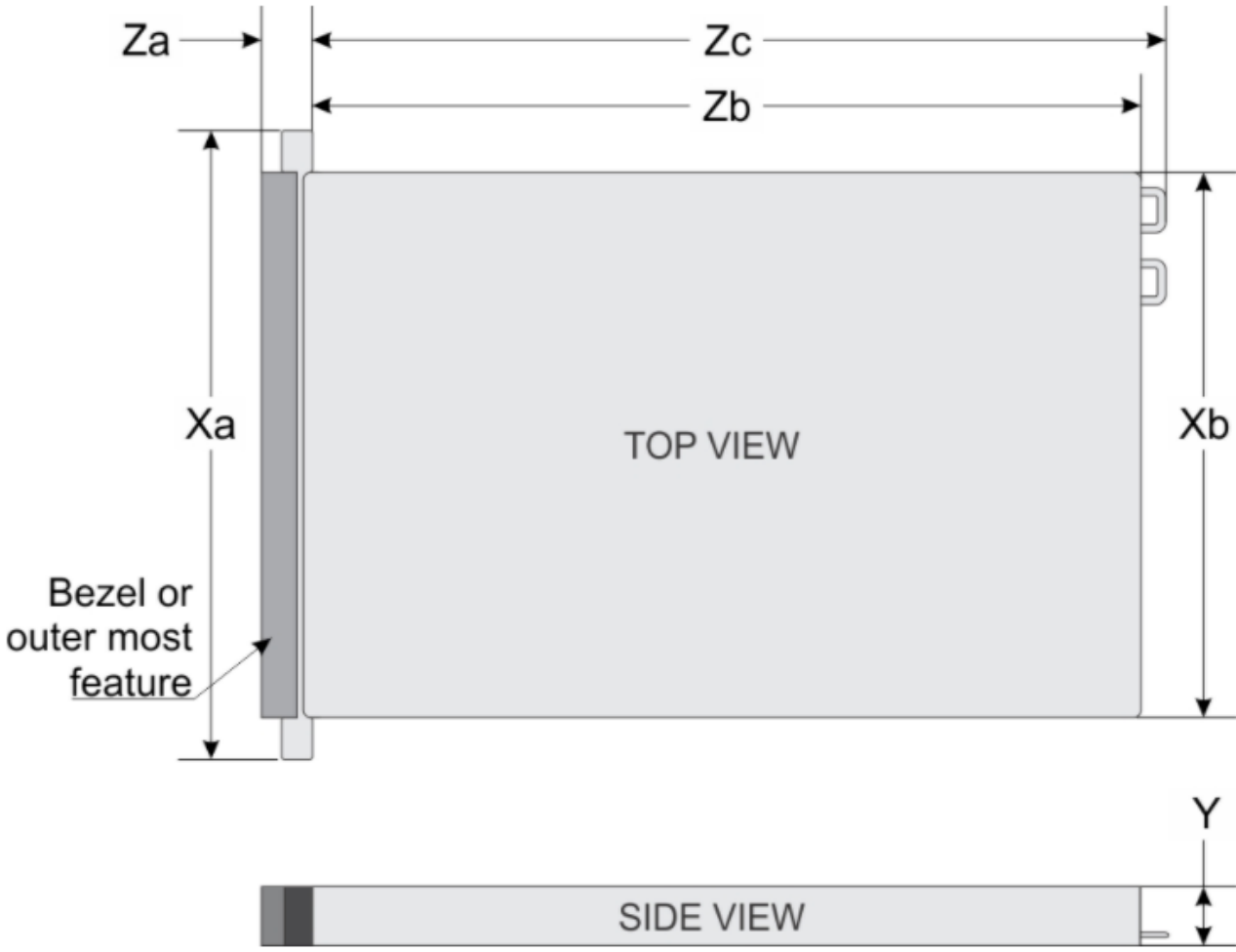
Rack-mounting your hardware appliance and connecting it to power

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. 12).

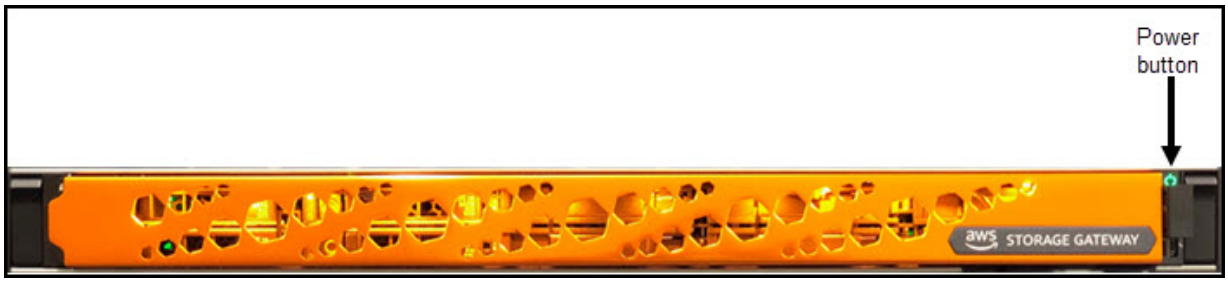
1. Plug in a power connection to each of the two power supplies. It's possible to plug in to only one power connection, but we recommend power connections to both power supplies.

   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.

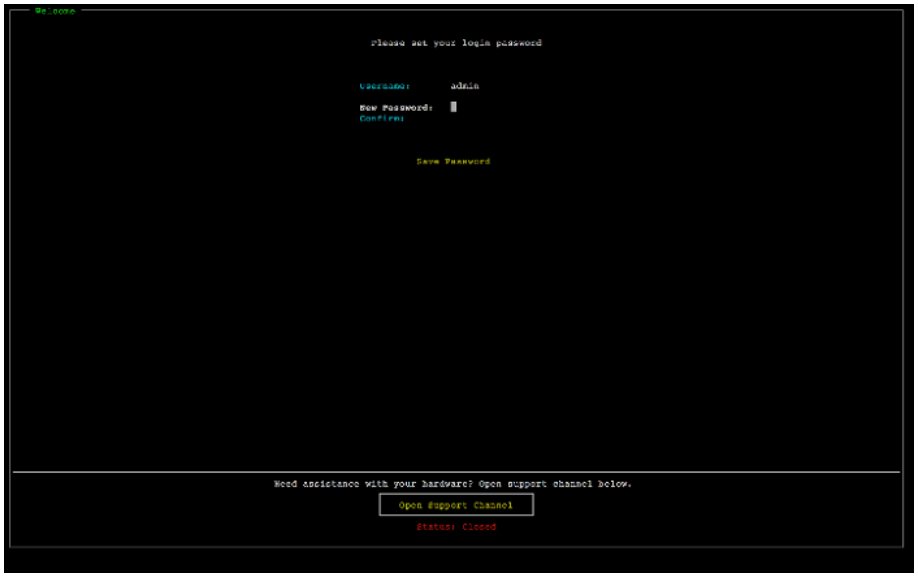


After the server boots up, the hardware console appears on the monitor. The hardware console presents a user interface specific to AWS that you can use to configure initial network parameters. You configure these parameters to connect the appliance to AWS and open up a support channel for troubleshooting by AWS 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. 22)

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. 19).

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. 24)

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 AWS 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 a splash screen. After you create a gateway in this AWS Region, the 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** in the **Connect to hardware appliance** section, enter the IPv4 address of your appliance, and then choose **Connect** 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. For **Hardware time zone**, enter your local settings.

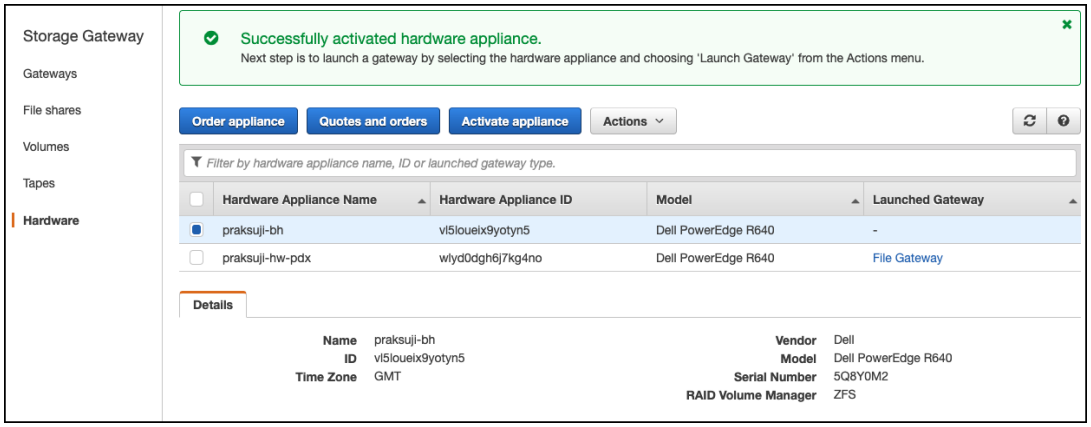
   The time zone controls when hardware updates take place, with 2 a.m. local time used as the time for updates.

   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 is used as the RAID volume manager on the hardware appliance to provide better performance and data protection. ZFS is a software-based, open-source file system and logical volume manager. The hardware appliance is specifically tuned for ZFS RAID. For more information on ZFS RAID, see the ZFS Wikipedia page.
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.



Next step

Launching a gateway (p. 26)

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 **File Gateway**, **Tape Gateway**, or **Volume Gateway (Cached)**.
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. 26)

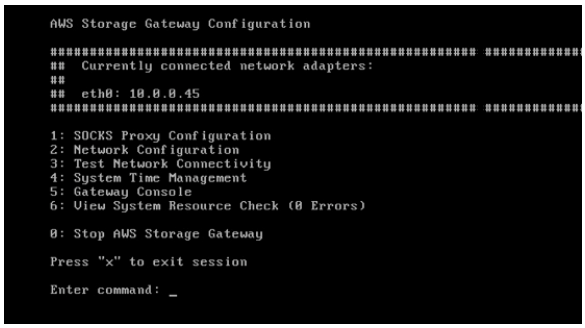
Configuring an IP address for the gateway

Before you activated your hardware appliance, you assigned an IP address to its physical network interface. Now that you have activated the appliance and launched your Storage Gateway on it, you need to assign another IP address to the Storage Gateway virtual machine that runs on the hardware appliance. To assign a static IP address to a gateway installed on your hardware appliance, configure the IP address from the local console for 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.

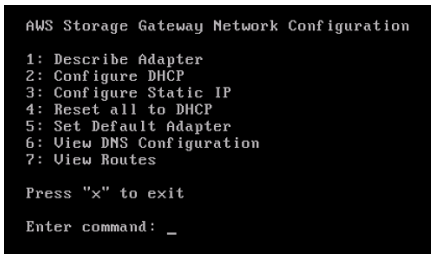
To configure an IP address on your appliance to work with applications

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 Rack-mounting your hardware appliance and connecting it to power (p. 19) for instructions.
5. Navigate to the Network Settings page of the gateway local console as shown following.



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



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. 27)

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. For instructions, see Configure your Amazon S3 File Gateway (p. 32).

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. Choose the check box for the gateway.
2. For **Actions**, choose **Remove Gateway**.
3. In the **Remove gateway from hardware appliance** dialog box, choose **Confirm**.

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. 124).

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 AWS account, you might have a need to move and activate it in a different AWS account. In this case, you first delete the appliance from the AWS account and activate it in another AWS account. You might also want to delete the appliance completely from your AWS 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. 27).
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 delete also, but the data on the hardware appliance itself is not deleted.

Creating Your Gateway

The overview topics on this page provide a high-level synopsis of how the Storage Gateway creation process works. For step-by-step procedures to create a specific type of gateway using the Storage Gateway console, see the following:

- Create and activate an Amazon S3 File Gateway
- Create and activate an Amazon FSx File Gateway
- Creating a Tape Gateway
- Creating a Volume Gateway

Overview - Gateway Activation

Gateway activation involves setting up your gateway, connecting it to AWS, then reviewing your settings and activating it.

Set up gateway

To set up your Storage Gateway, you first choose the type of gateway you want to create and the host platform on which you will run the gateway virtual appliance. You then download the gateway virtual appliance template for the platform of your choice and deploy it in your on-premises environment. You can also deploy your Storage Gateway as a physical hardware appliance that you order from AWS, or as an Amazon EC2 instance in your AWS cloud environment. When you deploy the gateway appliance, you allocate local physical disk space on the virtualization host.

Connect to AWS

The next step is to connect your gateway to AWS. To do this, you first choose the type of service endpoint you want to use for communications between the gateway virtual appliance and AWS services in the cloud. This endpoint can be accessible from the public internet, or only from within your Amazon VPC, where you have full control over the network security configuration. You then specify the gateway's IP address or its activation key, which you can obtain by connecting to the local console on the gateway appliance.

Review and activate

At this point, you'll have an opportunity to review the gateway and connection options you chose, and make changes if necessary. When everything is set up the way you want you can activate the gateway. Before you can start using your activated gateway, you will need to configure some additional settings and create your storage resources.

Overview - Gateway Configuration

After you activate your Storage Gateway, you need to perform some additional configuration. In this step, you allocate the physical storage you provisioned on the gateway host platform to be used as either the cache or the upload buffer by the gateway appliance. You then configure settings to help monitor the health of your gateway using Amazon CloudWatch Logs and CloudWatch alarms, and add tags to help identify the gateway, if desired. Before you can start using your activated and configured gateway, you will need to create your storage resources.

Overview - Storage Resources

After you activate and configure your Storage Gateway, you need to create cloud storage resources for it to use. Depending on the type of gateway you created, you will use the Storage Gateway console to create Volumes, Tapes, or Amazon S3 or Amazon FSx files shares to associate with it. Each gateway type uses its respective resources to emulate the related type of network storage infrastructure, and transfers the data you write to it into the AWS cloud.

Create and activate an Amazon S3 File Gateway

In this section, you can find instructions on how to create, deploy, and activate a File Gateway in AWS Storage Gateway.

Topics

- Set up an Amazon S3 File Gateway (p. 30)
- Connect your Amazon S3 File Gateway to AWS (p. 31)
- Review settings and activate your Amazon S3 File Gateway (p. 31)
- Configure your Amazon S3 File Gateway (p. 32)

Set up an Amazon S3 File Gateway

To set up a new S3 File Gateway

1. Open the AWS Management Console at https://console.aws.amazon.com/storagegateway/home/, and choose the AWS Region where you want to create your gateway.
2. Choose **Create gateway** to open the **Set up gateway** page.
3. In the **Gateway settings** section, do the following:

   a. For **Gateway name**, enter a name for your gateway. After your gateway is created, you can search for this name to find your gateway on the list pages in the AWS Storage Gateway console.

   b. For **Gateway time zone**, choose the local time zone for the part of the world where you want to deploy your gateway.
4. In the **Gateway options** section, for **Gateway type**, choose **Amazon S3 File Gateway**.
5. In the **Platform options** section, do the following:

   a. For **Host platform**, choose the platform on which you want to deploy your gateway. Then follow the platform-specific instructions displayed on the Storage Gateway console page to set up your host platform. You can choose from the following options:

   - **VMware ESXi** – Download, deploy, and configure the gateway virtual machine using VMware ESXi.
   - **Microsoft Hyper-V** – Download, deploy, and configure the gateway virtual machine using Microsoft Hyper-V.
   - **Linux KVM** – Download, deploy, and configure the gateway virtual machine using Linux Kernel-based Virtual Machine (KVM).
   - **Amazon EC2** – Configure and launch an Amazon EC2 instance to host your gateway.
   - **Hardware appliance** – Order a dedicated physical hardware appliance from AWS to host your gateway.

b. For **Confirm set up gateway**, select the check box to confirm that you performed the deployment steps for the host platform that you chose. This step is not applicable for the **Hardware appliance** host platform.

6. Now that your gateway is set up, you must choose how you want it to connect and communicate with AWS. Choose **Next** to proceed.

Connect your Amazon S3 File Gateway to AWS

To connect a new S3 File Gateway to AWS

1. If you have not done so already, complete the procedure described in Set up an Amazon S3 File Gateway. When finished, choose **Next** to open the **Connect to AWS** page in the AWS Storage Gateway console.
2. In the **Endpoint options** section, for **Service endpoint**, choose the type of endpoint that your gateway will use to communicate with AWS. You can choose from the following options:

   - **Publicly accessible** – Your gateway communicates with AWS over the public internet. If you select this option, use the **FIPS enabled endpoint** check box to specify whether the connection must comply with Federal Information Processing Standards (FIPS).

     Note
     If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS-compliant endpoint. For more information, see Federal Information Processing Standard (FIPS) 140-2.
     The FIPS service endpoint is available only in some AWS Regions. For more information, see AWS Storage Gateway endpoints and quotas in the *AWS General Reference*.
   - **VPC hosted** – Your gateway communicates with AWS through a private connection with your virtual private cloud (VPC), allowing you to control your network settings. If you select this option, you must specify an existing VPC endpoint by choosing its VPC endpoint ID from the dropdown list. You can also provide its VPC endpoint Domain Name System (DNS) name or IP address.
3. In the **Gateway connection options** section, for **Connection options**, choose how to identify your gateway to AWS. You can choose from the following options:

   - **IP address** – Provide the IP address of your gateway in the corresponding field. This IP address must be public or accessible from within your current network, and you must be able to connect to it from your web browser.

     You can obtain the gateway IP address by logging into the gateway's local console from your hypervisor client, or by copying it from your Amazon EC2 instance details page.
   - **Activation key** – Provide the activation key for your gateway in the corresponding field. You can generate an activation key using the gateway's local console. If your gateway's IP address is unavailable, choose this option.
4. Now that you have chosen how you want your gateway to connect to AWS, you must activate the gateway. Choose **Next** to proceed.

Review settings and activate your Amazon S3 File Gateway

To activate a new S3 File Gateway

1. If you have not done so already, complete the procedures described in the following topics:

   - Set up an Amazon S3 File Gateway

- Connect your Amazon S3 File Gateway to AWS

When finished, choose **Next** to open the **Review and activate** page in the AWS Storage Gateway console.

2. Review the initial gateway details for each section on the page.
3. If a section contains errors, choose **Edit** to return to the corresponding settings page and make changes.

   Important
   You cannot modify the gateway options or connection settings after your gateway is activated.

4. Now that you have activated your gateway, you must perform the first-time configuration to allocate local storage disks and configure logging. Choose **Next** to proceed.

Configure your Amazon S3 File Gateway

To perform the first-time configuration on a new S3 File Gateway

1. If you have not done so already, complete the procedures described in the following topics:

   - Set up an Amazon S3 File Gateway
   - Connect your Amazon S3 File Gateway to AWS
   - Review settings and activate your Amazon S3 File Gateway

   When finished, choose **Next** to open the **Configure gateway** page in the AWS Storage Gateway console.
2. In the **Configure cache storage** section, use the dropdown lists to allocate at least one local disk with at least 150 gibibytes (GiB) capacity to **Cache**. The local disks listed in this section correspond to the physical storage that you provisioned on your host platform.
3. In the **CloudWatch log group** section, choose how to set up Amazon CloudWatch Logs to monitor the health of your gateway. You can choose from the following options:

   - **Create a new log group** – Set up a new log group to monitor your gateway.
   - **Use an existing log group** – Choose an existing log group from the corresponding dropdown list.
   - **Deactivate logging** – Do not use Amazon CloudWatch Logs to monitor your gateway.
4. In the **CloudWatch alarms** section, choose how to set up Amazon CloudWatch alarms to notify you when your gateway's metrics deviate from defined limits. You can choose from the following options:

   - **Deactivate alarms** – Do not use CloudWatch alarms to be notified about your gateway's metrics.
   - **Create custom CloudWatch alarm** – Configure a new CloudWatch alarm to be notified about your gateway's metrics. Choose **Create alarm** to define metrics and specify alarm actions in the Amazon CloudWatch console. For instructions, see Using Amazon CloudWatch alarms in the *Amazon CloudWatch User Guide*.
5. (Optional) In the **Tags** section, choose **Add new tag**, then enter a case-sensitive key-value pair to help you search and filter for your gateway on the list pages in the AWS Storage Gateway console. Repeat this step to add as many tags as you need.
6. (Optional) In the **Verify VMware High Availability configuration** section, if your gateway is deployed on a VMware host as part of a cluster that is enabled for VMware High Availability (HA), choose **Verify VMware HA** to test whether the HA configuration is working properly.

Note
This section appears only for gateways that are running on the VMware host platform. This step is not required to complete the gateway configuration process. You can test your gateway's HA configuration at any time. Verification takes a few minutes, and reboots the Storage Gateway virtual machine (VM).

7. Choose **Configure** to finish creating your gateway.

   To check the status of your new gateway, search for it on the **Gateways** page of the AWS Storage Gateway console.

Now that you have created your gateway, you must create a file share for it to use. For instructions, see Create a file share.

Activating a gateway in a virtual private cloud

You can create a private connection between your on-premises gateway appliance and cloud-based storage infrastructure. You can use this connection to activate your gateway and enable it to transfer data to AWS storage services without communicating over the public internet. Using the Amazon VPC service, you can launch AWS resources, including private network interface endpoints, in a custom virtual private cloud (VPC). A VPC gives you control over network settings such as 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 activate your gateway in a VPC, use the Amazon VPC Console to create a VPC endpoint for Storage Gateway and get the VPC endpoint ID, then specify this VPC endpoint ID when you create and activate the gateway. For more information, see Connect your Amazon S3 File Gateway to AWS.

To enable your S3 File Gateway to transfer data through the VPC, you must create a separate VPC endpoint for Amazon S3, then specify this VPC endpoint when you create file shares for the gateway.

Note
You must activate your gateway in the same region where you create the VPC endpoint for Storage Gateway, and the Amazon S3 storage that you configure for the file share must be in the same region where you create the VPC endpoint for Amazon S3.

Topics

- Creating a VPC endpoint for Storage Gateway (p. 33)

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 and activate your gateway. For more information, see Create and activate an Amazon S3 File Gateway.

Important
To enable your S3 File Gateway to transfer data through the VPC, you must create a separate VPC endpoint for Amazon S3, then specify this VPC endpoint when you create file shares for the gateway.
To do this, follow the same steps as shown above, but choose `com.amazonaws.region.s3` for **Service Name**, then select the route table that you want the S3 endpoint associated with instead of subnet/security group. For instructions, see Creating a gateway endpoint.

Create a file share

In this section, you can find instructions on 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, and so on). 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 are 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. Test all file operations that you plan to use with AWS Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.
> Carefully consider the use of S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 when you're uploading data 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. 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.

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 (through an allow list). Users and groups can also be denied access (through a 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. 154).

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. 36) or Create an SMB file share (p. 40). You can also do this by using the Storage Gateway API. For instructions, see CreateNFSFileShare or CreateSMBFileShare in the *AWS 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.
If you configure your file gateway to use SSE-KMS for encryption, you must manually add `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenerateDataKey`, and `kms:DescribeKey` permissions to the IAM role associated with the file share. For more information, see Using Identity-Based Policies (IAM Policies) for Storage Gateway.

Topics

- Create an NFS file share (p. 36)
- Create an SMB file share (p. 40)

Create an NFS file share

Use the following procedure to create a Network File System (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, and so on). 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 are 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. Test all file operations that you plan to use with AWS Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.
Carefully consider the use of S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 when you're uploading data 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 the transfer costs associated with CRR. 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) storage class.

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 S3 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 S3 User Guide*.
   - To connect the file share to an S3 bucket through an access point alias, choose **S3 access point alias**, then enter the S3 access point alias name and, optionally, a prefix name for objects created by the file share. If you choose this option, the file gateway cannot create a new AWS Identity and Access Management (IAM) role and access policy on your behalf. You must select an existing IAM role and configure an access policy in the **Access to your S3 bucket** section that follows. For more information about access point aliases, see Using a bucket-style alias for your access point in the *Amazon S3 User Guide*.

     Note

     - Each file share can only connect to one S3 bucket, but multiple file shares can connect to the same bucket. If you connect more than one file share to the same bucket, you must configure each file share to use a unique, non-overlapping prefix name to prevent read/write conflicts.
     - If you enter a prefix name, or choose to connect through an access point or access point alias, 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.
     - For information about using prefix names, see Organizing objects using prefixes in the *Amazon S3 User Guide*.
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, or chose to connect through an access point or access point alias, 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 virtual private cloud (VPC) powered by AWS PrivateLink, choose **Use VPC endpoint**.
   2. To identify the VPC interface endpoint that you want the file share to connect through, choose either **VPC endpoint ID** or **VPC endpoint DNS name**, 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 or through an alias associated with 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 S3 User Guide*.

8. For **Access objects using**, choose **Network File System (NFS)**.
9. For **Audit logs**, choose one of the following:

   - To turn off logging, choose **Disable logging**.
   - To create a new audit log, choose **Create a new log group**.
   - To use an existing audit log, choose **Use an existing log group**, and then choose an audit log from the list.

   For more information about audit logs, see Understanding File Gateway audit logs (p. 86).
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. 77).

    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:

    - To store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated, choose **S3 Standard**. For more information about the S3 Standard storage class, see Storage classes for frequently accessed objects in the *Amazon Simple Storage Service User Guide*.
    - To optimize storage costs by automatically moving data to the most cost-effective storage access tier, choose **S3 Intelligent-Tiering**. 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*.
    - To store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated, choose **S3 Standard-IA**. 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*.
    - To store your infrequently accessed object data in a single Availability Zone, choose **S3 One Zone-IA**. 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:

    - To enable guessing of the MIME type for uploaded objects based on file extensions, choose **Guess MIME type**.
    - To give full control to the owner of the S3 bucket that maps to the NFS file share, choose **Give bucket owner full control**. 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. 56).

      Note
      This option requires that Access Control Lists (ACLs) are enabled on the S3 bucket associated with your file share. If ACLs are disabled, the file share will not be able to access the S3 bucket, and will remain in the **Unavailable** state indefinitely.

    - 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, choose **Enable requester pays**. 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:

    - To enable the file gateway to create a new IAM role and access policy on your behalf, choose **Create a new IAM role**. This option is not available if the file share connects to Amazon S3 using an access point alias.
    - To select an existing IAM role and to set up the access policy manually, choose **Use an existing IAM role**. You must use this option if your file share connects to Amazon S3 using an access point alias. 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. 53).

17. For **Encryption**, choose the type of encryption keys to use to encrypt objects that your file gateway stores in Amazon S3:

    - To use server-side encryption managed with Amazon S3 (SSE-S3), choose **S3-Managed Keys (SSE-S3)**.
    - To use server-side encryption managed with AWS Key Management Service (SSE-KMS), choose **KMS-Managed Keys (SSE-KMS)**. In the **Primary key** box, choose an existing AWS 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 KMS keys 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. 16).
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. 60).
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

Mount your NFS file share on your client (p. 47)

Create an SMB file share

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

Note
An SMB file share does not work properly unless the required ports are open in your security group. For more information, see Port Requirements (p. 200).

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, and so on). 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 are 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. Test all file operations that you plan to use with AWS Storage Gateway so that you understand how each file operation interacts with Amazon S3 storage.
Carefully consider the use of S3 Versioning and Cross-Region Replication (CRR) in Amazon S3 when you're uploading data 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. 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) storage class.

Creating an SMB file share

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 S3 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 S3 User Guide*.
   - To connect the file share to an S3 bucket through an access point alias, choose **S3 access point alias**, then enter the S3 access point alias name and, optionally, a prefix name for objects created by the file share. If you choose this option, the file gateway cannot create a new AWS Identity and Access Management (IAM) role and access policy on your behalf. You must select an existing IAM role and configure an access policy in the **Access to your S3 bucket** section that follows. For more information about access point aliases, see Using a bucket-style alias for your access point in the *Amazon S3 User Guide*.

     Note

     - Each file share can only connect to one S3 bucket, but multiple file shares can connect to the same bucket. If you connect more than one file share to the same bucket, you must configure each file share to use a unique, non-overlapping prefix name to prevent read/write conflicts.
     - If you enter a prefix name, or choose to connect through an access point or access point alias, 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.
- For information about using prefix names, see Organizing objects using prefixes in the *Amazon S3 User Guide*.

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, or chose to connect through an access point or access point alias, 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 virtual private cloud (VPC) powered by AWS PrivateLink, choose **Use VPC endpoint**.
   2. To identify the VPC interface endpoint that you want the file share to connect through, choose either **VPC endpoint ID** or **VPC endpoint DNS name**, 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 or through an alias associated with 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:

   - To turn off logging, choose **Disable logging**.
   - To create a new audit log, choose **Create a new log group**.
   - To use an existing log group, choose **Use an existing log group**, and then choose an audit log from the list.

   For more information about audit logs, see Understanding File Gateway audit logs (p. 86).
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. 77).

    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:

    - To store your frequently accessed object data redundantly in multiple Availability Zones that are geographically separated, choose **S3 Standard**. For more information about the S3 Standard storage class, see Storage classes for frequently accessed objects in the *Amazon Simple Storage Service User Guide*.
    - To optimize storage costs by automatically moving data to the most cost-effective storage access tier, choose **S3 Intelligent-Tiering**. 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*.
    - To store your infrequently accessed object data redundantly in multiple Availability Zones that are geographically separated, choose **S3 Standard-IA**. 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*.
    - To store your infrequently accessed object data in a single Availability Zone, choose **S3 One Zone-IA**. 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:

    - To enable guessing of the MIME type for uploaded objects based on file extensions, choose **Guess MIME type**.
    - To give full control to the owner of the S3 bucket that maps to the SMB file share, choose **Give bucket owner full control**. 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. 56).

      Note
      This option requires that Access Control Lists (ACLs) are enabled on the S3 bucket associated with your file share. If ACLs are disabled, the file share will not be able to access the S3 bucket, and will remain in the **Unavailable** state indefinitely.
    - To give full control to the owner of the S3 bucket that maps to the SMB file share, choose **Enable requester pays**. 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:

    - To enable the file gateway to create a new IAM role and access policy on your behalf, choose **Create a new IAM role**. This option is not available if the file share connects to Amazon S3 using an access point alias.
    - To select an existing IAM role and to set up the access policy manually, choose **Use an existing IAM role**. You must use this option if your file share connects to Amazon S3 using an access point alias. 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. 53).
17. For **Encryption**, choose the type of encryption keys to use to encrypt objects that your file gateway stores in Amazon S3:

- To use server-side encryption managed with Amazon S3 (SSE-S3), choose **S3-Managed Keys (SSE-S3)**.
- To use server-side encryption managed with AWS Key Management Service (SSE-KMS), choose **KMS-Managed Keys (SSE-KMS)**. In the **Primary key** box, choose an existing AWS 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 KMS keys 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.

    - To use your corporate Microsoft AD for user authenticated access to your SMB file share, choose **Active Directory**.

      Note
      Your file gateway must be joined to a domain. For more information, see Using Active Directory to authenticate users.
      Joining a domain creates an Active Directory computer account in the default computers container (which is not an OU), using the gateway's **Gateway ID** as the account name (for example, SGW-1234ADE).
      If your Active Directory environment requires that you pre-stage accounts to facilitate the join domain process, you will need to create this account ahead of time.
      If your Active Directory environment has a designated OU for new computer objects, you must specify that OU when joining the domain.
    - To provide only guest access, choose **Guest access**. If you choose this authentication method, 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:

    - To set fine-grained permissions on files and folders in your SMB file share, choose **Windows Access Control List**. For more information, see Using Microsoft Windows ACLs to control access to an SMB file share (p. 154).
    - To use POSIX permissions to control access to files and directories that are stored through an NFS or SMB file share, choose **POSIX permissions**.

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 one of the following:

- To allow the gateway to control the case sensitivity, choose **Client specified**.
- To allow the client to control the case sensitivity, choose **Force case sensitivity**.

Note

- If selected, 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.

For **Access based enumeration**, choose one of the following:

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

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:

- To allow the file share to use opportunistic locking to optimize the file buffering strategy, choose **Enabled**. In most cases, enabling opportunistic locking improves performance, particularly with regard to Windows context menus.
- To prevent the use of opportunistic locking, choose **Disabled**. 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 any allowed or denied 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.

Next Step

Mount your SMB file share on your client (p. 48)

Mount and use your file share

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. 16). For more information about supported Service Message Block (SMB) clients, see Supported SMB clients for a File Gateway (p. 17).

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

- Mount your NFS file share on your client (p. 47)
- Mount your SMB file share on your client (p. 48)
- Working with file shares on a bucket with pre-exisiting objects (p. 51)
- Test your S3 File Gateway (p. 51)
- Where do I go from here? (p. 52)

Mount 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 nolock,hard [GatewayVMIPAddress]:/[FileShareName]
     [ClientMountPath]
     ```

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

     ```
     sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v
     [GatewayVMIPAddress]:/[FileShareName] [ClientMountPath]
     ```

   - For Windows clients, type the following command at the command prompt (**cmd.exe**).

     ```
     mount -o nolock -o mtype=hard [GatewayVMIPAddress]:/[FileShareName]
     [WindowsDriveLetter]
     ```

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

   ```
   mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare 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 that 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

Test your S3 File Gateway (p. 51)

Mount 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:

- Command Prompt (`cmdkey` and `net use`) – Use the command prompt to mount your file share. Store your credentials with `cmdkey`, then mount the drive with `net use` and include the `/persistent:yes` and `/savecred` switches if you want the connection to persist across system reboots. The specific commands you use will be different depending on whether you want to mount the drive for Microsoft Active Directory (AD) access or guest user access. Examples are provided below.
- File Explorer (Map Network Drive) – Use Windows File Explorer to mount your file share. Configure settings to specify whether you want the connection to persist across system reboots and prompt for network credentials.
- PowerShell script – Create a custom PowerShell script to mount your file share. Depending on the parameters you specify in the script, the connection can be persistent across system reboots, and the share 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 authorized Microsoft AD users using the command prompt:

1. Make sure the Microsoft AD user has the necessary permissions to the SMB file share before mounting the file share to the user's system.

2. Enter the following at the command prompt to mount the file share:

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

To mount your SMB file share with a specific username and password combination using the command prompt:

1. Make sure that the user account has access to the SMB file share before mounting the file share to the system.
2. Enter the following at the command prompt to save the user credentials in Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Enter the following at the command prompt to mount the file share:

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

To mount your SMB file share for guest users using the command prompt:

1. Make sure that you have the guest user account password before mounting the file share.
2. Type the following at the command prompt to save the guest credentials in Windows Credential Manager:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```
3. Type the following at the command prompt.

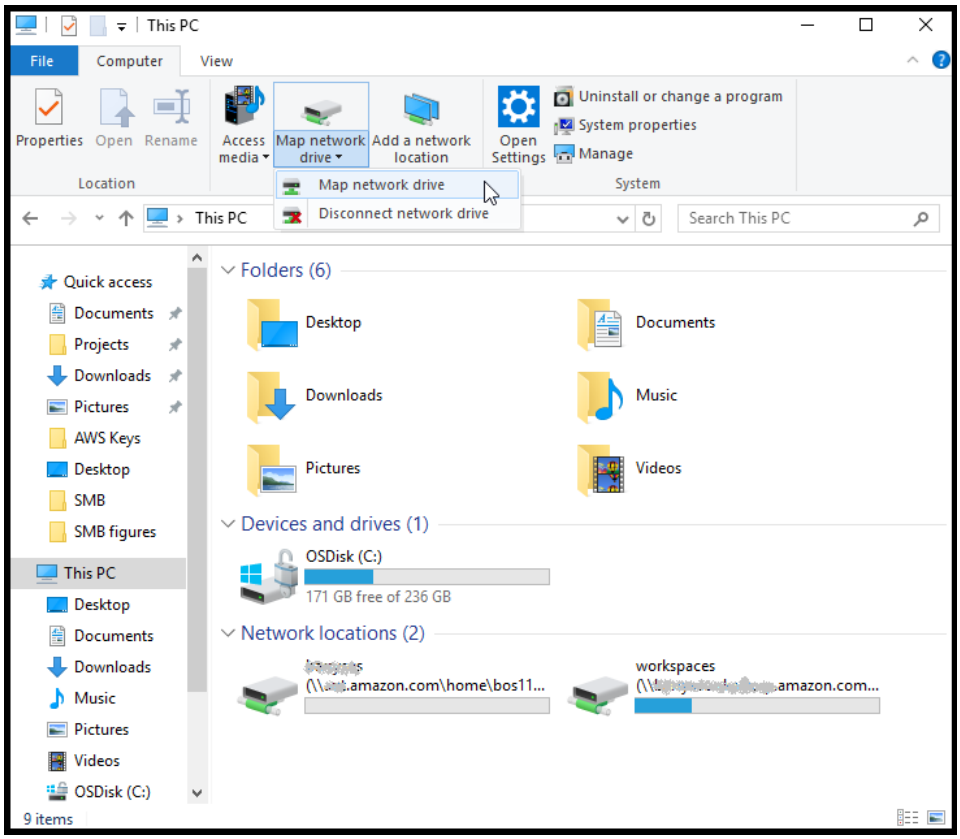
   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
   ID\smbguest /persistent:yes /savecred
   ```

   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.
   - Unless you configure your file share connection to save your user credentials and persist across system restarts, you might need to remount your file share each time you restart your client system.

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. 154).

Next Step

Test your S3 File Gateway (p. 51)

Working with file shares on a bucket with pre-exisiting 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 “Refresh Amazon S3 bucket objects” (p. 67).

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 *Managing your Amazon S3 File Gateway* (p. 53).

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).

Test your S3 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 -l`) depends on the number of objects in your bucket.

Next Step

Where do I go from here? (p. 52)

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 Amazon S3 File Gateway (p. 53).
- To optimize your File Gateway, see Optimizing Gateway Performance (p. 133).
- To troubleshoot gateway problems, see Troubleshooting and best practices (p. 169).
- To learn about Storage Gateway metrics and how you can monitor how your gateway performs, see .

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. 124).
2. Delete the Storage Gateway VM from your on-premises host. If you created your gateway on an Amazon EC2 instance, terminate the instance.

Managing your Amazon S3 File Gateway

Following, you can find information about how to manage your Amazon S3 File Gateway resources.

Topics

- Adding a file share (p. 53)
- Deleting a file share (p. 57)
- Editing settings for your NFS file share (p. 58)
- Editing metadata defaults for your NFS file share (p. 60)
- Editing access settings for your NFS file share (p. 61)
- Editing SMB settings for a gateway (p. 61)
- Editing settings for your SMB file share (p. 65)
- Refreshing objects in your Amazon S3 bucket (p. 67)
- Using S3 Object Lock with an Amazon S3 File Gateway (p. 70)
- Understanding file share status (p. 71)
- File share best practices (p. 71)

Adding a file share

After your S3 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 AWS account than your file share. For information about how to add a file share, see Create a file share (p. 35).

Topics

- Granting access to an Amazon S3 bucket (p. 53)
- Cross-service confused deputy prevention (p. 55)
- Using a file share for cross-account access (p. 56)

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, and to perform actions on any access points or virtual private cloud (VPC) endpoints that it uses to connect to the 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 and any associated access points or VPC endpoints must have an access policy that allows the IAM role to access them.

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 can create your own policy and attach it to your file share. For more information about how to do this, see Create a file share (p. 35).

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"
        }
    ]
}
```

The following example policy is similar to the preceding one, but allows your file gateway to perform actions required to access a bucket through an access point.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:123456789:accesspoint/TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

Note
If you need to connect your file share to an S3 bucket through a VPC endpoint, see Endpoint policies for Amazon S3 in the *AWS PrivateLink User Guide*.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that AWS Storage Gateway gives another service to the resource. If you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The value of `aws:SourceArn` must be the ARN of the Storage Gateway with which your file share is associated.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (`*`) for the unknown portions of the ARN. For example, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Storage Gateway to prevent the confused deputy problem.

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

```
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/
sgw-712345DA"
        }
      }
    }
  ]
}
```

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. 53).
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. 53).

   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. 53).
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

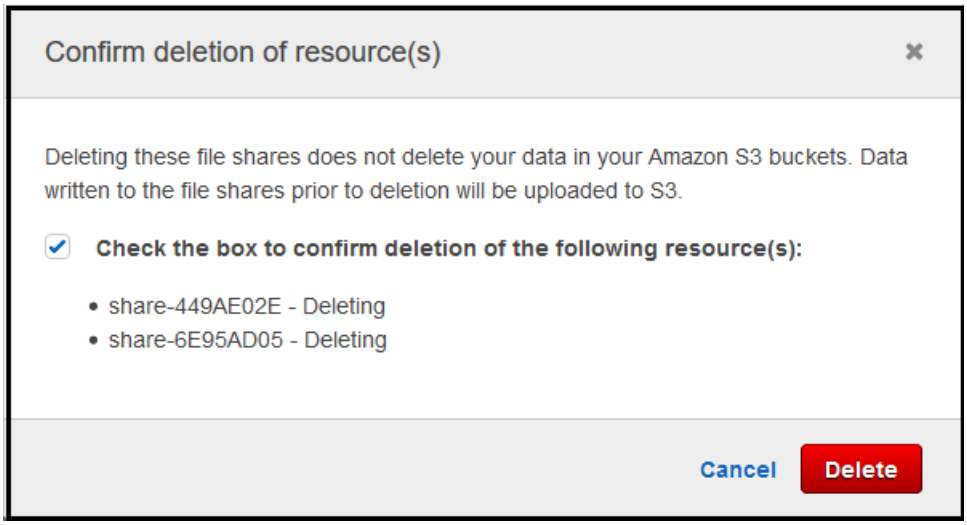
If you no longer need a file share, you can delete it from the Storage Gateway console. When you delete a file share, the gateway is detached from the Amazon S3 bucket that the file share maps to. However, the S3 bucket and its contents aren't deleted.

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.



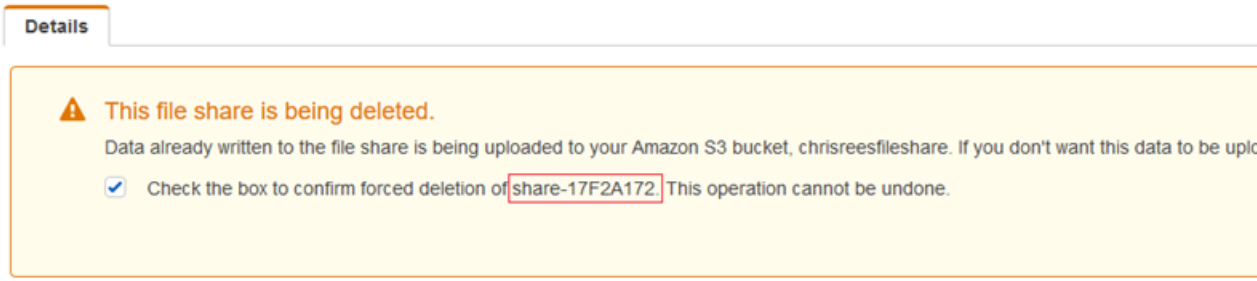
4. In the confirmation dialog box, select the check box for the file share or shares that you want to delete, and then choose **Delete**.

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 AWS 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.

Note
You cannot edit an existing file share to point to a new bucket or access point, or to modify the VPC endpoint settings. You can configure those settings only when creating a new file share.

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:

   - (Optional) For **File share name**, enter a new name for the file share.
   - 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. 86).
   - (Optional) For **Automated cache refresh from S3**, 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 the TTL interval has elapsed, accessing the directory causes 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 S3 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. 77).

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

- 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*.
- 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. 56).
  - 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 **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**.
- 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.

5. Choose **Save**.

Editing metadata defaults for your NFS file share

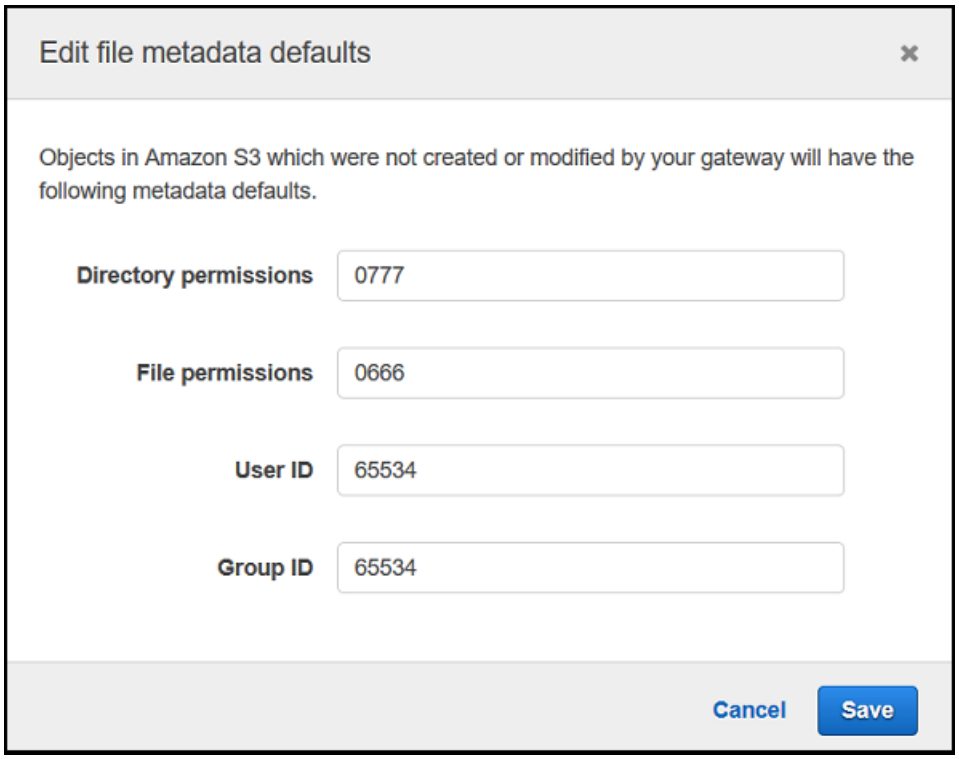
If you don't set metadata values for your files or directories in your bucket, your S3 File Gateway sets default metadata values. These values include Unix permissions for files and folders. You can edit the metadata defaults on the Storage Gateway console.

When your S3 File Gateway stores files and folders in Amazon S3, the Unix file permissions are stored in object metadata. When your S3 File Gateway discovers objects that weren't stored by the S3 File Gateway, these objects are assigned default Unix file permissions. You can find the default Unix permissions in the following table.

Metadata	Description
Directory permissions	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.
File permissions	The Unix file mode in the form "nnnn". For example, "0666" represents the file mode inside the file share. The default value is 0666.
User ID	The default owner ID for files in the file share. The default value is 65534.
Group ID	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 clients that you want to allow, and then choose **Save**.

Editing SMB settings for a gateway

Gateway-level SMB settings let you configure the security strategy, Active Directory authentication, guest access, local group permissions, and file share visibility for the SMB file shares on a gateway.

To edit gateway level SMB settings

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** dropdown menu, choose **Edit SMB settings**, then choose the settings you want to edit.

See the following topics for more information.

Topics

- Setting a security level for your gateway (p. 62)
- Using Active Directory to authenticate users (p. 62)
- Providing guest access to your file share (p. 64)
- Configure Local Groups for your gateway (p. 64)
- Setting file share visibility (p. 64)

Setting a security level for your gateway

By using a S3 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. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** dropdown menu, choose **Edit SMB settings**, then choose **SMB security settings**.
4. 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, S3 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 later.
   - **Enforce signing** – If you choose this option, S3 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 later.
   - **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**.
5. 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 AWS 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. 154).

To enable Active Directory authentication

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** drop-down menu, choose **Edit SMB settings**, then choose **Active Directory settings**.
4. 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
   Active Directory status shows **Detached** when a gateway has never joined a domain.
   Joining a domain creates an Active Directory computer account in the default computers container (which is not an OU), using the gateway's **Gateway ID** as the account name (for example, SGW-1234ADE).
   If your Active Directory environment requires that you pre-stage accounts to facilitate the join domain process, you will need to create this account ahead of time.
   If your Active Directory environment has a designated OU for new computer objects, you must specify that OU when joining the domain.
   If your gateway can't join an Active Directory directory, try joining with the directory's IP address by using the JoinDomain API operation.
5. 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. From the **Actions** drop-down menu, choose **Edit file share access settings**.
3. 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 any allowed or denied users or groups, any authenticated AD user can export the file share.
4. When you finish adding your entries, choose **Save**.

Providing guest access to your file share

If you want to provide only guest access, your S3 File Gateway doesn't have to be part of a Microsoft AD domain. You can also use a S3 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. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** drop-down menu, choose **Edit SMB settings**, then choose **Guest access settings**.
4. For **Guest password**, provide a password, and then choose **Save**.

Configure Local Groups for your gateway

Local Group settings allow you to grant Active Directory users or groups special permissions for the SMB file shares on your gateway.

You can use Local Group settings to assign Gateway Admin permissions. Gateway Admins can use the Shared Folders Microsoft Management Console snap-in to force-close files that are open and locked.

> **Note**
> You must add at least one Gateway Admin user or group before you can join your gateway to an Active Directory domain.

To assign Gateway Admins

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** dropdown menu, choose **Edit SMB settings**, then choose **Local Group settings**.
4. In the **Local Group settings** section, choose your settings. This section appears only for file shares that use Active Directory.

   For **Gateway Admins**, add Active Directory users and groups that you want to grant local Gateway Admin permissions. Add one user or group per line, including the domain name. For example, **`corp\Domain Admins`**. To create additional lines, choose **Add new Gateway Admin**.

   > **Note**
   > Editing Gateway Admins disconnects and reconnects all SMB file shares.
5. Choose **Save changes**, then choose **Proceed** to acknowledge the warning message that appears.

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. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Gateways**, then choose the gateway for which you want to edit SMB settings.
3. From the **Actions** drop-down menu, choose **Edit SMB settings**, then choose **File share visibility settings**.

4. 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**
> You cannot edit an existing file share to point to a new bucket or access point, or to modify the VPC endpoint settings. You can configure those settings only when creating a new file share.

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:

   - (Optional) For **File share name**, enter a new name for the file share.
   - 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. 86).
   - (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 the TTL interval has elapsed, accessing the directory causes 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 S3 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. 77).

     > **Note**
     > This setting has no effect on the timing of the object uploading to S3, only on the timing of the notification.
   - 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*.
- 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 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. 56).
  - 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 that are 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 **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. 154).
  - 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 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**, 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 loss 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 **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.

5. Choose **Save changes**.

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 S3 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 object cache for your file share, select the method that best fits your use case from the following list, then complete the corresponding procedure below.

Topics

- Configure an automated cache refresh schedule using the Storage Gateway console (p. 67)
- Configure an automated cache refresh schedule using AWS Lambda with an Amazon CloudWatch rule (p. 68)
- Perform a manual cache refresh using the Storage Gateway console (p. 70)
- Perform a manual cache refresh using the Storage Gateway API (p. 70)

Configure an automated cache refresh schedule using the Storage Gateway console

To configure an automated cache refresh schedule using the Storage Gateway console

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **File shares**.
3. Choose the file share for which you want to configure the refresh schedule.
4. For **Actions**, choose **Edit file share settings**.
5. 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.
6. Choose **Save changes**.

Configure an automated cache refresh schedule using AWS Lambda with an Amazon CloudWatch rule

To configure an automated cache refresh schedule using AWS Lambda with an Amazon CloudWatch rule

1. Identify the S3 bucket used by the S3 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": "*"
        },
        {
            "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 you 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/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

    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'`.

Perform a manual cache refresh using the Storage Gateway console

To perform a manual cache refresh using the Storage Gateway 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 for which you want to perform the 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.

Perform a manual cache refresh using the Storage Gateway API

To perform a manual cache refresh using the Storage Gateway API

- Send an HTTP POST request to invoke the `RefreshCache` operation with your desired parameters through the Storage Gateway API. For more information, see RefreshCache in the *AWS Storage Gateway API Reference*.

  Note
  Sending the `RefreshCache` request only initiates the cache 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. For more information, see Getting notified about file operations (p. 76).

Using S3 Object Lock with an Amazon S3 File Gateway

Amazon S3 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 S3 File Gateway. When you modify an object in this way, S3 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 S3 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 S3 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

- Working with multiple file shares and Amazon S3 buckets (p. 72)
- Allowing specific NFS clients to mount your file share (p. 72)

Working with multiple file shares and Amazon S3 buckets

Unpredictable results can sometimes occur if you configure one Amazon S3 bucket to be written to by multiple gateways or file shares, but there are two different configuration methods you can use to prevent this. Choose the method that best fits your use case from the following options:

- Configure your S3 buckets so that only one file share can write to each bucket. Use a different file share to write to each bucket.

  To do this, you create an S3 bucket policy that denies all roles except the role used for a specific file share to put or delete objects in the bucket. Attach a similar policy to each bucket, specifying a different file share to write to each bucket.

  The following example policy denies S3 bucket write permissions to all roles except the role that created the 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:*"
            }
         }
      }
   ]
}
```

- If you want to write to the same Amazon S3 bucket from multiple file shares, you must prevent the file shares from trying to write to the same objects simultaneously.

  To do this, you configure a separate, unique object prefix for each file share, which means that each file share will only write to objects with its corresponding prefix, and will not write to objects associated with the other file shares in your deployment. You configure the object prefix in the **S3 prefix name** field when you create a new file share.

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. 61).

Monitoring your File Gateway

You can monitor your File Gateway and associated resources in AWS Storage Gateway by using Amazon CloudWatch metrics and file share audit logs. You can also use CloudWatch Events to get notified when your file operations are done. For information about File Gateway type metrics, see Monitoring your File Gateway (p. 73).

Topics

- Getting File Gateway health logs with CloudWatch log groups (p. 73)
- Using Amazon CloudWatch metrics (p. 75)
- Getting notified about file operations (p. 76)
- Understanding gateway metrics (p. 81)
- Understanding file share metrics (p. 84)
- Understanding File Gateway audit logs (p. 86)

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 Amazon S3 bucket. You can configure the group either 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 Configure your Amazon S3 File Gateway (p. 32). 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 a 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 the File Gateway is unable to upload the object `myFolder/myFile.text` to Amazon S3 because it has transitioned out of the Amazon S3 Standard storage class to either the S3 Glacier Flexible Retrieval or the 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. 179).
- `"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"` indicates the time that the error occurred.

For information about how to troubleshoot the errors that may be reported by File Gateway, see Troubleshooting: File Gateway issues (p. 179).

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.

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. 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, in the **Details** tab, next to **Logging**, under **Not Enabled**, choose **Configure log group** to open the **Edit gateway information** dialog box.
4. For **Gateway log group**, choose **Use an existing log group**, and then choose the log group that you want to use.

   If you don't have a log group, choose **Create a new log group** to create one. You are directed to the CloudWatch Logs console where you can create the log group. If you create a new log group, choose the refresh button to view the new log group in the drop-down list.
5. When you are done, choose **Save**.
6. To see the logs for your gateway, choose the gateway, and then choose the **Details** tab.

For information about how to troubleshoot errors, see Troubleshooting: File Gateway issues (p. 179).

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 SDKs or 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 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 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`	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 `GatewayId` and the `GatewayName` dimensions. Throughput and latency data of a gateway are based on all the file shares in the gateway. Data is available automatically in 5-minute periods at no charge.

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 initiate 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. 77).
- 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. 78).
- 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 API, subscribe to the notification when the operation is complete. For more information, see Getting refresh cache notification (p. 80).

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

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 AWS 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.
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 Upload Notification Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

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 AWS 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 `NotifyWhenUploaded` is called.
request-received	When the gateway received the `NotifyWhenUploaded` 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 Amazon 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 AWS 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.

Field names	Description
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 gateway metrics

The following table describes metrics that cover S3 File Gateways. Each gateway has a set of metrics associated with it. Some gateway-specific metrics have the same name as certain file-share-specific metrics. These metrics represent the same kinds of measurements, but are scoped to the gateway rather than the file share.

Always specify whether you want to work with a gateway or a file share when working with a particular metric. Specifically, when working with gateway metrics, you must specify the `Gateway Name` for the gateway whose metric data you want to view. For more information, see Using Amazon CloudWatch metrics (p. 75).

The following table describes the metrics that you can use to get information about your S3 File Gateways.

Metric	Description
`AvailabilityNotifications`	This metric reports the number of availability-related health notifications that were generated by the gateway in the reporting period. Units: Count
`CacheFileSize`	This metric tracks the size of files in the gateway cache. Use this metric with the `Average` statistic to measure the average size of a file in the gateway cache. Use this metric with the `Max` statistic to measure the maximum size of a file in the gateway cache. Units: Bytes

Metric	Description
`CacheFree`	This metric reports the number of available bytes in the gateway cache. Units: Bytes
`CacheHitPercent`	Percent of application read operations from the gateway that are served from cache. The sample is taken at the end of the reporting period. When there are no application read operations from the gateway, this metric reports 100 percent. Units: Percent
`CachePercentDirty`	The overall percentage of the gateway cache that has not been persisted to AWS. The sample is taken at the end of the reporting period. Units: Percent
`CachePercentUsed`	The overall percent of the gateway cache storage that is used. The sample is taken at the end of the reporting period. Units: Percent
`CacheUsed`	This metric reports the number of used bytes in the gateway cache. Units: Bytes
`CloudBytesDownloaded`	The total number of bytes that the gateway downloaded from AWS during the reporting period. Use this metric with the `Sum` statistic to measure throughput and with the `Samples` statistic to measure IOPS. Units: Bytes
`CloudBytesUploaded`	The total number of bytes that the gateway uploaded to AWS during the reporting period. Use this metric with the `Sum` statistic to measure throughput and with the `Samples` statistic to measure input/output operations per second (IOPS). Units: Bytes

Metric	Description
`FilesFailingUpload`	This metric tracks the number of files which are failing to upload to AWS. These files will generate health notifications which contain more information on the issue. Use this metric with the `Sum` statistic to show the number of files which are currently failing to upload to AWS. Units: Count
`FileSharesUnavailable`	This metric provides the number of file shares on this gateways which are in the **Unavailable** state. If this metric reports any file shares are unavailable, then it is likely there is a problem with the gateway which is may cause disruption to your workflow. It is recommended to create an alarm for when this metric reports a non-zero value. Units: Count
`FilesRenamed`	This metric tracks the number of files renamed in the reporting period. Units: Count
`HealthNotifications`	This metric reports the number of health notifications that were generated by this gateway in the reporting period. Units: Count
`IoWaitPercent`	This metric reports the percentage of time that the CPU is waiting for a response from the local disk. Units: Percent
`MemTotalBytes`	This metric reports the total amount of memory on the gateway. Units: Bytes
`MemUsedBytes`	This metric reports the amount of used memory on the gateway. Units: Bytes
`NfsSessions`	This metric reports the number of NFS sessions that are active on the gateway. Units: Count

Metric	Description
RootDiskFreeBytes	This metric reports the number of available bytes on the root disk of the gateway. If this metric reports less than 20 GB are free, you should increase the size of the root disk. Units: Bytes
S3GetObjectRequestTime	This metric reports the time for the gateway to complete S3 get object requests. Units: Milliseconds
S3PutObjectRequestTime	This metric reports the time for the gateway to complete S3 put object requests. Units: Milliseconds
S3UploadPartRequestTime	This metric reports the time for the gateway to complete S3 upload part requests. Units: Milliseconds
SmbV1Sessions	This metric reports the number of SMBv1 sessions that are active on the gateway. Units: Count
SmbV2Sessions	This metric reports the number of SMBv2 sessions that are active on the gateway. Units: Count
SmbV3Sessions	This metric reports the number of SMBv3 sessions that are active on the gateway. Units: Count
TotalCacheSize	This metric reports the total size of the cache. Units: Bytes
UserCpuPercent	This metric reports the percentage of time that is spent on gateway processing. Units: Percent

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. 75).

The following table describes the Storage Gateway metrics that you can use to get information about your file shares.

Metric	Description
`CacheHitPercent`	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. When there are no application read operations from the file share, this metric reports 100 percent. Units: Percent
`CachePercentDirty`	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. Use the `CachePercentDirty` metric of the gateway to view the overall percentage of the gateway's cache that has not been persisted to AWS. Units: Percent
`CachePercentUsed`	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. Use the `CachePercentUsed` metric of the gateway to view overall percent use of the gateway's cache storage. Units: Percent
`CloudBytesUploaded`	The total number of bytes that the gateway uploaded to AWS during the reporting period. Use this metric with the `Sum` statistic to measure throughput and with the `Samples` statistic to measure IOPS. Units: Bytes
`CloudBytesDownloaded`	The total number of bytes that the gateway downloaded from AWS during the reporting period. Use this metric with the `Sum` statistic to measure throughput and with the `Samples` statistic to measure input/output operations per second (IOPS). Units: Bytes

Metric	Description
`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 `Sum` statistic to measure throughput and with the `Samples` statistic to measure IOPS. Units: Bytes
`WriteBytes`	The total number of bytes written to your on-premises applications in the reporting period. Use this metric with the `Sum` statistic to measure throughput and with the `Samples` statistic to measure IOPS. Units: Bytes

Understanding File Gateway audit logs

Amazon S3 File Gateway (S3 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.

Operations

The following table describes the File Gateway audit log file access operations.

Operation name	Definition
Read Data	Read the contents of a file.
Write Data	Change the contents 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).

Attributes

The following table describes S3 File Gateway audit log file access attributes.

Attribute	Definition
`accessMode`	The permission setting for the object.

Attribute	Definition
`accountDomain` **(SMB only)**	The Active Directory (AD) domain that the client's account belongs to.
`accountName` **(SMB only)**	The Active Directory user name of the client.
`bucket`	The S3 bucket name.
`clientGid` **(NFS only)**	The identifier of the group of the user accessing the object.
`clientUid` **(NFS only)**	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` **(SMB only)**	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.

Attributes logged per operation

The following table describes the S3 File Gateway audit log attributes logged in each file access operation.

	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)
accessMode			X	X					X	
accountDomain **(SMB only)**	X	X	X	X	X	X	X	X	X	X
accountName **(SMB only)**	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
clientGid **(NFS only)**	X	X	X	X	X	X		X	X	X
clientUid **(NFS only)**	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 **(SMB only)**							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

	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

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.

Topics

- Shutting down your gateway VM (p. 90)
- Managing local disks for your Storage Gateway (p. 90)
- Managing Bandwidth for Your Amazon S3 File Gateway (p. 92)
- Managing Gateway Updates Using the AWS Storage Gateway Console (p. 98)
- Performing Maintenance Tasks on the Local Console (p. 98)
- Deleting Your Gateway by Using the AWS Storage Gateway Console and Removing Associated Resources (p. 124)

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 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.

You might need to shutdown or reboot your VM for maintenance, such as when applying a patch to your hypervisor. For File Gateway, you just shutdown your VM. You don't shutdown the gateway. Although this section focuses on starting and stopping your gateway using the Storage Gateway Management Console, you can also 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 Performing Maintenance Tasks on the Local Console (p. 98).
- Storage Gateway API-—see ShutdownGateway

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. 90)
- Determining the size of cache storage to allocate (p. 91)
- Adding cache storage (p. 91)
- Using ephemeral storage with EC2 gateways (p. 91)

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. File Gateways require at least one 150 GiB disk to use as a cache. The cache storage acts as the on-premises durable store for data that is pending upload to Amazon S3 or file system. After the initial configuration and deployment of your gateway, you can add more disks for cache storage as your workload demands increase.

Note
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), 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. 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. This is also true if the backup is a less-performant RAID configuration such as RAID1.

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.

You can use the initial approximation of 150 GiB to provision disks for the cache storage during gateway setup. 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 Performance (p. 131).

Adding cache storage

As your application needs change, you can increase the gateway's cache storage capacity. You can add more cache capacity to your gateway without interrupting existing gateway functions. When you add more storage capacity, you do so with the gateway VM turned on.

Important
When adding cache 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. Do not remove cache disks that have been allocated as cache storage.

The following procedure shows you how to configure or cache storage for your gateway.

To add and configure 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. You configure this disk as 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 cached storage.

   If you don't see your disks, choose the **Refresh** button.
6. 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 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. 76).
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. 84).
6. You can now restart or stop the File Gateway without risk of losing any data.

Managing Bandwidth for Your Amazon S3 File Gateway

You can limit the upload throughput from your gateway to AWS to control the amount of network bandwidth the gateway uses. By default, an activated gateway has no rate limits.

You can configure a bandwidth-rate-limit schedule using the AWS Management Console, an AWS Software Development Kit (SDK), or the AWS Storage Gateway API (see UpdateBandwidthRateLimitSchedule in the *AWS Storage Gateway API Reference*.). Using a bandwidth rate limit schedule, you can configure limits to change automatically throughout the day or week. For more information, see View and edit the bandwidth-rate-limit schedule for your gateway using the Storage Gateway console (p. 93).

You can monitor your gateway's upload throughput using the `CloudBytesUploaded` metric on the **Monitoring** tab in the Storage Gateway console, or in Amazon CloudWatch.

> **Note**
> Bandwidth rate limits apply to Storage Gateway file uploads only. Other gateway operations are not affected.
> Bandwidth rate limiting works by balancing the throughput of all files being uploaded, averaged over every second. While it is possible for uploads to cross the bandwidth rate limit briefly for any given micro- or millisecond, this does not typically result in large spikes over longer periods of time.

Configuring bandwidth rate limits and schedules is not currently supported for the Amazon FSx File Gateway type.

Topics

- View and edit the bandwidth-rate-limit schedule for your gateway using the Storage Gateway console (p. 93)
- Updating Gateway Bandwidth-Rate Limits Using the AWS SDK for Java (p. 94)
- Updating Gateway Bandwidth-Rate Limits Using the AWS SDK for .NET (p. 95)
- Updating Gateway Bandwidth-Rate Limits Using the AWS Tools for Windows PowerShell (p. 97)

View and edit the bandwidth-rate-limit schedule for your gateway using the Storage Gateway console

This section describes how to view and edit the bandwidth rate limit schedule for your gateway.

To view and edit the bandwidth rate limit schedule

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. In the left 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 current bandwidth-rate-limit schedule is displayed on the **Edit bandwidth rate limit schedule** page. By default, a new gateway has no defined bandwidth-rate limits.
4. (Optional) Choose **Add new bandwidth rate limit** to add a new configurable interval to the schedule. For each interval you add, enter the following information:

   - **Upload rate** – Enter the upload rate limit, in megabits per second (Mbps). The minimum value is 100 Mbps.
   - **Days of week** – Select the day or days during each week when you want the interval to apply. You can apply the interval on weekdays (Monday through Friday), weekends (Saturday and Sunday), every day of the week, or on one specific day each week. To apply the bandwidth-rate limit uniformly and constantly on all days and at all times, choose **No schedule**.
   - **Start time** – Enter the start time for the bandwidth interval, using the HH:MM format and the time-zone offset from UTC 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 time-zone 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.
5. (Optional) Repeat the previous step as necessary until your bandwidth-rate-limit schedule is complete. If you need to delete an interval from your schedule, choose **Remove**.

   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. When finished, choose **Save changes**.

Updating Gateway Bandwidth-Rate Limits Using the AWS SDK for Java

By updating bandwidth-rate limits programmatically, you can adjust these 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-Rate Limits Using the AWS SDK for Java

The following Java code example updates a gateway's bandwidth-rate limits. To use this example code, you must provide the service endpoint, your gateway Amazon Resource Name (ARN), and the upload limit. For a list of AWS service endpoints that 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.
UpdateBandwidthRateLimitScheduleRequest;
    import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

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

    public class UpdateBandwidthExample {

        public static AWSStorageGatewayClient sgClient;

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

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

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

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

            // Create a Storage Gateway client
            sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

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

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

        }

        private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
```

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

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

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

Updating Gateway Bandwidth-Rate Limits Using the AWS SDK for .NET

By updating bandwidth-rate limits programmatically, you can adjust these 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 Software Development Kit (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-Rate Limits by Using the AWS SDK for .NET

The following C# code example updates a gateway's bandwidth-rate limits. To use this example code, you must provide the service endpoint, your gateway Amazon Resource Name (ARN), and the upload limit. For a list of AWS service endpoints that 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 = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

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

               UpdateBandwidth(gatewayARN, uploadRate, null);

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

           public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
           {
               try
               {
                  BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

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

```
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

Updating Gateway Bandwidth-Rate Limits Using the AWS Tools for Windows PowerShell

By updating bandwidth-rate limits programmatically, you can adjust these 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-Rate Limits by Using the AWS Tools for Windows PowerShell

The following PowerShell script example updates a gateway's bandwidth-rate limits. To use this example script, you must provide your gateway Amazon Resource Name (ARN) and the upload limit.

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

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


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

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

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

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

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

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

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.

Before any update is applied to your gateway, AWS notifies you with a message on the Storage Gateway console and your AWS Health Dashboard. For more information, see AWS 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.

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 pen 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.

Topics

- Performing tasks on the VM local console (File Gateway) (p. 99)
- Performing tasks on the Amazon EC2 local console (File Gateway) (p. 109)
- Accessing the Gateway Local Console (p. 114)
- Configuring Network Adapters for Your Gateway (p. 118)

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. 99)
- Configuring an HTTP proxy (p. 100)
- Configuring your gateway network settings (p. 101)
- Testing your gateway's network connectivity (p. 103)
- Viewing your gateway system resource status (p. 104)
- Configuring a Network Time Protocol (NTP) server for your gateway (p. 105)
- Running Storage Gateway commands on the local console (p. 106)
- Configuring network adapters for your gateway (p. 107)

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. 100).

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 by entering the corresponding numeral for **Gateway Console** from the **AWS Appliance Activation - Configuration** main menu, then running the `passwd` command. For information about how to run the command, see Running Storage Gateway commands on the local console (p. 106). 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. 100).

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. 8).

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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - 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. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Configure HTTP Proxy**.
3. From the **AWS Appliance Activation HTTP Proxy Configuration** menu, enter the corresponding numeral for the task you want to perform:
   - **Configure HTTP proxy** - You will need to supply a host name and port to complete configuration.

- **View current HTTP proxy configuration** - If an HTTP proxy is not configured, the message `HTTP Proxy not configured` is displayed. If an HTTP proxy is configured, the host name and port of the proxy are displayed.
- **Remove an HTTP proxy configuration** - The message `HTTP Proxy Configuration Removed` 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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Network Configuration**.
3. From the **Network Configuration** menu, perform one of the following tasks:

To Perform This Task	Do This
Get information about your network adapter	Enter the corresponding numeral to select **Describe Adapter**. A list of adapter names appears, and you are prompted to enter an adapter name—for example, **`eth0`**. If the adapter you specify is in use, the following information about the adapter is displayed: • Media access control (MAC) address • IP address • Netmask • Gateway IP address • DHCP enabled status You use the adapter names listed here when you configure a static IP address or when you set your gateway's default adapter.
Configure DHCP routing	Enter the corresponding numeral to select **Configure DHCP**. You are prompted to configure the network interface to use DHCP.

To Perform This Task	Do This
Configure a static IP address for your gateway	Enter the corresponding numeral to select **Configure Static IP**. You are prompted to enter the following information to configure a static IP: • Network adapter name • IP address • Netmask • Default gateway address • Primary Domain Name Service (DNS) address • Secondary DNS address **Important** 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 Shutting down your gateway VM (p. 90). If your gateway uses more than one network interface, you must set all enabled interfaces to use DHCP or static IP addresses. 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. If both interfaces are initially set to use static IP addresses and you then set the gateway to use DHCP, both interfaces use DHCP.
Reset all your gateway's network configuration to DHCP	Enter the corresponding numeral to select **Reset all to DHCP**. All network interfaces are set to use DHCP. **Important** 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 Shutting down your gateway VM (p. 90).

To Perform This Task	Do This
Set your gateway's default route adapter	Enter the corresponding numeral to select **Set Default Adapter**. The available adapters for your gateway are shown, and you are prompted to choose one of the adapters—for example, **`eth0`**.
Edit your gateway's DNS configuration	Enter the corresponding numeral to select **Edit DNS Configuration**. 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 the corresponding numeral to select **View DNS Configuration**. The available adapters of the primary and secondary DNS servers are displayed. **Note** For some versions of the VMware hypervisor, you can edit the adapter configuration in this menu.
View routing tables	Enter the corresponding numeral to select **View Routes**. The default route of your gateway is displayed.

Testing your gateway's network connectivity

You can use your gateway's local console to test your network connectivity. This test can be useful when you are troubleshooting network issues with your gateway.

To test your gateway's network connectivity

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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Test Network Connectivity**.

   If your gateway has already been activated, the connectivity test begins immediately. For gateways that have not yet been activated, you must specify the endpoint type and AWS Region as described in the following steps.
3. If your gateway is not yet activated, enter the corresponding numeral to select the endpoint type for your gateway.
4. If you selected the public endpoint type, enter the corresponding numeral to select the AWS Region that you want to test. 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*.

As the test progresses, each endpoint displays either **[PASSED]** or **[FAILED]**, indicating the status of the connection as follows:

Message	Description
[PASSED]	Storage Gateway has network connectivity.
[FAILED]	Storage Gateway does not have network 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 more information on logging in to the VMware ESXi console, see Accessing the Gateway Local Console with VMware ESXi (p. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **View System Resource Check**.

   Each resource displays **[OK]**, **[WARNING]**, or **[FAIL]**, indicating the status of the resource as follows:

Message	Description
[OK]	The resource has passed the system resource check.
[WARNING]	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.
[FAIL]	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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **System Time Management**.
3. From the **System Time Management** menu, enter the corresponding numeral to perform one of the following tasks.

To Perform This Task	Do This
View and synchronize your VM time with NTP server time.	Enter the corresponding numeral to select **View and Synchronize System Time**. 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. 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. 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. 191). 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. 195).

To Perform This Task	Do This
	For a gateway deployed on KVM, you can check and synchronize the VM time using `virsh` command line interface for KVM.
Edit your NTP server configuration	Enter the corresponding numeral to select **Edit NTP Configuration**. You are prompted to provide a preferred and a secondary NTP server.
View your NTP server configuration	Enter the corresponding numeral to select **View NTP Configuration**. Your NTP server configuration is displayed.

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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Gateway Console**.
3. From the gateway console command prompt, enter **h**.

   The console displays the **AVAILABLE COMMANDS** menu, which lists the available commands:

Command	Function
dig	Collect output from dig for DNS troubleshooting.
exit	Return to Configuration menu.
h	Display available command list.
ifconfig	View or configure network interfaces. **Note** We recommend configuring network or IP settings using the Storage Gateway console or the dedicated local console menu option. For instructions, see Configuring your gateway network settings.

Command	Function
ip	Show / manipulate routing, devices, and tunnels. **Note** We recommend configuring network or IP settings using the Storage Gateway console or the dedicated local console menu option. For instructions, see Configuring your gateway network settings.
iptables	Administration tool for IPv4 packet filtering and NAT.
ncport	Test connectivity to a specific TCP port on a network.
nping	Collect output from nping for network troubleshooting.
open-support-channel	Connect to AWS Support.
passwd	Update authentication tokens.
save-iptables	Persist IP tables.
save-routing-table	Save newly added routing table entry.
tcptraceroute	Collect traceroute output on TCP traffic to a destination.

4. From the gateway console command prompt, enter the corresponding command for the function you want to use, and follow the instructions.

To learn about a command, enter **`man`** + *`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. 107)
- Configuring your gateway for multiple NICs (p. 109)

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**.

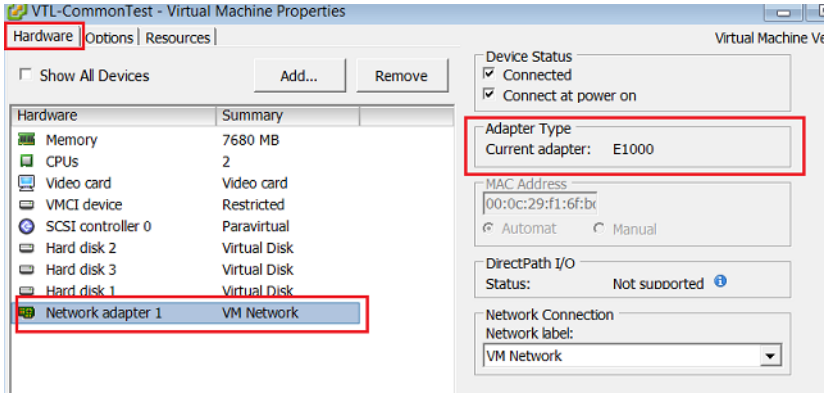
Following are the steps you take to configure your gateway to use the VMXNET3 adapter:

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. 99).

2. At the prompt, enter the corresponding numeral to select **Network Configuration**.
3. At the prompt, enter the corresponding numeral 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.

   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's network connectivity (p. 103).

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. 118)
- Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host (p. 122)

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. 110)
- Routing your gateway deployed on EC2 through an HTTP proxy (p. 110)
- Testing your gateway's network connectivity (p. 111)

- Viewing your gateway system resource status (p. 111)
- Running Storage Gateway commands on the local console (p. 112)
- Configuring your gateway network settings (p. 113)

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, from which you can perform various tasks.

To Learn About This Task	See This Topic
Configure an HTTP proxy for your gateway	Routing your gateway deployed on EC2 through an HTTP proxy (p. 110)
Configure network settings for your gateway	Configuring your gateway network settings (p. 113)
Test network connectivity	Testing your gateway's network connectivity (p. 111)
View a system resource check	Viewing your gateway system resource status (p. 111).
Run Storage Gateway console commands	Running Storage Gateway commands on the local console (p. 112)

To shut down the gateway, enter **0**.

To exit the configuration session, enter **x**.

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. 110).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Configure HTTP Proxy**.

3. From the **AWS Appliance Activation HTTP Proxy Configuration** menu, enter the corresponding numeral for the task you want to perform:

   - **Configure HTTP proxy** - You will need to supply a host name and port to complete configuration.
   - **View current HTTP proxy configuration** - If an HTTP proxy is not configured, the message `HTTP Proxy not configured` is displayed. If an HTTP proxy is configured, the host name and port of the proxy are displayed.
   - **Remove an HTTP proxy configuration** - The message `HTTP Proxy Configuration Removed` is displayed.

Testing your gateway's network connectivity

You can use your gateway's local console to test your network connectivity. This test can be useful when you are troubleshooting network issues with your gateway.

To test your gateway's connectivity

1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 110).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Test Network Connectivity**.

   If your gateway has already been activated, the connectivity test begins immediately. For gateways that have not yet been activated, you must specify the endpoint type and AWS Region as described in the following steps.
3. If your gateway is not yet activated, enter the corresponding numeral to select the endpoint type for your gateway.
4. If you selected the public endpoint type, enter the corresponding numeral to select the AWS Region that you want to test. 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*.

As the test progresses, each endpoint displays either **[PASSED]** or **[FAILED]**, indicating the status of the connection as follows:

Message	Description
[PASSED]	Storage Gateway has network connectivity.
[FAILED]	Storage Gateway does not have network 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. 110).

2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **View System Resource Check**.

   Each resource displays **[OK]**, **[WARNING]**, or **[FAIL]**, indicating the status of the resource as follows:

Message	Description
[OK]	The resource has passed the system resource check.
[WARNING]	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.
[FAIL]	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. 110).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Gateway Console**.
3. From the gateway console command prompt, enter `h`.

   The console displays the **AVAILABLE COMMANDS** menu, which lists the available commands:

Command	Function
dig	Collect output from dig for DNS troubleshooting.
exit	Return to Configuration menu.
h	Display available command list.
ifconfig	View or configure network interfaces. **Note** We recommend configuring network or IP settings using the Storage Gateway console or the dedicated local console menu option. For instructions, see

Command	Function
	Configuring your gateway network settings.
ip	Show / manipulate routing, devices, and tunnels. **Note** We recommend configuring network or IP settings using the Storage Gateway console or the dedicated local console menu option. For instructions, see Configuring your gateway network settings.
iptables	Administration tool for IPv4 packet filtering and NAT.
ncport	Test connectivity to a specific TCP port on a network.
nping	Collect output from nping for network troubleshooting.
open-support-channel	Connect to AWS Support.
save-iptables	Persist IP tables.
save-routing-table	Save newly added routing table entry.
tcptraceroute	Collect traceroute output on TCP traffic to a destination.

4. From the gateway console command prompt, enter the corresponding command for the function you want to use, and follow the instructions.

To learn about a command, enter **`man`** + *`command name`* at the command prompt.

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. 110).
2. From the **AWS Appliance Activation - Configuration** main menu, enter the corresponding numeral to select **Network Configuration**.
3. From the **AWS Appliance Activation - Network Configuration** menu, enter the corresponding numeral for the task you want to perform:
   - **Edit DNS Configuration** - The available adapters of the primary and secondary DNS servers are displayed. You are prompted to provide the new IP address.
   - **View DNS Configuration** - The available adapters of the primary and secondary DNS servers are displayed.

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.

Topics

- Accessing the Gateway Local Console with Linux KVM (p. 114)
- Accessing the Gateway Local Console with VMware ESXi (p. 116)
- Access the Gateway Local Console with Microsoft Hyper-V (p. 117)

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`.

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 File Gateway local console (p. 99).
4. After you have logged in, you can activate and configure your gateway.

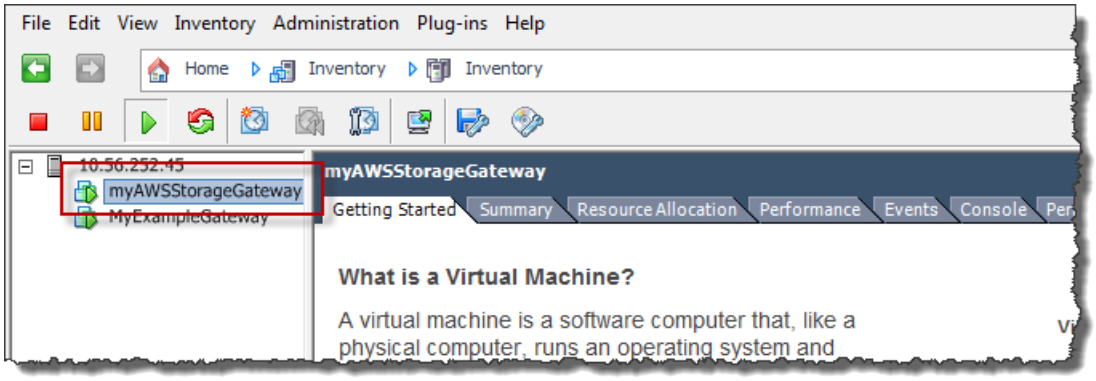
```
        AWS Appliance Activation - Configuration

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

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

        0: Get activation key

        Press "x" to exit session

        Enter command: _
```

Accessing the Gateway Local Console with VMware ESXi

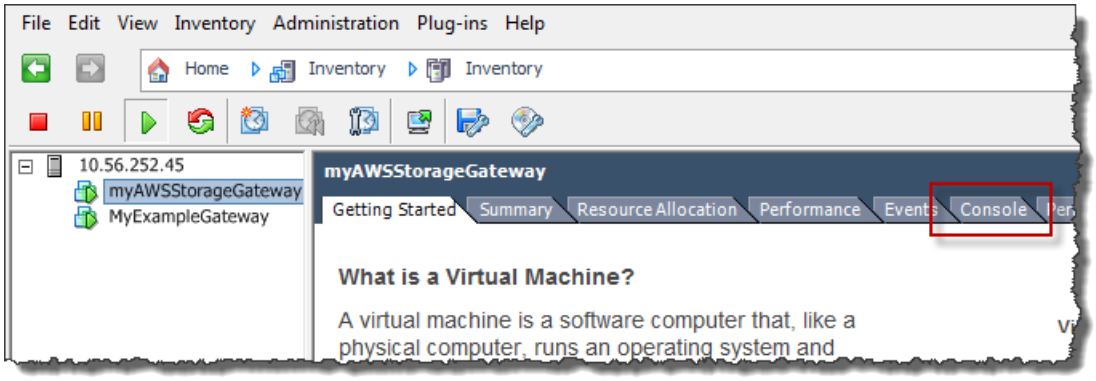
To access your gateway's local console with VMware ESXi

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**.

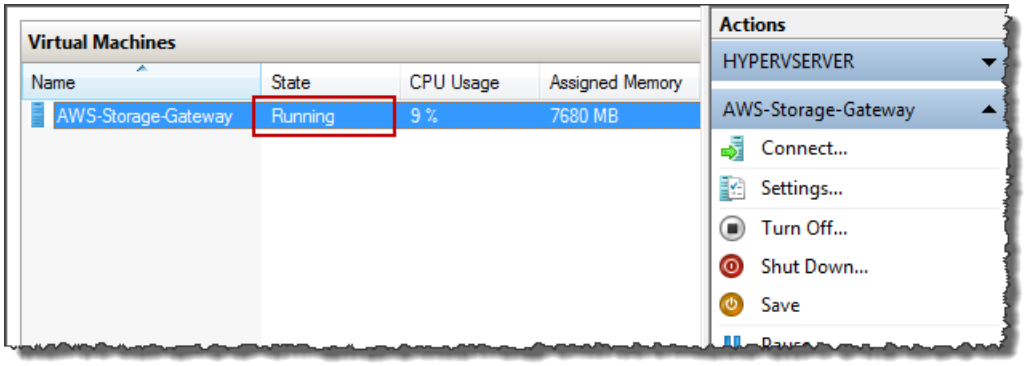
4. To log in using the default credentials, continue to the procedure Logging in to the File Gateway local console (p. 99).

Access the Gateway Local Console with Microsoft Hyper-V

To access your gateway's local console (Microsoft Hyper-V)

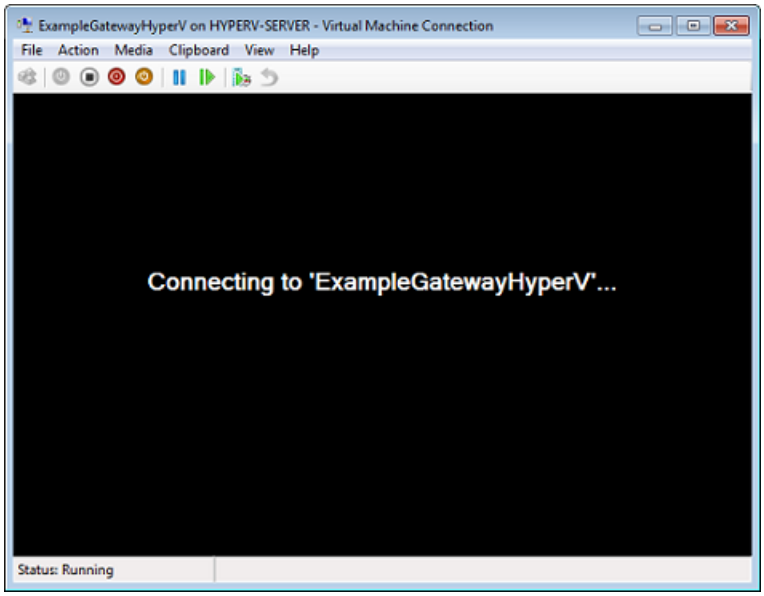
1. In the **Virtual Machines** list of the Microsoft Hyper-V Manager, select your gateway VM.
2. Make sure that the gateway is turned on.

   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 File Gateway local console (p. 99).

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. 118)
- Configuring Your Gateway for Multiple NICs in Microsoft Hyper-V Host (p. 122)

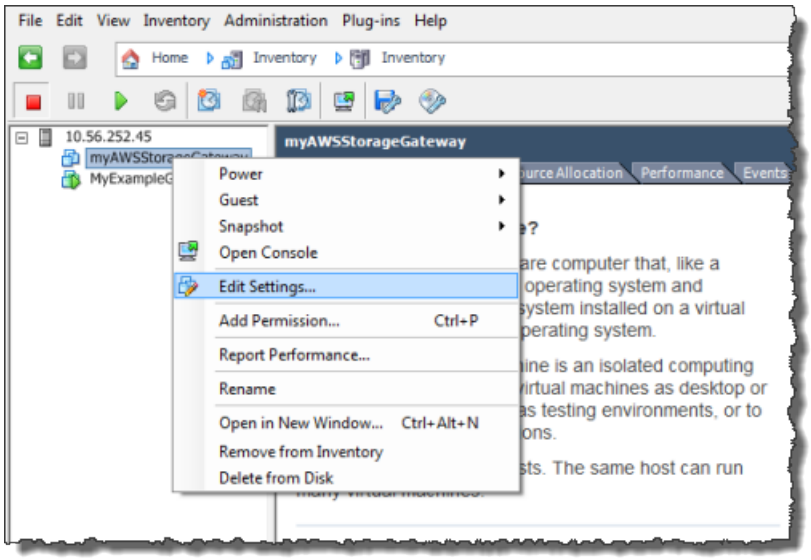
Configuring Your Gateway for Multiple NICs in a VMware ESXi Host

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.

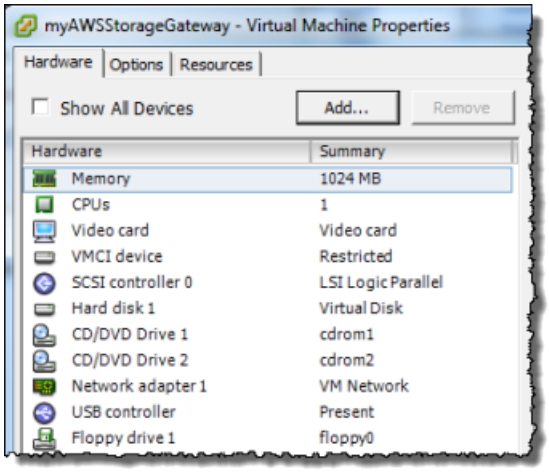
To configure your gateway to use an additional network adapter in VMware ESXi host

1. Shut down the gateway.
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**.

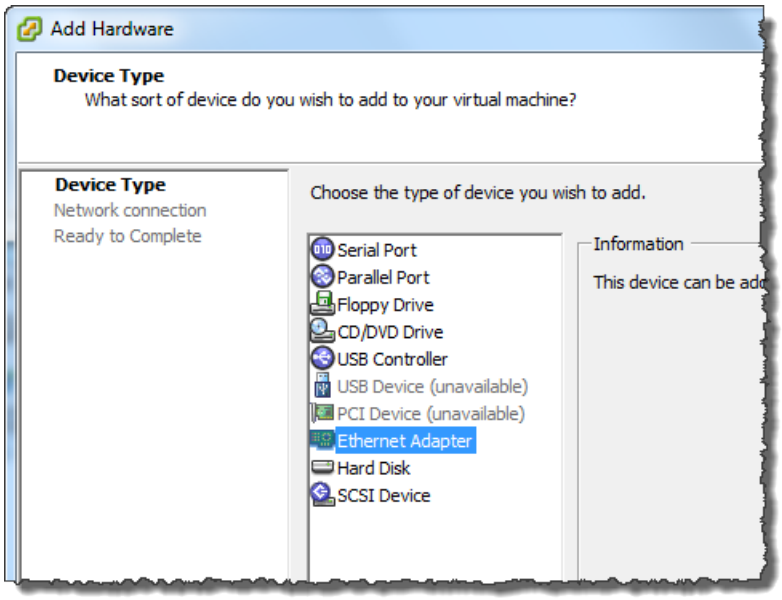


4. On the **Hardware** tab of the **Virtual Machine Properties** dialog box, choose **Add** to add a device.



5. Follow the Add Hardware wizard to add a network adapter.

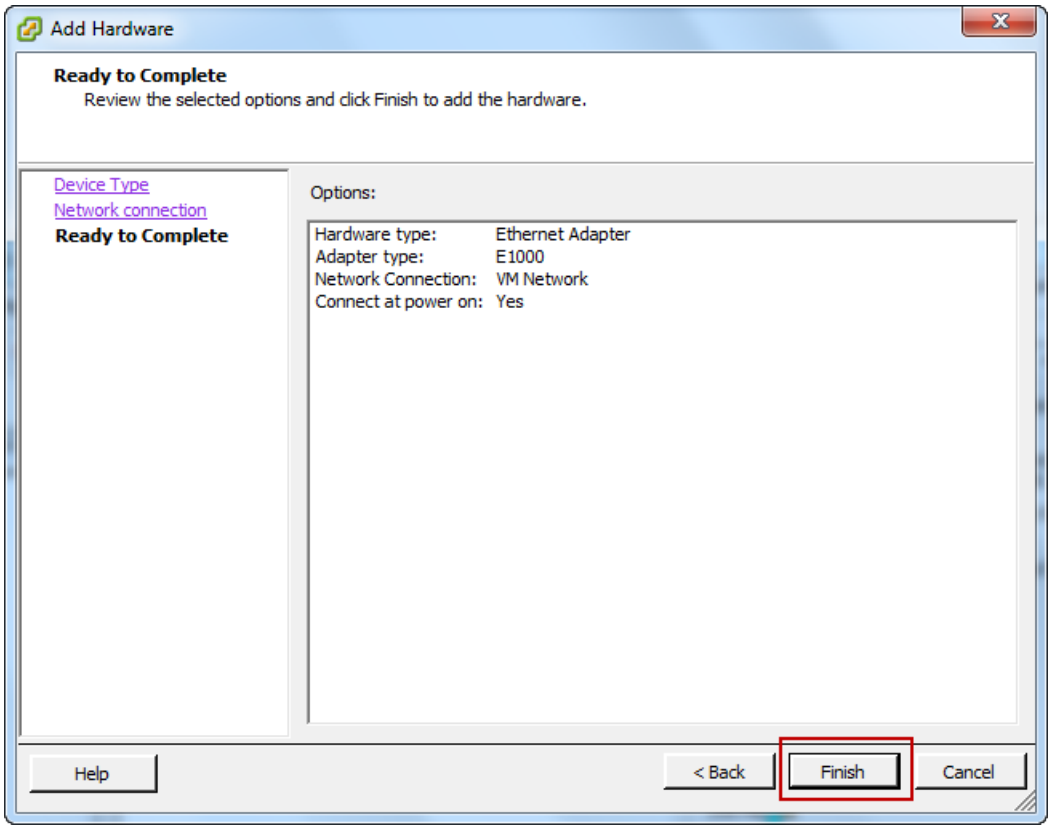
   a. In the **Device Type** pane, choose **Ethernet Adapter** to add an adapter, and then choose **Next**.



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 E1000 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.

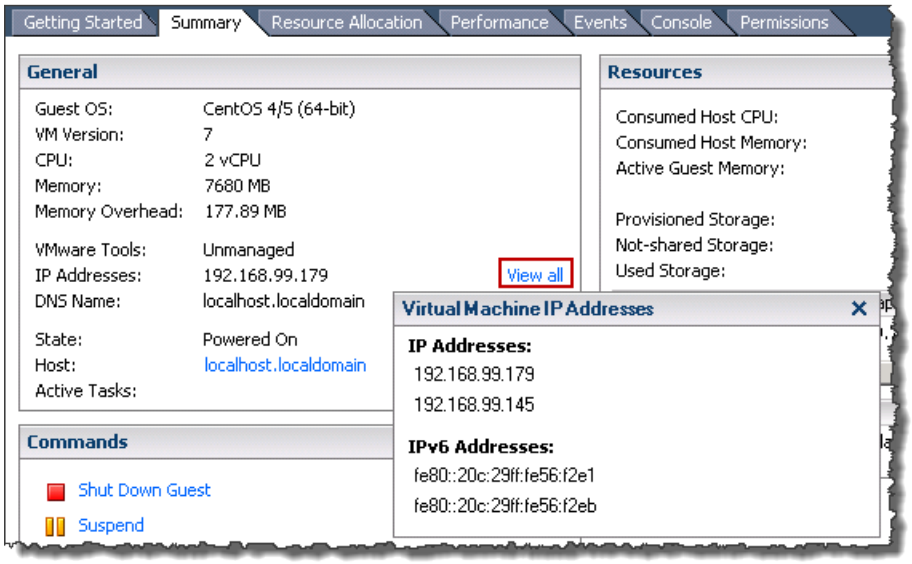
c. In the **Ready to Complete** pane, review the information, and then choose **Finish**.



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.
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.

   Note
   The example mounting commands provided on the info page for a file share in the Storage Gateway console will always include the IP address of the network adapter that was most recently added to the file share's associated gateway.

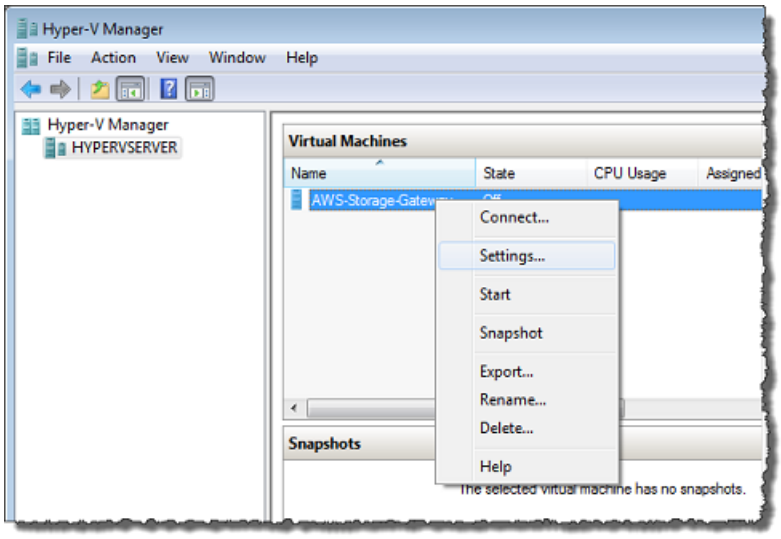
For information about local console tasks common to VMware, Hyper-V, and KVM hosts, see Performing tasks on the VM local console (File Gateway) (p. 99)

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.

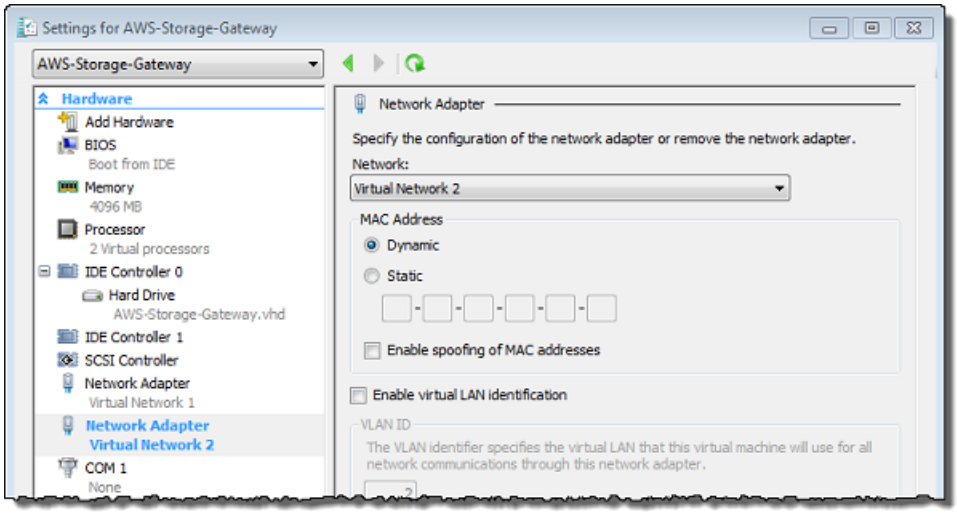
To configure your gateway to use an additional network adapter in a Microsoft Hyper-V Host

1. On the Storage Gateway console, turn off the gateway.
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.
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.

    Note
    The example mounting commands provided on the info page for a file share in the Storage Gateway console will always include the IP address of the network adapter that was most recently added to the file share's associated gateway.

For information about local console tasks common to VMware, Hyper-V, and KVM hosts, see Performing tasks on the VM local console (File Gateway) (p. 99)

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. 124)
- Removing Resources from a Gateway Deployed On-Premises (p. 125)
- Removing Resources from a Gateway Deployed on an Amazon EC2 Instance (p. 125)

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.

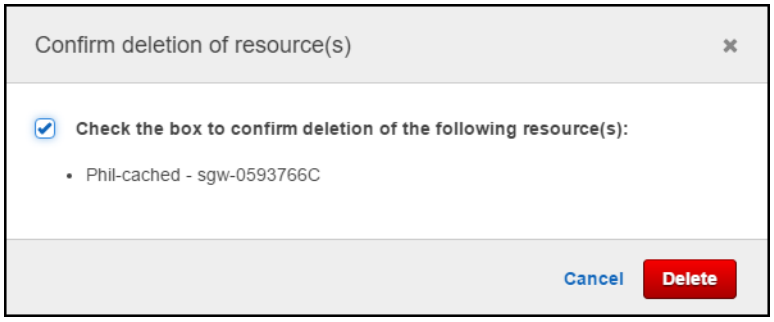
> **Note**
> For gateways deployed on an Amazon EC2 instance, the instance continues to exist until you delete it.
> For gateways deployed on a virtual machine (VM), after you delete your gateway the gateway VM still exists in your virtualization environment. To remove the VM, use the VMware vSphere 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, be 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.

Also, when a gateway is deleted, there is no way to get it back.

In the confirmation dialog box that appears, select the check box to confirm your deletion. Make sure the gateway ID listed specifies the gateway you want to delete. and then choose **Delete**.



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.

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, 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. 124).

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*.

Replacing your existing File Gateway with a new instance

You can replace an existing File Gateway with a new instance as your data and performance needs grow, or if you receive an AWS notification to migrate your gateway. You might need to do this if you want to move your gateway to a better host platform or newer Amazon EC2 instances, or to refresh the underlying server hardware.

There are two methods to replace an existing File Gateway. The following table describes the benefits and drawbacks of each method. Using this information, select the method best suited for your gateway environment, then refer to the procedure steps in the corresponding section below.

Note
If you need to log into your new Storage Gateway's local console to complete either method, the default username is *admin*, and the default password is *password*.

	Method 1: Migrate cache disk and Gateway ID to replacement instance	**Method 2: Replacement instance with empty cache disk and new Gateway ID**
Cache disk data	Data on the cache disk is preserved. This method is useful if your gateway has a large cache disk, or if your applications are sensitive to the delay caused by out-of-cache read operations.	Data in cache is downloaded from the AWS cloud. This method is optimal for write-heavy workloads, if your applications can tolerate the delay caused by out-of-cache reads.
Down time	Your gateway will be offline for 1-2 hours during the migration process.	File shares are always available, but clients will experience short cutover downtime when switching from one file share to another during the transition to the new instance. **Note** Writing to one Amazon S3 bucket from two file shares simultaneously is *not supported*, so all clients must be remapped from one share to the other simultaneously, rather than gradually.
Gateway ID	The new gateway inherits the Gateway ID from the gateway it replaces.	The existing gateway and replacement gateway have separate, unique Gateway IDs.

Note
Migration can only be performed between gateways of the same type.

Method 1: Migrate cache disk and Gateway ID to replacement instance

To migrate your File Gateway's cache disk and Gateway ID to a replacement instance:

1. Stop any applications that are writing to the existing File Gateway.
2. Verify that the `CachePercentDirty` metric on the **Monitoring** tab for the existing File Gateway is `0`.
3. Shut down the existing File Gateway by powering off the host virtual machine (VM) using its hypervisor controls.

   For more information about shutting down an Amazon EC2 instance, see Stop and start your instance in the *Amazon EC2 User Guide*.

   For more information about shutting down a KVM, VMware, or Hyper-V VM, see your hypervisor documentation.
4. 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 will need to detach this disk from the new Storage Gateway hypervisor in a later step.

   If you are using an Amazon EC2 instance as the VM for your File Gateway, see Detach an Amazon EBS volume from a Windows instance or Detach an Amazon EBS volume from a Linux instance in the *Amazon EC2 User Guide*.

   For information about detaching disks from a KVM, VMware, or Hyper-V VM, see the documentation for your hypervisor.
5. Create a new AWS Storage Gateway hypervisor VM instance, but don't activate it as a gateway. In a later step, this new VM will assume the identity of the old gateway.

   For more information about creating a new Storage Gateway hypervisor VM, see Choosing a Host Platform and Downloading the VM.

   Note
   Do not add cache disks for the new VM. This VM will use the same cache disks that were used by the old VM.
6. Configure your new Storage Gateway VM to use the same network settings 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 gateway VM, see Configuring Your Gateway Network.

   If your gateway VM must use a Socket Secure version 5 (SOCKS5) proxy to connect to the internet, see Routing Your On-Premises Gateway Through a Proxy.
7. Start the new Storage Gateway VM.
8. Attach the disks that you detached from the old gateway VM to the new gateway VM. Do not detach the existing root disk from the new gateway VM.

   Note
   To migrate successfully, all disks must remain unchanged. Changing the disk size or other values causes inconsistencies in metadata that prevent successful migration.

9. 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 use the same IP address for the new gateway VM that you used for the old gateway VM. Your URL should look similar to the following example:

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

   Use this URL from a browser, or from the command line using cURL.

   When the gateway migration initiates successfully, the following message appears:

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

10. Wait for the gateway status to show as **Running** in the AWS Storage Gateway console. Depending on available bandwidth, this can take up to 10 minutes.
11. Stop the new Storage Gateway VM.
12. Detach the old gateway's root disk, whose volume ID you noted previously, from the new gateway.
13. Start the new Storage Gateway VM.
14. If your gateway was joined to an Active Directory domain, re-join the domain. For instructions, see Using Active Directory to authenticate users.

    Note
    You must complete this step even if the status of the File Gateway appears as **Joined**.

15. Confirm that your shares are available at the new gateway VM's IP address, then delete the old gateway VM.

    Warning
    When a gateway is deleted, there is no way to recover it.

    For more information about deleting an Amazon EC2 instance, see Terminate your instance in the *Amazon EC2 User Guide*. For more information about deleting a KVM, VMware, or Hyper-V VM, see the documentation for your hypervisor.

Method 2: Replacement instance with empty cache disk and new Gateway ID

To set up a replacement File Gateway instance with empty cache disk and new Gateway ID:

1. Stop any applications that are writing to the existing File Gateway. Verify that the `CachePercentDirty` metric on the **Monitoring** tab is `0` before you set up file shares on the new gateway.
2. Use the AWS Command Line Interface (AWS CLI) to gather and save the configuration information about your existing File Gateway and file shares by doing the following:

   a. Save the gateway configuration information for the File Gateway.

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

This command outputs a JSON block that contains metadata about the gateway, such as its name, network interfaces, configured time zone, and its state (whether the gateway is running).

b. Save the Server Message Block (SMB) settings of the File Gateway.

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

This command outputs a JSON block that contains metadata about the SMB file share, such as its domain name, Microsoft Active Directory status, whether the guest password is set, and the type of security strategy.

c. Save file share information for each SMB and Network File System (NFS) file share of the File Gateway:

- Use the following command for SMB file shares.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

This command outputs a JSON block that contains metadata about the NFS file share, such as its name, storage class, status, IAM role Amazon Resource Name (ARN), a list of clients that are allowed to access the File Gateway, and the path used by the SMB client to identify the mount point.

- Use the following command for NFS file shares.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

This command outputs a JSON block that contains metadata about the NFS file share, such as its name, storage class, status, IAM role ARN, a list of clients that are allowed to access the File Gateway, and the path used by the NFS client to identify the mount point.

3. Create a new File Gateway with the same settings and configuration as the old gateway. If necessary, refer to the information you saved in Step 2.
4. Create new file shares for the new gateway with the same settings and configuration as the file shares that were configured on the old gateway. If necessary, refer to the information you saved in Step 2.
5. Confirm that your new gateway is working correctly, then remap/cut-over your clients from the old file shares to the new file shares in the manner that best suits your environment.
6. Confirm that your new gateway is working correctly, then delete the old gateway from the Storage Gateway console.

   Important
   Before you delete a gateway, make sure that there are no applications currently writing to that File Gateway's cache. If you delete a File Gateway while it is in use, data loss can occur.

   Warning
   When a gateway is deleted, there is no way to recover it.
7. Delete the old gateway virtual machine or EC2 instance.

Performance

In this section, you can find information about Storage Gateway performance.

Topics

- Performance guidance for File Gateways (p. 131)
- Optimizing Gateway Performance (p. 133)
- Using VMware vSphere High Availability with Storage Gateway (p. 135)

Performance guidance for File Gateways

In this section, you can find guidance for provisioning hardware for your File Gateway VM. The instance configurations 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.

> **Note**
> We don't recommend using ephemeral storage. For information about using ephemeral storage, see Using ephemeral storage with EC2 gateways (p. 91).
> For Amazon EC2 instances, 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).

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.

Following are example File Gateway configurations.

S3 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 SSD, 4,000 IOPS Cache disk: 512 GiB cache, io1, 1,500 provisioned IOPS Minimum network performance: 10 Gbps CPU: 16 vCPU | RAM: 32 GB	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)
	SMBV3 - 8 threads	190 MiB/sec (1.6 Gbps)	590 MiB/sec (4.9 Gbps)	335 MiB/sec (2.8 Gbps)

Example Configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
NFS protocol recommended for Linux				
Storage Gateway Hardware Appliance 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

Example Configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Root disk: 80 GB, io1 SSD, 4,000 IOPS Cache disk: 512 GiB cache, io1, 1,500 provisioned 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)
	NFSv3 - 1 thread	95 MiB/sec (0.8 Gbps)	130 MiB/sec (1.1 Gbps)	20 MiB/sec (0.2 Gbps)

Example Configurations	Protocol	Write throughput (file sizes 1 GB)	Cache hit read throughput	Cache miss read throughput
Minimum network performance: 10 Gbps CPU: 16 vCPU | RAM: 32 GB SMB protocol recommended for Windows	NFSv3 - 8 threads	190 MiB/sec (1.6 Gbps)	330 MiB/sec (2.8 Gbps)	190 MiB/sec (1.6 Gbps)
Storage Gateway Hardware Appliance Minimum network performance: 10 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)
	NFSv3 - 8 threads	545 MiB/sec (4.6 Gbps)	470 MiB/sec (4.0 Gbps)	190 MiB/sec (1.6 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	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.

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). For information about adding disks, see Adding cache storage (p. 91).

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.

Note
CloudWatch metrics are not available for all gateways. For information about gateway metrics, see Monitoring your File Gateway (p. 73).

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
  - 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 local 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.

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 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. 136)
- Download the .ova Image for Your Gateway Type (p. 137)
- Deploy the Gateway (p. 137)
- (Optional) Add Override Options for Other VMs on Your Cluster (p. 137)
- Activate Your Gateway (p. 138)
- Test Your VMware High Availability Configuration (p. 138)

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.

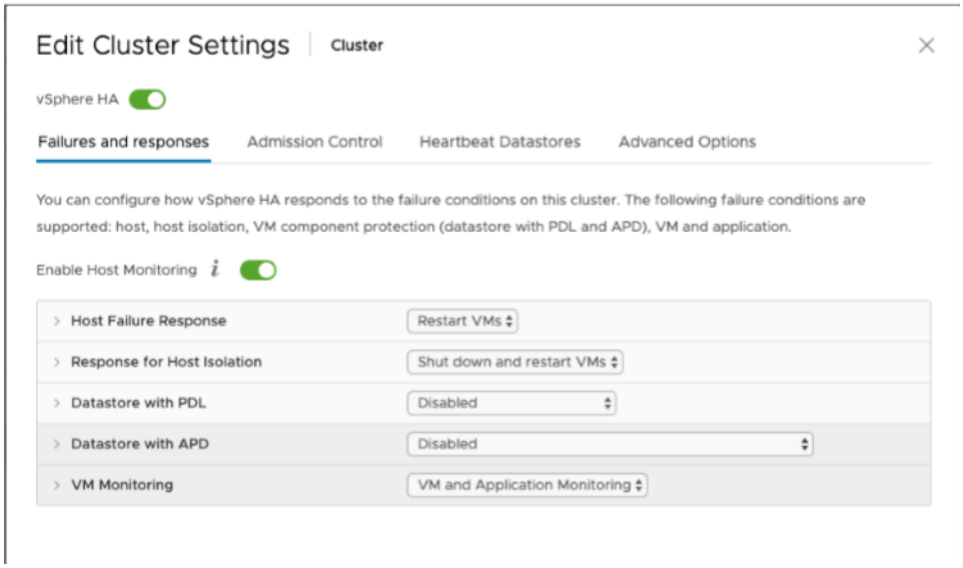
Next, configure your VMware cluster to work with Storage Gateway.

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. 137).

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 –

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.

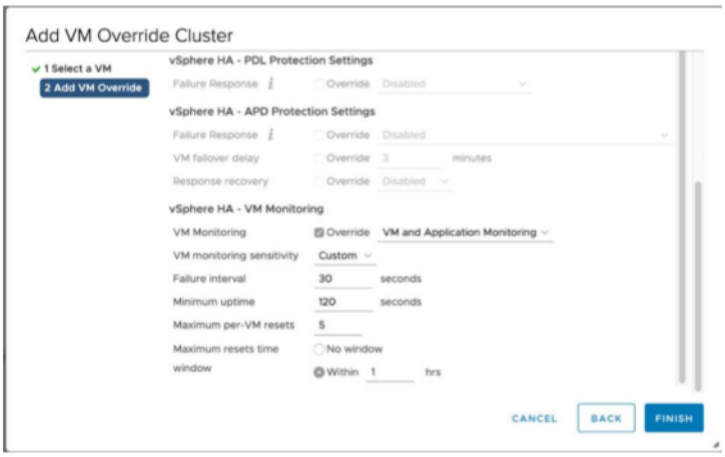
(Optional) Add Override Options for Other VMs on Your Cluster

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 –

Test Your VMware High Availability Configuration

After you activate your gateway, test your configuration.

To test your VMware HA configuration

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 that you want to test for VMware HA.
3. For **Actions**, choose **Verify VMware HA**.
4. 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.
5. 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. 73).

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 AWS 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. 139)
- Authentication and access control for Storage Gateway (p. 141)
- Logging and monitoring in AWS Storage Gateway (p. 164)
- Compliance validation for AWS Storage Gateway (p. 166)
- Resilience in AWS Storage Gateway (p. 167)
- Infrastructure security in AWS Storage Gateway (p. 167)
- AWS Security Best Practices (p. 167)

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) keys.

> **Important**
> When you use an AWS KMS key for server-side encryption, you must choose a symmetric key. Storage Gateway does not support asymmetric keys. 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 file system

For information see, Data Encryption in Amazon FSxin the *Amazon FSx for Windows File Server User Guide*.

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 KMS key or revoke the grant token, you can't access the data on the volume or tape. For more information, see Deleting KMS 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?

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. 141)
- Access control (p. 142)

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. 143)
- Identity-based policies (IAM policies) (p. 144)

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. 143)
- Understanding resource ownership (p. 144)
- Managing access to resources (p. 144)
- Specifying policy elements: Actions, effects, resources, and principals (p. 145)
- Specifying conditions in a policy (p. 146)

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	`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*
File share ARN	`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:share/`*`share-id`*

> **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 provides a set of API actions for you to create and manage these resources and subresources. For a list of API actions, see Actions in the *AWS Storage Gateway API Reference*.

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. 156).

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. 144)
- Resource-based policies (p. 145)

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 a 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. 146). 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. 156)), 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. 143).
- **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. 156).

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. 143).

The sections in this topic cover the following:

- Permissions required to use the Storage Gateway console (p. 147)
- AWS managed policies for Storage Gateway (p. 148)
- Customer managed policy examples (p. 148)

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. 149).

  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. 156).

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. 149).

AWS managed policies for Storage Gateway

Amazon Web Services 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. 147).

> **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. 148)
- Example 2: Allow read-only access to a gateway (p. 149)
- Example 3: Allow access to a specific gateway (p. 150)
- Example 4: Allow a user to access a specific volume (p. 151)
- Example 5: Allow all actions on gateways with a specific prefix (p. 152)

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 a 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 AWS 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 AWS Storage Gateway console, you must grant additional permissions as described in Example 3: Allow access to a specific gateway (p. 150).

Using tags to control access to your gateway and resources

To control access to gateway resources and actions, you can use AWS Identity and Access Management (IAM) policies based on tags. You can provide the control in two ways:

1. Control access to gateway resources based on the tags on those resources.
2. Control what tags can be passed in an IAM request condition.

For information about how to use tags to control access, see Controlling Access Using Tags.

Controlling access based on tags on a resource

To control what actions a user or role can perform on a gateway resource, you can use tags on the gateway resource. For example, you might want to allow or deny specific API operations on a File Gateway resource based on the key-value pair of the tag on the resource.

The following example allows a user or a role to perform the `ListTagsForResource`, `ListFileShares`, and `DescribeNFSFileShares` actions on all resources. The policy applies only if the tag on the resource has its key set to `allowListAndDescribe` and the value set to `yes`.

```
{
  "Version": "2012-10-17",
   "Statement": [
      {
          "Effect": "Allow",
                    "Action": [
                        "storagegateway:ListTagsForResource",
                        "storagegateway:ListFileShares",
                        "storagegateway:DescribeNFSFileShares"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/allowListAndDescribe": "yes"
                        }
                    }
      },
      {
          "Effect": "Allow",
          "Action": [
              "storagegateway:*"
          ],
          "Resource": "arn:aws:storagegateway:region:account-id:*/*"
      }
  ]
}
```

Controlling access based on tags in an IAM request

To control what an IAM user can do on a gateway resource, you can use conditions in an IAM policy based on tags. For example, you can write a policy that allows or denies an IAM user the ability to perform specific API operations based on the tag they provided when they created the resource.

In the following example, the first statement allows a user to create a gateway only if the key-value pair of the tag they provided when creating the gateway is **`Department`** and **`Finance`**. When using the API operation, you add this tag to the activation request.

The second statement allows the user to create a Network File System (NFS) or Server Message Block (SMB) file share on a gateway only if the key-value pair of the tag on the gateway matches **`Department`**and **`Finance`**. Additionally, the user must add a tag to the file share, and the key-value pair of the tag must be **`Department`** and **`Finance`**. You add tags to a file share when creating the file share. There aren't permissions for the `AddTagsToResource` or `RemoveTagsFromResource` operations, so the user can't perform these operations on the gateway or the file share.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
```

```
            }
        },
        {
            "Effect":"Allow",
            "Action":[
                "storagegateway:CreateNFSFileShare",
                "storagegateway:CreateSMBFileShare"
            ],
            "Resource":"*",
            "Condition":{
                "StringEquals":{
                    "aws:ResourceTag/Department":"Finance",
                    "aws:RequestTag/Department":"Finance"
                }
            }
        }
    ]
}
```

Using Microsoft Windows ACLs to control access to an SMB file share

Amazon S3 File Gateway supports two different methods for controlling access to files and directories that are stored through an SMB file share: POSIX permissions, or Windows ACLs.

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.

Following are some important characteristics of Windows ACLs on SMB file shares:

- Windows ACLs are selected by default for SMB file shares when your File Gateway is joined to an Active Directory domain.
- 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 .
2. If the gateway is not joined to a domain, add it to a domain. For more information, see .
3. Create an SMB file share.

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. 142) 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. 143).

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/vtldevice`

Related topics

- Access control (p. 142)
- Customer managed policy examples (p. 148)

Using service-linked roles for Storage Gateway

Storage Gateway uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Storage Gateway. Service-linked roles are predefined by Storage Gateway and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Storage Gateway easier because you don't have to manually add the necessary permissions. Storage Gateway defines the permissions of its service-linked roles, and unless defined otherwise, only Storage Gateway can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Storage Gateway

Storage Gateway uses the service-linked role named **AWSServiceRoleForStorageGateway** – AWSServiceRoleForStorageGateway.

The AWSServiceRoleForStorageGateway service-linked role trusts the following services to assume the role:

- `storagegateway.amazonaws.com`

The role permissions policy allows Storage Gateway to complete the following actions on the specified resources:

- Action: `fsx:ListTagsForResource` on `arn:aws:fsx:*:*:backup/*`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create and edit a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for Storage Gateway

You don't need to manually create a service-linked role. When you make an Storage Gateway `AssociateFileSystem` API call in the AWS Management Console, the AWS CLI, or the AWS API, Storage Gateway creates the service-linked role for you.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, if you were using the Storage Gateway service before March 31, 2021, when it began supporting service-linked roles, then Storage Gateway created the AWSServiceRoleForStorageGateway role in your account. To learn more, see A New Role Appeared in My IAM Account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you make an Storage Gateway `AssociateFileSystem` API call, Storage Gateway creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role with the **AWSServiceRoleForStorageGateway** use case. In the AWS CLI or the AWS API, create a service-linked role with the `storagegateway.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for Storage Gateway

Storage Gateway does not allow you to edit the AWSServiceRoleForStorageGateway service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for Storage Gateway

Storage Gateway doesn't automatically delete the AWSServiceRoleForStorageGateway role. To delete AWSServiceRoleForStorageGateway role, you need to invoke the `iam:DeleteSLR` API. If there are no Storage Gateway resources that depend on the service-linked-role then the deletion will succeed, otherwise the deletion will fail. If you want to delete the service linked role, you need to use IAM APIs `iam:DeleteRole` or `iam:DeleteServiceLinkedRole`. In this case, you need to use the Storage Gateway APIs to first delete any gateways or file system associations in the account, then delete the service linked role by using `iam:DeleteRole` or `iam:DeleteServiceLinkedRole` API. When you are deleting the service linked role using IAM, you need to use Storage Gateway `DisassociateFileSystemAssociation` API first to delete all file system associations in the account. Otherwise, the deletion operation will fail.

> **Note**
> If the Storage Gateway service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Storage Gateway resources used by the AWSServiceRoleForStorageGateway

1. Use our service console, CLI, or API to make a call that cleans up the resources and deletes the role or use the IAM console, CLI, or API to do the deletion. In this case, you need to use Storage Gateway APIs to first delete any gateways and file-system-associations in the account.
2. If you use the IAM console, CLI, or API, delete the service-linked role using IAM `DeleteRole` or `DeleteServiceLinkedRole` API.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForStorageGateway service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for Storage Gateway service-linked roles

Storage Gateway supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS service endpoints.

Storage Gateway does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForStorageGateway role in the following Regions.

Region name	Region identity	Support in Storage Gateway
US East (N. Virginia)	us-east-1	Yes
US East (Ohio)	us-east-2	Yes
US West (N. California)	us-west-1	Yes
US West (Oregon)	us-west-2	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes

Region name	Region identity	Support in Storage Gateway
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Paris)	eu-west-3	Yes
South America (São Paulo)	sa-east-1	Yes
AWS GovCloud (US)	us-gov-west-2	Yes

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 AWS 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 AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS 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": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                        "gatewayTimezone": "GMT-5:00",
                                        "gatewayName": "cloudtrailgatewayvtl",
                                        "gatewayRegion": "us-east-2",
                                        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                        "gatewayType": "VTL"
                                             },
                                             "responseElements": {
                                                                  "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                             },
                                             "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                             "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
```

```
                                                "eventType": "AwsApiCall",
                                                "apiVersion": "20130630",
                                                "recipientAccountId": "444455556666"
            }]
}
```

The following example shows a CloudTrail log entry that demonstrates the ListGateways action.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                 "type": "IAMUser",
                                 "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                 "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/
JohnDoe",
                                 "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                 " userName ":" JohnDoe "
                                 },

                                 " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                 " eventSource ":" storagegateway.amazonaws.com ",
                                 " eventName ":" ListGateways ",
                                 " awsRegion ":" us-east-2 ",
                                 " sourceIPAddress ":" 192.0.2.0 ",
                                 " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6 Linux /
 2.6.18 - 164.el5 ",
                                 " requestParameters ":null,
                                 " responseElements ":null,
                                 "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                 " eventID ":" f76e5919 - 9362 - 48ff - a7c4 - d203a189ec8d
 ",
                                 " eventType ":" AwsApiCall ",
                                 " apiVersion ":" 20130630 ",
                                 " recipientAccountId ":" 444455556666"
              }]
}
```

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, MTCS, 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.
- Use AWS Backup to back up your volumes. For more information, see Using AWS Backup to back up your volumes.
- Clone your volume from a recovery point. For more information, see Cloning a volume.
- Archive virtual tapes in Amazon S3 Glacier. For more information, see Archiving virtual tapes.

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.

AWS Security Best Practices

AWS provides a number of security features to consider as you develop and implement your own security policies. These best practices are general guidelines and don't represent a complete security solution.

Because these 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 and best practices

Following, you can find information about best practices and troubleshooting issues related to gateways, file shares, and snapshots. The on-premises gateway troubleshooting information covers gateways deployed on supported virtualization platforms. The troubleshooting information for high availability issues covers gateways running on VMware vSphere High Availability (HA) platform.

Topics

- Troubleshooting: on-premises gateway issues (p. 169)
- Troubleshooting: Microsoft Hyper-V setup (p. 172)
- Troubleshooting: Amazon EC2 gateway issues (p. 175)
- Troubleshooting: hardware appliance issues (p. 177)
- Troubleshooting: File Gateway issues (p. 179)
- Troubleshooting: file share issues (p. 183)
- High Availability Health Notifications (p. 188)
- Troubleshooting: high availability issues (p. 188)
- Best practices: recovering your data (p. 189)

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.	Use the hypervisor client to connect to your host to find the gateway IP address. • For VMware ESXi, the VM's IP address can be found in the vSphere client on the **Summary** tab. • For Microsoft Hyper-V, the VM's IP address can be found by logging into the local console. If you are still having trouble finding the gateway IP address: • Check that the VM is turned on. Only when the VM is turned on does an IP address get assigned to your gateway. • 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.
You're having network or firewall problems.	• Allow the appropriate ports for your gateway. • 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 Network and firewall requirements (p. 8).

Issue	Action to Take
Your gateway's activation fails when you click the **Proceed to Activation** button in the Storage Gateway Management Console.	• Check that the gateway VM can be accessed by pinging the VM from your client. • 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 Testing your gateway's network connectivity (p. 103). • 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 Configuring a Network Time Protocol (NTP) server for your gateway (p. 105). • After performing these steps, you can retry the gateway deployment using the Storage Gateway console and the **Setup and Activate Gateway** wizard. • 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 File Gateway setup requirements (p. 6).
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 AWS Direct Connect 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 Performance (p. 131). 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.	• On the **Gateway** 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 Shutting down your gateway VM (p. 90). After the restart, the addresses in the **IP Addresses** list in the Storage Gateway console's **Gateway** tab should match the IP addresses for your gateway, which you determine from the hypervisor client.
	  • For VMware ESXi, the VM's IP address can be found in the vSphere client on the **Summary** tab.
	  • For Microsoft Hyper-V, the VM's IP address can be found by logging into the local console.
	• Check your gateway's connectivity to AWS as described in Testing your gateway's network connectivity (p. 103).
	• 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 Configuring network adapters for your gateway (p. 107) and select the option for viewing your gateway's network configuration.
	
	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 Performance (p. 131).

You are having trouble importing (deploying) Storage Gateway on Microsoft Hyper-V.	See Troubleshooting: Microsoft Hyper-V setup (p. 172), 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 Supportaccess 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. 116).
- Microsoft Hyper-V – for more information, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).

2. At the prompt, enter the corresponding numeral to select **Gateway Console**.
3. Enter **`h`** to open the list of available commands.
4. Do one of the following:

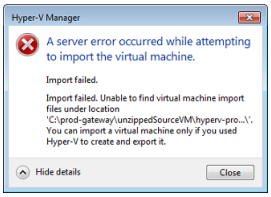
   - If your gateway is using a public endpoint, in the **AVAILABLE COMMANDS** window, enter **`open-support-channel`** to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support 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.

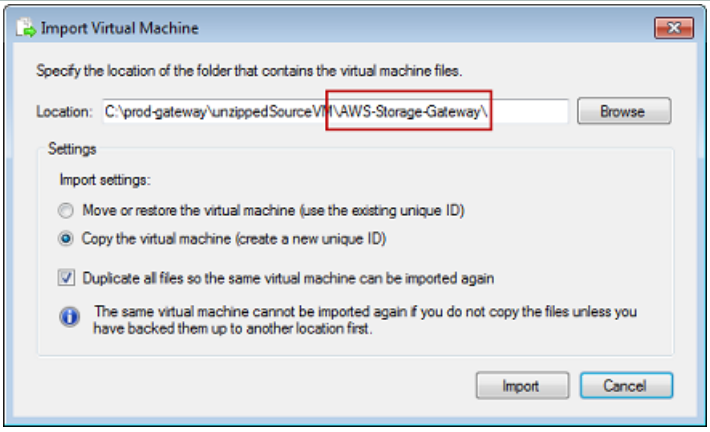
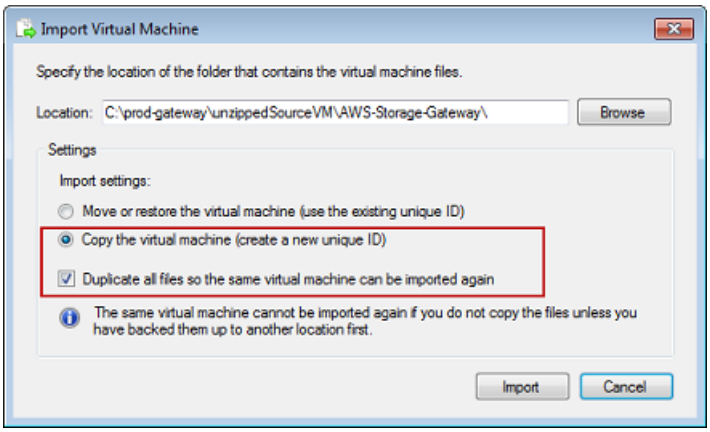
     Note
     The channel number is not a Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number. Instead, the gateway makes a Secure Shell (SSH) (TCP 22) connection to Storage Gateway servers and provides the support channel for the connection.

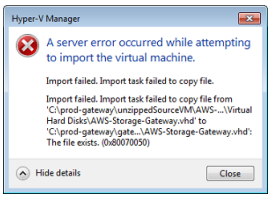
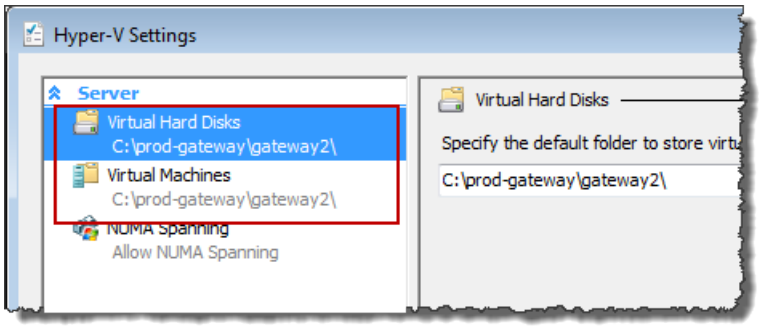
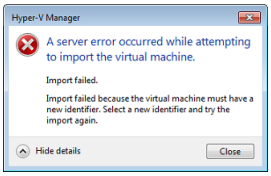
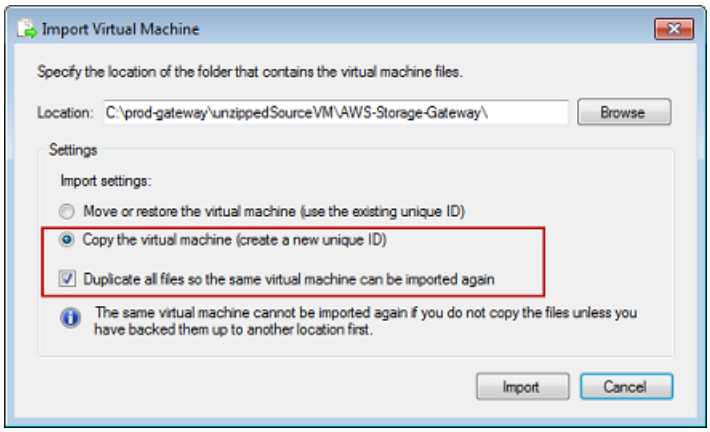
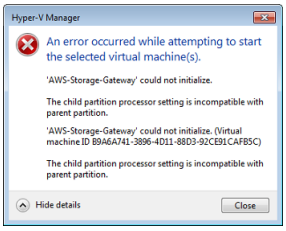
5. After the support channel is established, provide your support service number to AWS Support so AWS Support can provide troubleshooting assistance.
6. When the support session is completed, enter **`q`** to end it. Don't close the session until Amazon Web Services Support notifies you that the support session is complete.
7. Enter **`exit`** to log out of the Storage Gateway console.
8. Follow the prompts to exit the local console.

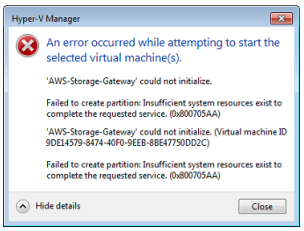
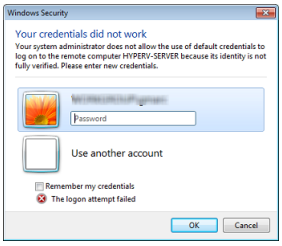
Troubleshooting: Microsoft Hyper-V setup

The following table lists typical issues that you might encounter when deploying Storage Gateway on the Microsoft Hyper-V platform.

Issue	Action to Take
You try to import a gateway and receive the error message: "Import failed. Unable to find virtual machine import file under location ...". 	This error can occur for the following reasons: • If you are not pointing to the root of the unzipped gateway source files. The last part of the location you specify in the **Import Virtual Machine** dialog box should be `AWS-Storage-Gateway`, as the following example shows:

Issue	Action to Take
	 • If you have already deployed a gateway and you did not select the **Copy the virtual machine** option and check the **Duplicate all files** option in the **Import Virtual Machine** 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. 

Issue	Action to Take
You try to import a gateway and receive the error message: "Import failed. Import task failed to copy file." 	If you have already deployed a gateway and you try to reuse the default folders that store the virtual hard disk files and virtual machine configuration files, then this error will occur. To fix this problem, specify new locations in the **Hyper-V Settings** dialog box. 
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." 	When you import the gateway make sure you select the **Copy the virtual machine** option and check the **Duplicate all files** option in the **Import Virtual Machine** dialog box to create a new unique ID for the VM. The following example shows the options in the **Import Virtual Machine** dialog box that you should use. 
You try to start a gateway VM and receive an error message "The child partition processor setting is incompatible with parent partition." 	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. For more information about the requirements for Storage Gateway, see File Gateway setup requirements (p. 6).

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." 	This error is likely caused by a RAM discrepancy between the required RAM for the gateway and the available RAM on the host. For more information about the requirements for Storage Gateway, see File Gateway setup requirements (p. 6).
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 Configuring a Network Time Protocol (NTP) server for your gateway (p. 105).
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 `hyperv-server`, then you can use the following UNC path `\\hyperv-server\c$`, which assumes that the name `hyperv-server` 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 Sconfig.cmd 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 File Gateway on an Amazon EC2 host (p. 196).

For information about using ephemeral storage, see Using ephemeral storage with EC2 gateways (p. 91).

Topics

- Your gateway activation hasn't occurred after a few moments (p. 176)
- You can't find your EC2 gateway instance in the instance list (p. 176)
- You want AWS Support to help troubleshoot your EC2 gateway (p. 176)

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. 8).

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 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 Amazon Web Services 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.

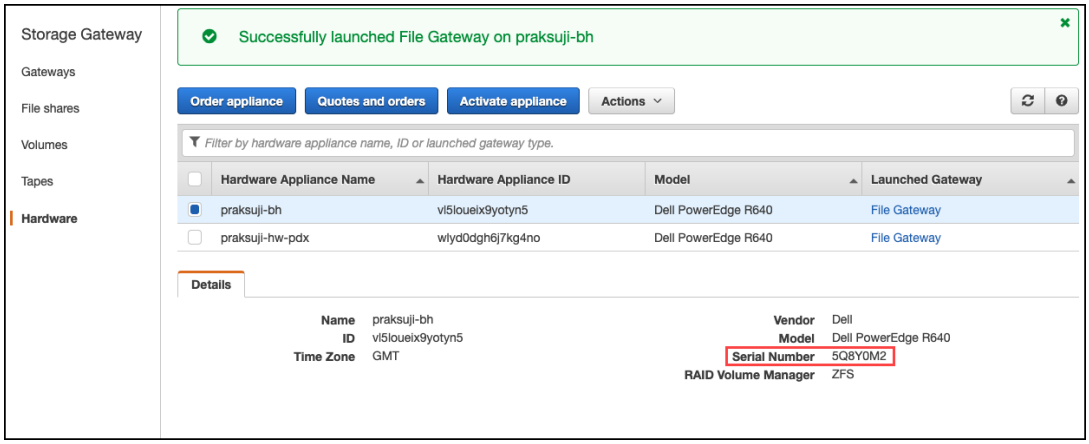
Where do you obtain Dell iDRAC support?

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.



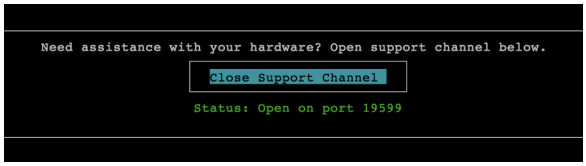
Where to obtain hardware appliance support

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. 179)
- Error: S3AccessDenied (p. 179)
- Error: InvalidObjectState (p. 180)
- Error: ObjectMissing (p. 180)
- Notification: Reboot (p. 180)
- Notification: HardReboot (p. 181)
- Notification: HealthCheckFailure (p. 181)
- Notification: AvailabilityMonitorTest (p. 181)
- Error: RoleTrustRelationshipInvalid (p. 181)
- Troubleshooting with CloudWatch metrics (p. 181)

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. 98), 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. 138) 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 AWS 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. 182)
- Your gateway isn't responding (p. 182)
- Your gateway is slow transferring data to Amazon S3 (p. 182)
- Your gateway is performing more Amazon S3 operations than expected (p. 183)

- You do not see files in your Amazon S3 bucket (p. 183)
- Your gateway backup job fails or there are errors when writing to your gateway (p. 183)

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 NVM Express (NVMe). If such disks aren't available, try using multiple cache disks from separate physical disks for a performance improvement.
- If `S3PutObjectRequestTime`, `S3UploadPartRequestTime`, or `S3GetObjectRequestTime` are high, there might be a network bottleneck. Try analyzing your network to verify that the gateway has the expected bandwidth.

Your gateway is performing more Amazon S3 operations than expected

If your File Gateway is performing more Amazon S3 operations than expected, check the `FilesRenamed` metric. Rename operations are expensive to execute in Amazon S3. Optimize your workflow to minimize the number of rename operations.

You do not see files in your Amazon S3 bucket

If you notice that files on the gateway are not reflected in the Amazon S3 bucket, check the `FilesFailingUpload` metric. If the metric reports that some files are failing upload, check your health notifications. When files fail to upload, the gateway generates a health notification containing more details on the issue.

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 FSx or 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 FSx or 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. 184)
- You can't create a file share (p. 184)
- SMB file shares don't allow multiple different access methods (p. 184)
- Multiple file shares can't write to the mapped S3 bucket (p. 184)
- Notification for deleted log group when using audit logs (p. 184)
- Can't upload files into your S3 bucket (p. 185)
- Can't change the default encryption to use SSE-KMS to encrypt objects stored in my S3 bucket (p. 185)
- Changes made directly in an S3 bucket with object versioning enabled may affect what you see in your file share (p. 185)
- When writing to an S3 bucket with object versioning enabled, the Amazon S3 File Gateway may create multiple versions of an S3 object (p. 186)
- Changes to an S3 bucket are not reflected in Storage Gateway (p. 187)

- ACL permissions aren't working as expected (p. 187)
- Your gateway performance declined after you performed a recursive operation (p. 187)

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. 53).

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. 184), 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 user cannot remain connected to two Guest Access SMB file shares, and may be disconnected when a new Guest Access connection is established.
3. 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. 71).

Notification for deleted log group when using audit logs

If the log group does not exist, the user could select the log group link below that message to go either create a new log group or use an existing log group to use as the target for audit logs

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 Amazon S3 File Gateway to upload files into your S3 bucket. For more information, see Granting access to an Amazon S3 bucket (p. 53).
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. 71).
3. If your file gateway uses SSE-KMS for encryption, make sure the IAM role associated with the file share includes *kms:Encrypt*, *kms:Decrypt*, *kms:ReEncrypt*, *kms:GenerateDataKey*, and *kms:DescribeKey* permissions. For more information, see Using Identity-Based Policies (IAM Policies) for Storage Gateway.

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 Amazon S3 File Gateway stores in the bucket are not encrypted with SSE-KMS. By default, a S3 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. 140).

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 S3 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. S3 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 S3 File Gateway creates a new version of a named object with your changes, and that version becomes the latest version.

Your S3 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. 67).

> **Important**
> We don't recommend that objects or files be written to your S3 File Gateway S3 bucket from outside of the file share.

When writing to an S3 bucket with object versioning enabled, the Amazon S3 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 Amazon S3 File Gateway by an NFS or SMB client after it has been uploaded to Amazon S3, the S3 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 S3 File Gateway by an NFS or SMB client, the S3 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 S3 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 S3 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 S3 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 S3 File Gateway recursively applies inheritance to all objects in the bucket. Such operations can cause your gateway performance to decline.

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. 188).

Troubleshooting: high availability issues

You can find information following about actions to take if you experience availability issues.

Topics

- Health notifications (p. 188)
- Metrics (p. 189)

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. 180)
- Notification: HardReboot (p. 181)
- Notification: HealthCheckFailure (p. 181)
- Notification: AvailabilityMonitorTest (p. 181)

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. 98), 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. 138) 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: 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. 189)
- Recovering your data from a malfunctioning cache disk (p. 190)
- Recovering your data from an inaccessible data center (p. 190)

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's network connectivity (p. 103).
- 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 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 Recovering your data from a malfunctioning cache disk (p. 190).

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 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. 196).
2. Create a new file share on the EC2 gateway you created. For more information, see Create a file share.
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 Mount and use your file share.

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. 191)
- Getting an Activation Key for Your Gateway (p. 198)
- Using AWS Direct Connect with Storage Gateway (p. 200)
- Port Requirements (p. 200)
- Connecting to Your Gateway (p. 205)
- Understanding Storage Gateway Resources and Resource IDs (p. 206)
- Tagging Storage Gateway resources (p. 207)
- Working with open-source components for AWS Storage Gateway (p. 208)
- Quotas (p. 209)
- Using storage classes (p. 210)
- Using Kubernetes Container Storage Interface (CSI) drivers (p. 213)

Host setup

Topics

- Configuring VMware for Storage Gateway (p. 191)
- Synchronizing Your Gateway VM Time (p. 195)
- Deploying a File Gateway on an Amazon EC2 host (p. 196)

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. 191)
- Using Storage Gateway with VMware High Availability (p. 194)

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.

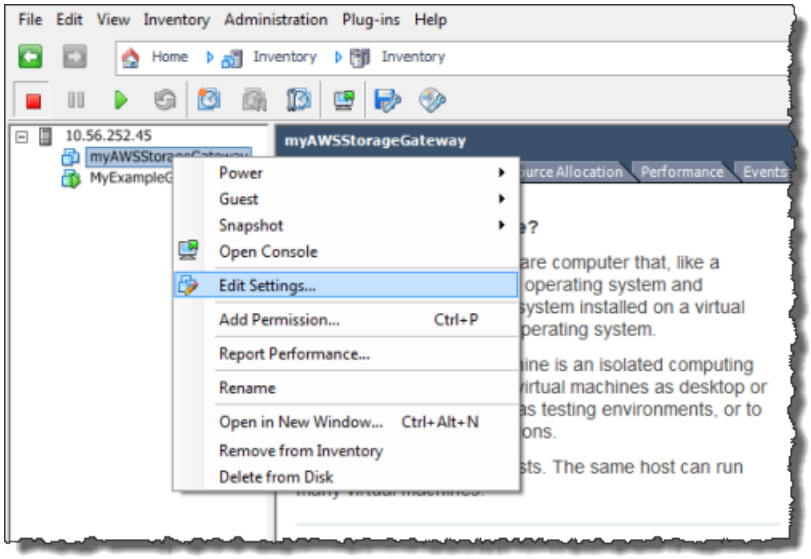
Important
Synchronizing the VM time with the host time is required for successful gateway activation.

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**.

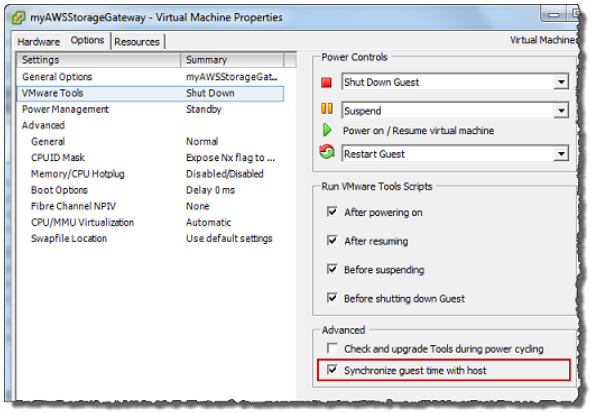
      The **Virtual Machine Properties** dialog box opens.



   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.



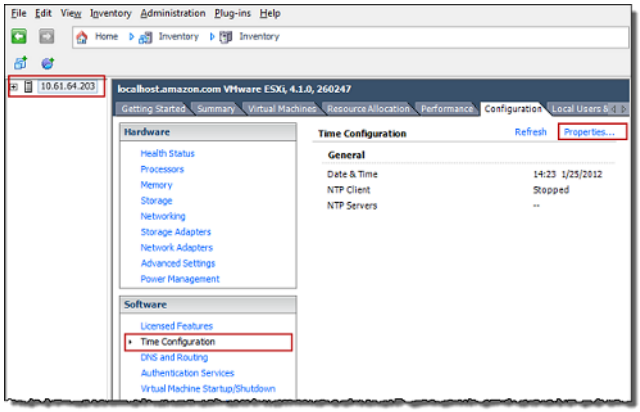
2. Configure the host time.

   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.

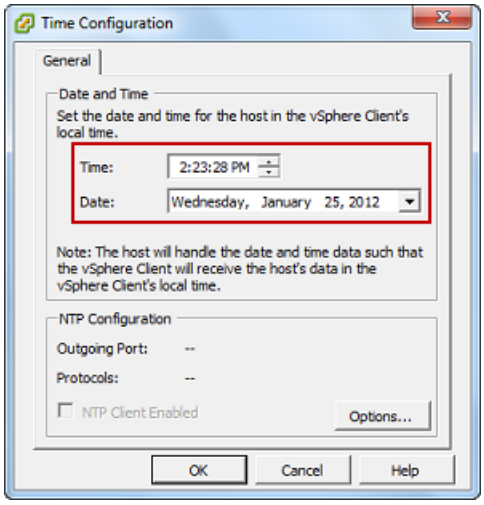
a. In the VMware vSphere client, select the vSphere host node in the left pane, and then choose the **Configuration** tab.

b. Select **Time Configuration** in the **Software** panel, and then choose the **Properties** link.

   The **Time Configuration** dialog box appears.

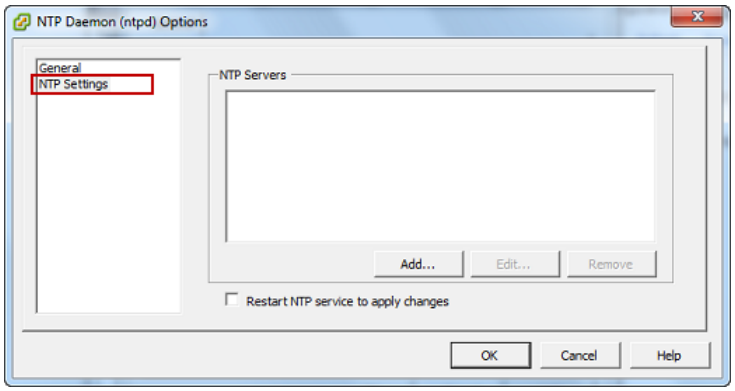


c. In the **Date and Time** panel, set the date and time.



d. Configure the host to synchronize its time automatically to an NTP server.

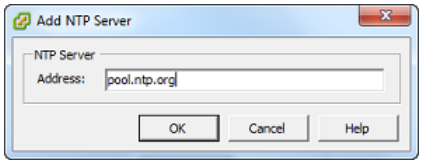
   i. Choose **Options** in the **Time Configuration** dialog box, and then in the **NTP Daemon (ntpd) Options** dialog box, choose **NTP Settings** in the left pane.



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**.

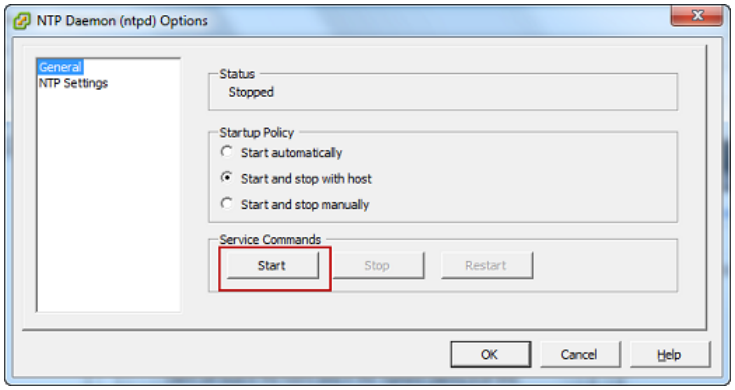
You can use `pool.ntp.org` as shown in the following example.



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.

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:

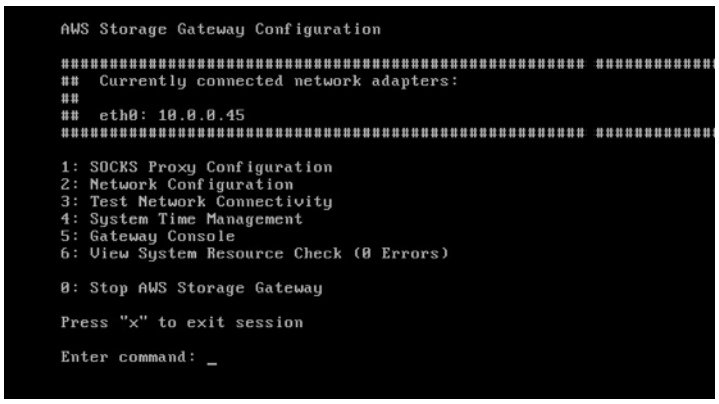
- Deploy the VMware ESX `.ova` downloadable package that contains the Storage Gateway VM on only one host in a cluster.
- When deploying the `.ova` package, select a data store that is not local to one host. Instead, use a data store that is accessible to all hosts in the cluster. If you select a data 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.
- 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

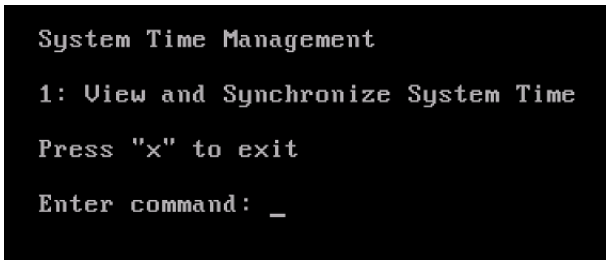
For a gateway deployed on VMware ESXi, setting the hypervisor host time and synchronizing the VM time to the host is sufficient to avoid time drift. For more information, see Synchronizing VM Time with Host Time (p. 191). For a gateway deployed on Microsoft Hyper-V, you should periodically check your 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. 116).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 117).
   - For more information on logging in to the local console for Linux Kernel-based Virtuam Machine (KVM), see Accessing the Gateway Local Console with Linux KVM (p. 114).
2. On the **Storage Gateway Configuration** main menu, enter **4** for **System Time Management**.



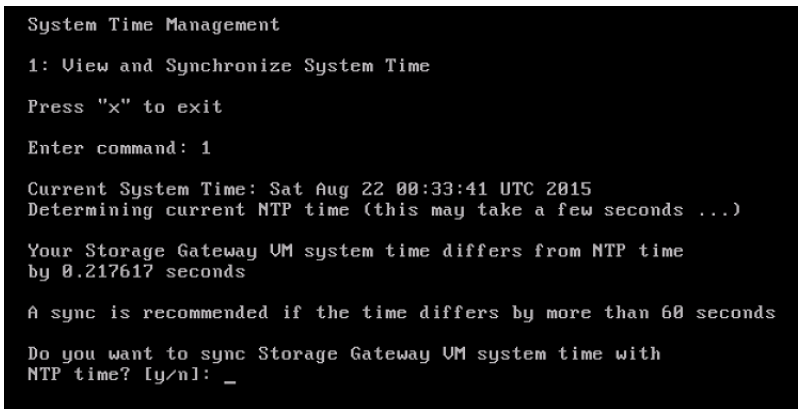
3. On the **System Time Management** menu, enter **1** for **View and Synchronize System Time**.



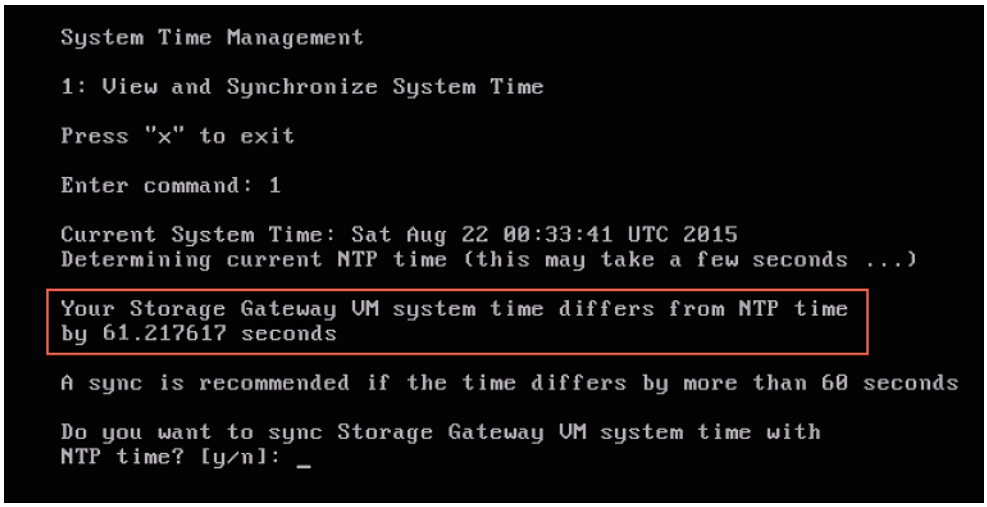
4. If the result indicates that you should synchronize your VM's time to the NTP time, enter **y**. Otherwise, enter **n**.

   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.



   The following screenshot shows a VM that does require time synchronization.



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. 7).

   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. 7).
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 Amazon EBS volume to configure for cache storage.

   Recommended disk sizes: Cache (Minimum) 150 GiB and Cache (Maximum) 64 TiB
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. 8).
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 AWS** page in 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 AWS Region you specify.

```
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"
    }
}
```

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. For more information, see ActivateGateway in the *Storage Gateway API Reference*.

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`*.

The URL returned by the redirect also includes the following query string parameters:

- `gatewayType` - The type of gateway that received the request
- `endpointType` - The type of endpoint the gateway uses to connect to AWS

- `vpcEndpoint` - The VPC Endpoint ID for gateways that connect using the VPC endpoint type

Topics

- AWS CLI (p. 199)
- Linux (bash/zsh) (p. 199)
- Microsoft Windows PowerShell (p. 199)

AWS CLI

If you haven't already done so, you must install and configure the AWS CLI. To do this, follow these instructions in the *AWS Command Line Interface User Guide:*

- Installing the AWS Command Line Interface
- Configuring the AWS Command Line Interface

The following example shows you how to use the AWS CLI to fetch the HTTP response, parse HTTP headers and get the activation key.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -oE 'activationKey=[A-Z0-9-]+' | \
pipe pipe pipe> cut -f2 -d=
```

Linux (bash/zsh)

The following example shows you how to use Linux (bash/zsh) to fetch the HTTP response, parse HTTP headers, and get the activation key.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

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]
    }
  }
}
```

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 AWS Direct Connect 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.*

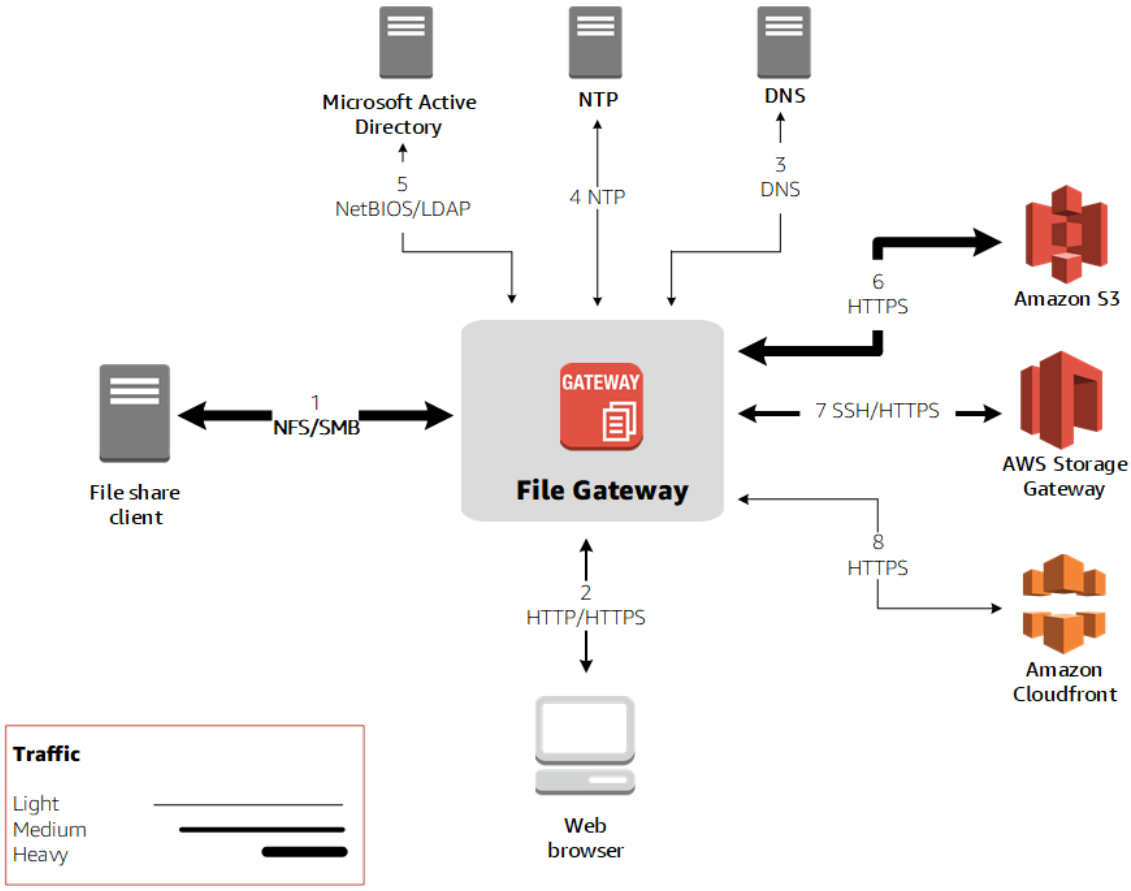
For details about AWS Direct Connect, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*.

Port Requirements

Storage Gateway requires the following ports for its operation. Some ports are common to all gateway types and are required by all gateway types. Other ports are required by specific gateway types. In this section, you can find an illustration of the required ports and a list of the ports required by each gateway type.

File Gateways

The following illustration shows the ports to open for file gateways' operation.



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

From	To	Protocol	Port	How Used	
Storage Gateway VM	Amazon Web Services	Transmission Control Protocol (TCP)	443 (HTTPS)	For communication from an Storage Gateway VM to an AWS service endpoint. For information about service endpoints, see Allowing AWS Storage Gateway access through firewalls and routers (p. 14).	
Your web browser	Storage Gateway VM	TCP	80 (HTTP)	By local systems to obtain the Storage	

From	To	Protocol	Port	How Used	
				Gateway activation key. Port 80 is used only during activation of a Storage Gateway appliance. 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 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.	

From	To	Protocol	Port	How Used	
Storage Gateway VM	Amazon Web Services	TCP	22 (Support channel)	Allows Amazon Web Services 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: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	
Storage Gateway Hardware Appliance	Hypertext Transfer Protocol (HTTP) proxy	TCP	8080 (HTTP)	Required briefly for activation.	

The following table lists the required ports that must be opened for a File Gateway using either the Network File System (NFS) or Server Message Block (SMB) protocol. These port rules are part of your security group definition.

Rul	Network Element	File Share Type	Protocol	Port	Inbou	Outbou	Require	Notes
1	File share client	NFS	TCP/UDP Data	111	✓	✓	✓	File sharing data transfer (for NFS only)
			TCP/UDP NFS	2049	✓	✓	✓	File sharing data transfer (for NFS only)

Rul	Network Element	File Share Type	Protocol	Port	Inbou	Outbou	Require	Notes
			TCP/UDP NFSv3	20048	✓	✓	✓	File sharing data transfer (for NFS only)
		SMB	TCP/UDP SMBv2	139	✓	✓	✓	File sharing data transfer session service (for SMB only); replaces ports 137–139 for Microsoft Windows NT and later
			TCP/UDP SMBv3	445	✓	✓	✓	File sharing data transfer session service (for SMB only); replaces ports 137–139 for Microsoft Windows NT and later
2	Web browser	NFS and SMB	TCP HTTP	80	✓	✓	✓	Amazon Web Services Management Console (activation only)
			TCP HTTPS	443	✓	✓	✓	Amazon Web Services Management Console (all other operations)
3	DNS	NFS and SMB	TCP/UDP DNS	53	✓	✓	✓	IP name resolution
4	NTP	NFS and SMB	UDP NTP	123	✓	✓	✓	Time synchronization service
5	Microsoft Active Directory	SMB	UDP NetBIOS	137	✓	✓	✓	Name service (not used for NFS)
			UDP NetBIOS	138	✓	✓	✓	Datagram service
			TCP LDAP	389	✓	✓		Directory System Agent (DSA); client connection
			TCP LDAPS	636	✓	✓		LDAPS—Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL)
6	Amazon S3	NFS and SMB	HTTPS data	443	✓	✓	✓	Storage data transfer

Rul	Network Element	File Share Type	Protocol	Port	Inbou	Outbou	Require	Notes
7	Storage Gateway	NFS and SMB	TCP SSH	22	✓	✓	✓	Support channel
			TCP HTTPS	443	✓	✓	✓	Management control
8	Amazon CloudFront	NFS and SMB	TCP HTTPS	443	✓	✓	✓	For activation

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. 116)
- HyperV host: Access the Gateway Local Console with Microsoft Hyper-V (p. 117)
- Linux Kernel-based Virtual Machine (KVM) host: Accessing the Gateway Local Console with Linux KVM (p. 114)
- EC2 host: Getting an IP Address from an Amazon EC2 Host (p. 205)

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 .

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:region:account-id:gateway/gateway-id`
File Share ARN	`arn:aws:storagegateway:region:account-id:share/share-id`
Volume ARN	`arn:aws:storagegateway:region:account-id:gateway/gateway-id/volume/volume-id`
Tape ARN	`arn:aws:storagegateway:region:account-id:tape/tapebarcode`
Target ARN (iSCSI target)	`arn:aws:storagegateway:region:account-id:gateway/gateway-id/target/iSCSItarget`
VTL Device ARN	`arn:aws:storagegateway:region:account-id:gateway/gateway-id/device/vtldevice`

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 a 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 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.

For File Gateway, you can use tags to control access to resources. For information about how to do this, see Using tags to control access to your gateway and resources (p. 152).

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 to 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**.

See also

Using tags to control access to your gateway and resources (p. 152)

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.

Topics

- Open-source components for Storage Gateway (p. 209)
- Open-source components for Amazon S3 File Gateway (p. 209)

Open-source components for Storage Gateway

Several third-party tools and licenses are used to deliver functionality for Volume Gateway, Tape Gateway, and Amazon S3 File Gateway.

Use the following links to download source code for certain open-source software components that are included with AWS Storage Gateway software:

- For gateways deployed on VMware ESXi: sources.tar
- For gateways deployed on Microsoft Hyper-V: sources_hyperv.tar
- For gateways deployed on Linux Kernel-based Virtual Machine (KVM): 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.

Open-source components for Amazon S3 File Gateway

Several third-party tools and licenses are used to deliver Amazon S3 File Gateway (S3 File Gateway) functionality.

Use the following links to download the source code for certain open-source software components that are included with S3 File Gateway software:

- For Amazon S3 File Gateway: sgw-file-s3-open-source.tgz

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.

Quotas

Quotas for file shares

The following table lists quotas for file shares.

Description	Limit
Maximum number of file shares per gateway **Note** Each file share can only connect to one S3 bucket, but multiple file shares can connect to the same bucket. If you connect more than one file share to the same bucket, you must configure each file share to use a unique, non-overlapping prefix name to prevent read/write conflicts.	10

Description	Limit
The maximum size of an individual file, which is the maximum size of an individual object in Amazon S3 **Note** If you write a file larger than 5 TB, you get a "file too large" error message and only the first 5 TB of the file is uploaded.	5 TB
Maximum path length **Note** Clients are not allowed to create a path exceeding this length, and doing so results in an error. This limit applies to both protocols supported by File Gateways, NFS and SMB.	1024 bytes

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)	Other Required Local Disks
S3 File Gateway	150 GiB	64 TiB	—

Note
You can configure one or more local drives for your cache up to the maximum capacity. When adding cache 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 a cache.

Using storage classes

Amazon S3 File Gateway supports the Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering, and S3 Glacier storage classes. For more information about storage classes, see Amazon S3 storage classes in the *Amazon Simple Storage Service User Guide*.

Note
S3 File Gateway does not currently support the Amazon S3 Glacier Instant Retrieval storage class.

Topics

- Using storage classes with a File Gateway (p. 211)
- Using the GLACIER storage class with File Gateway (p. 213)

Using storage classes with a File Gateway

When you create or update a file share, you have the option to select a storage class for your objects. You can choose the Amazon S3 Standard storage class, or any of the S3 Standard-IA, S3 One Zone-IA, or S3 Intelligent-Tiering storage classes. Objects stored in any of these storage classes can be transitioned to GLACIER using a lifecycle policy

Amazon S3 storage class	Considerations
Standard	Choose Standard to store your frequently accessed files redundantly in multiple Availability Zones that are geographically separated. This is the default storage class. See Amazon S3 pricing for more details.
S3 Intelligent-Tiering	Choose Intelligent-Tiering to optimize storage costs by automatically moving data to the most cost-effective storage access tier. Objects stored in the Intelligent-Tiering storage class can incur additional charges for overwriting, deleting, requesting, or transitioning objects between storage classes within 30 days. There is a minimum storage duration of 30 days, and objects deleted before 30 days incur a pro-rated charge equal to the storage charge for the remaining days. Consider how often these objects change, how long you plan to keep these objects, and how often you need to access them. Objects smaller than 128 KB are not eligible for auto tiering in the Intelligent-Tiering storage class. These objects are charged at the frequent access tier rates, and early deletion fees apply. S3 Intelligent-Tiering now supports an Archive Access tier and a Deep Archive Access tier. S3 Intelligent-Tiering automatically moves objects that haven't been accessed for 90 days to the Archive Access tier, and after 180 days without being accessed, to the Deep Archive Access tier. Whenever an object in one of the archive access tiers is restored, the object moves to the Frequent Access tier within a few hours and is ready to be retrieved. This creates timeout errors for users or applications trying to access files through a file share if the object only exists in one of the two archive tiers. Don't use the archive tiers with S3 Intelligent-Tiering if your applications are accessing files through the file shares that are presented by the File Gateway. When file operations that update metadata (such as owner, timestamp, permissions, and ACLs) are performed against files managed by the File Gateway, the existing object is deleted and a new version of the object is created in this Amazon S3 storage class. You should validate how file

Amazon S3 storage class	Considerations
	operations impact object creation before using this storage class in production because early deletion fees apply. See Amazon S3 pricing for more details.
S3 Standard-IA	Choose Standard-IA to store your infrequently accessed files redundantly in multiple Availability Zones that are geographically separated. Objects stored in the Standard-IA storage class can incur additional charges for overwriting, deleting, requesting, retrieving, or transitioning objects between storage classes within 30 days. There is a minimum storage duration of 30 days. Objects deleted before 30 days incur a pro-rated charge equal to the storage charge for the remaining days. Consider how often these objects change, how long you plan to keep these objects, and how often you need to access them. Objects smaller than 128 KB are charged for 128 KB and early deletion fees apply. When file operations that update metadata (such as owner, timestamp, permissions, and ACLs) are performed against files managed by the File Gateway, the existing object is deleted and a new version of the object is created in this Amazon S3 storage class. You should validate how file operations impact object creation before using this storage class in production because early deletion fees apply. See Amazon S3 pricing for more details.

Amazon S3 storage class	Considerations
S3 One Zone-IA	Choose One Zone-IA to store your infrequently accessed files in a single Availability Zone. Objects stored in the One Zone-IA storage class can incur additional charges for overwriting, deleting, requesting, retrieving, or transitioning objects between storage classes within 30 days. There is a minimum storage duration of 30 days, and objects deleted before 30 days incur a pro-rated charge equal to the storage charge for the remaining days. Consider how often these objects change, how long you plan to keep these objects, and how often you need to access them. Objects smaller than 128 KB are charged for 128 KB and early deletion fees apply. When file operations that update metadata (such as owner, timestamp, permissions, and ACLs) are performed against files managed by the File Gateway, the existing object is deleted and a new version of the object is created in this Amazon S3 storage class. You should validate how file operations impact object creation before using this storage class in production because early deletion fees apply. See Amazon S3 pricing for more details.

Although you can write objects directly from a file share to the S3-Standard-IA, S3-One Zone-IA, or S3 Intelligent-Tiering storage class, we recommend that you use a lifecycle policy to transition your objects rather than write directly from the file share, especially if you're expecting to update or delete the object within 30 days of archiving it. For information about lifecycle policy, see Object lifecycle management.

Using the GLACIER storage class with File Gateway

If you transition a file to S3 Glacier through Amazon S3 lifecycle policies, and the file is visible to your file share clients through the cache, you get I/O errors when you update the file. We recommend that you set up CloudWatch Events to receive notification when these I/O errors occur, and use the notification to take action. For example, you can take action to restore the archived object to Amazon S3. After the object is restored to S3, your file share clients can access and update them successfully through the file share.

For information about how to restore archived objects, see Restoring archived objects in the *Amazon Simple Storage Service User Guide*.

Using Kubernetes Container Storage Interface (CSI) drivers

Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. If you have a Kubernetes cluster, you can install and configure Kubernetes Container Storage Interface (CSI) drivers across the instances in your cluster to allow them to use an existing Amazon S3 File Gateway for storage.

After you install the CSI drivers for the type of file share that you want to use, you must create an object or objects. Depending on the type of provisioning that you want Kubernetes to use when your pods request storage, create either a single Kubernetes `StorageClass` object, or both a `PersistentVolume` object *and* a `PersistentVolumeClaim` object to connect your Kubernetes compute pods to your file share.. For more information, refer to the Kubernetes online documentation at https://kubernetes.io/docs/concepts/storage/.

Topics

- SMB CSI drivers (p. 214)
- NFS CSI drivers (p. 217)

SMB CSI drivers

Follow the procedures in this section to install and configure the CSI drivers that are required to use an SMB file share on an Amazon S3 File Gateway for storage in your Kubernetes cluster. For more information, see the open-source SMB CSI driver documentation on GitHub at https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md.

> **Note**
> When you create a `PersistentVolume` object or a `StorageClass` object, you can specify a `ReclaimPolicy` parameter to determine what happens to the external storage when objects are deleted. The SMB CSI driver supports the `Retain` and `Recycle` options, but does not currently support a `Delete` option.

Install drivers

To install Kubernetes SMB CSI drivers:

1. From a command-line terminal with access to `kubectl` for your Kubernetes cluster, run the following command:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. Wait for the previous command to finish, then use the following commands to ensure that the CSI driver pods are running:

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   The output should look similar to the following:

```
NAME                                     READY   STATUS    RESTARTS   AGE     IP
        NODE
csi-smb-controller-56bfddd689-dh5tk      4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4      4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                       3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                       3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

Create an SMB StorageClass object

To create a new SMB StorageClass object for your Kubernetes cluster:

1. Create a configuration file named `storageclass.yaml` with contents similar to the following example. Substitute your own deployment-specific information for the *`ExampleValues`* shown.

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. From a command-line terminal with access to `kubectl` and `storageclass.yaml`, run the following command:

   kubectl apply -f storageclass.yaml

   Note
   You can also create the StorageClass by providing the `.yaml` configuration text from the previous step to most third-party Kubernetes management and containerization platforms.

3. Configure the pods in your Kubernetes cluster to use the new StorageClass that you created. For more information, refer to the Kubernetes online documentation at https://kubernetes.io/docs/concepts/storage/.

Create SMB PersistentVolume and PersistentVolumeClaim objects

To create new SMB PersistentVolume and PersistentVolumeClaim objects:

1. Create two configuration files. One named `persistentvolume.yaml`, and one named `persistentvolumeclaim.yaml`.
2. For `persistentvolume.yaml`, add contents that are similar to the following example. Substitute your own deployment-specific information for the *`ExampleValues`* shown.

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
```

```
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim must
 use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. For `persistentvolumeclaim.yaml`, add contents that are similar to the following example. Substitute your own deployment-specific information for the *`ExampleValues`* shown.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim must
 use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. From a command-line terminal with access to `kubectl` and both of the `.yaml` files that you created, run the following commands:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   > You can also create the PersistentVolume and PersistentVolumeClaim objects by providing the `.yaml` configuration text from the previous step to most third-party Kubernetes management and containerization platforms.

5. Configure the pods in your Kubernetes cluster to use the new PersistentVolumeClaim that you created. For more information, refer to the Kubernetes online documentation at https://kubernetes.io/docs/concepts/storage/.

Uninstall drivers

To uninstall the Kubernetes SMB CSI drivers:

- From a command-line terminal with access to `kubectl` for your Kubernetes cluster, run the following command:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

NFS CSI drivers

Follow the procedures in this section to install and configure the CSI drivers that are required to use an NFS file share on an Amazon S3 File Gateway for storage in your Kubernetes cluster. For more information, see the open-source NFS CSI driver documentation on GitHub at https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md.

Install drivers

To install Kubernetes NFS CSI drivers:

1. From a command-line terminal with access to `kubectl` for your Kubernetes cluster, run the following command:

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --
2. Wait for the previous command to finish, then use the following commands to ensure that the CSI driver pods are running:

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   The output should look similar to the following:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
        NODE
csi-nfs-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19     k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35     k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35     k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                        3/3     Running   0          35s
 10.240.0.4      k8s-agentpool-22533604-0
```

Create an NFS StorageClass object

To create an NFS StorageClass object for your Kubernetes cluster:

1. Create a configuration file named `storageclass.yaml` with contents that are similar to the following example. Substitute your own deployment-specific information for the *`ExampleValues`* shown.

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. From a command-line terminal with access to `kubectl` and `storageclass.yaml`, run the following command:

   kubectl apply -f storageclass.yaml

   Note
   You can also create the StorageClass by providing the `.yaml` configuration text from the previous step to most third-party Kubernetes management and containerization platforms.

3. Configure the pods in your Kubernetes cluster to use the new StorageClass object that you created. For more information, refer to the Kubernetes online documentation at https://kubernetes.io/docs/concepts/storage/.

Create NFS PersistentVolume and PersistentVolumeClaim objects

To create new NFS PersistentVolume and PersistentVolumeClaim objects:

1. Create two configuration files named `persistentvolume.yaml` and `persistentvolumeclaim.yaml`.
2. For `persistentvolume.yaml`, add contents that are similar to the following example. Substitute your own deployment-specific information for the *ExampleValues* shown.

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
```

```
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. For `persistentvolumeclaim.yaml`, add contents that are similar to the following example. Substitute your own deployment-specific information for the *`ExampleValues`* shown.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name of
 the PersistentVolume you created
    storageClassName: ""
```

4. From a command-line terminal with access to `kubectl` and both `.yaml` files, run the following commands:

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   > You can also create the PersistentVolume and PersistentVolumeClaim objects by providing the `.yaml` configuration text from the previous step to most third-party Kubernetes management and containerization platforms.

5. Configure the pods in your Kubernetes cluster to use the new PersistentVolumeClaim object that you created. For more information, refer to the Kubernetes online documentation at https://kubernetes.io/docs/concepts/storage/.

Uninstall drivers

To uninstall Kubernetes NFS CSI drivers:

- From a command-line terminal with access to `kubectl` for your Kubernetes cluster, run the following command:

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

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 Storage Gateway. The AWS SDKs for Java, .NET, and PHP wrap the underlying Storage Gateway API, simplifying your programming tasks. For information about downloading the SDK libraries, see Sample Code Libraries.

Topics

- AWS Storage Gateway Required Request Headers (p. 220)
- Signing Requests (p. 222)
- Error Responses (p. 223)
- Actions

AWS Storage Gateway Required Request Headers

This section describes the required headers that you must send with every POST request to AWS 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 AWS 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 AWS 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
	`Authorization: AWS4-HMAC_SHA456 Credentials=YourAccessKey/yyyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature=CalculatedSignature` In the preceding syntax, you specify *YourAccessKey*, the year, month, and day (*yyyymmdd*), the *region*, and the *CalculatedSignature*. 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 Signing Requests (p. 222).
`Content-Type`	Use `application/x-amz-json-1.1` as the content type for all requests to AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`
`Host`	Use the host header to specify the AWS Storage Gateway endpoint where you send your request. For example, `storagegateway.us-east-2.amazonaws.com` is the endpoint for the US East (Ohio) region. For more information about the endpoints available for AWS Storage Gateway, see AWS Storage Gateway Endpoints and Quotas in the *AWS General Reference*. `Host: storagegateway.region.amazonaws.com`
`x-amz-date`	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 AWS Storage Gateway ignores any `Date` header during the request authentication. The `x-amz-date` format must be ISO8601 Basic in the YYYYMMDD'T'HHMMSS'Z' format. If both the `Date` and `x-amz-date` header are used, the format of the Date header does not have to be ISO8601. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	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. `x-amz-target: StorageGateway_APIversion.operationName` The *operationName* value (e.g. "ActivateGateway") can be found from the API list, API Reference for Storage Gateway (p. 220).

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. 222) is:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

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. 222) is:

```
AWS4-HMAC-SHA256
20120910T000000Z
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. 222), the *derived key* can be represented as:

```
derived key = HMAC(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. 224)

- Operation Error Codes (p. 225)
- Error Responses (p. 237)

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. 237).

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. 225) message codes that give the specific operation error code.

Exception	Message	HTTP Status Code
`IncompleteSignatureException`	The specified signature is incomplete.	400 Bad Request
`InternalFailure`	The request processing has failed due to some unknown error, exception or failure.	500 Internal Server Error
`InternalServerError`	One of the operation error code messages Operation Error Codes (p. 225).	500 Internal Server Error
`InvalidAction`	The requested action or operation is invalid.	400 Bad Request
`InvalidClientTokenId`	The X.509 certificate or AWS Access Key ID provided does not exist in our records.	403 Forbidden
`InvalidGatewayRequestException`	One of the operation error code messages in Operation Error Codes (p. 225).	400 Bad Request
`InvalidSignatureException`	The request signature we calculated does not match the signature you provided. Check your AWS Access Key and signing method.	400 Bad Request
`MissingAction`	The request is missing an action or operation parameter.	400 Bad Request
`MissingAuthenticationToken`	The request must contain either a valid (registered) AWS Access Key ID or X.509 certificate.	403 Forbidden
`RequestExpired`	The request is past the expiration date or the request date (either with 15 minute padding), or the request date	400 Bad Request

Exception	Message	HTTP Status Code
	occurs more than 15 minutes in the future.	
`SerializationException`	An error occurred during serialization. Check that your JSON payload is well-formed.	400 Bad Request
`ServiceUnavailable`	The request has failed due to a temporary failure of the server.	503 Service Unavailable
`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 Operations in Storage Gateway (p. 239).	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. 224).

Operation Error Code	Message	Operations That Return this Error Code
`ActivationKeyExpired`	The specified activation key has expired.	ActivateGateway
`ActivationKeyInvalid`	The specified activation key is invalid.	ActivateGateway
`ActivationKeyNotFound`	The specified activation key was not found.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	The specified bandwidth throttle was not found.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	The specified snapshot cannot be exported.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	The specified initiator was not found.	DeleteChapCredentials
`DiskAlreadyAllocated`	The specified disk is already allocated.	AddCache AddUploadBuffer

Operation Error Code	Message	Operations That Return this Error Code
		AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	The specified disk does not exist.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	The specified disk is not gigabyte-aligned.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	The specified disk size is greater than the maximum volume size.	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	The specified disk size is less than the volume size.	CreateStorediSCSIVolume
DuplicateCertificateInfo	The specified certificate information is a duplicate.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	Existing File System Association endpoint configuration conflicts with specified configuration.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	The specified endpoint IP address is already in use.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	File System Association Endpoint IP address is missing.	AssociateFileSystem
FileSystemAssociationNotFound	The specified file system association was not found.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	The specified file system was not found.	AssociateFileSystem

Operation Error Code	Message	Operations That Return this Error Code
`GatewayInternalError`	A gateway internal error occurred.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operation Error Code	Message	Operations That Return this Error Code
`GatewayNotConnected`	The specified gateway is not connected.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operation Error Code	Message	Operations That Return this Error Code
`GatewayNotFound`	The specified gateway was not found.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow

Operation Error Code	Message	Operations That Return this Error Code
		UpdateSnapshotSchedule
GatewayProxyNetworkConnectionBusy	The specified gateway proxy network connection is busy.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operation Error Code	Message	Operations That Return this Error Code
`InternalError`	An internal error occurred.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime

Operation Error Code	Message	Operations That Return this Error Code
		UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Operation Error Code	Message	Operations That Return this Error Code
`InvalidParameters`	The specified request contains invalid parameters.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime

Operation Error Code	Message	Operations That Return this Error Code
		UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	The local storage limit was exceeded.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	The specified LUN is invalid.	CreateStorediSCSIVolume
`MaximumVolumeCountExceeded`	The maximum volume count was exceeded.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	The gateway network configuration has changed.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Operation Error Code	Message	Operations That Return this Error Code
`NotSupported`	The specified operation is not supported.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime

Operation Error Code	Message	Operations That Return this Error Code
		UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	The specified gateway is out of date.	ActivateGateway
`SnapshotInProgressException`	The specified snapshot is in progress.	DeleteVolume
`SnapshotIdInvalid`	The specified snapshot is invalid.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`StagingAreaFull`	The staging area is full.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	The specified target already exists.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	The specified target is invalid.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	The specified target was not found.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Operation Error Code	Message	Operations That Return this Error Code
`UnsupportedOperationForGatewayType`	The specified operation is not valid for the type of the gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	The specified volume already exists.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	The specified volume is invalid.	DeleteVolume
`VolumeInUse`	The specified volume is already in use.	DeleteVolume
`VolumeNotFound`	The specified volume was not found.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	The specified volume is not ready.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

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. 224).

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 Storage Gateway

- **API version**: 2013-06-30
- **Latest documentation update**: October 12, 2021

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
Updated gateway creation procedures (p. 240)	The procedure for creating a new gateway has been updated to reflect changes in the Storage Gateway console. For more information, see Create and activate an Amazon S3 File Gateway.	October 12, 2021
Support for force-closing files on SMB file shares (p. 240)	You can now use Local Group settings to assign Gateway Admin permissions. Gateway Admins can use the Shared Folders Microsoft Management Console snap-in to force-close files that are open and locked on SMB file shares. For more information, see Configure Local Groups for your gateway.	October 12, 2021
Audit log support for NFS file shares (p. 240)	You can now configure NFS file shares to generate audit logs that provide details about user access to files and folders within a file share. You can use these logs to monitor user activities and take action if inappropriate activity patterns are identified. For more information, see Understanding File Gateway audit logs.	October 12, 2021
Access point alias support (p. 240)	File Gateway file shares can now connect to Amazon S3 storage using bucket-style access point aliases. For more information, see Create a file share.	October 12, 2021
VPC endpoint and access point support (p. 240)	File Gateway file shares can now connect to S3 buckets through access points or interface endpoints in your VPC powered	July 7, 2021

	by AWS PrivateLink. For more information, see Create a file share.	
Opportunistic locking support (p. 240)	File Gateway file shares can now use opportunistic locking to optimize their file buffering strategy, which improves performance in most cases, particularly with regard to Windows context menus. For more information, see Create an SMB file share.	July 7, 2021
FedRAMP compliance (p. 240)	Storage Gateway is now FedRAMP compliant. For more information, see Compliance validation for Storage Gateway.	November 24, 2020
Schedule-based bandwidth throttling (p. 240)	Storage Gateway now supports schedule-based bandwidth throttling for tape and Volume Gateways. For more information, see Scheduling bandwidth throttling using the Storage Gateway console.	November 9, 2020
File upload notification for File Gateway (p. 240)	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 Getting file upload notification.	November 9, 2020
Access-based enumeration for File Gateway (p. 240)	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 Creating an SMB file share.	November 9, 2020
File Gateway migration (p. 240)	File Gateway now provides a documented process for replacing an existing File Gateway with a new File Gateway. For more information, see Replacing a File Gateway with a new File Gateway.	October 30, 2020
File Gateway cold cache read performance 4x increase (p. 240)	Storage Gateway has increased cold cache read performance 4x. For more information, see Performance guidance for File Gateways.	August 31, 2020

Order the hardware appliance through the console (p. 240)	You can now order the hardware appliance through the AWS Storage Gateway console. For more information, see Using the Storage Gateway Hardware Appliance.	August 12, 2020
Support for Federal Information Processing Standard (FIPS) endpoints in new AWS Regions (p. 240)	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 AWS Storage Gateway endpoints and quotas in the *AWS General Reference*.	July 31, 2020
Support for multiple file shares attached to a single Amazon S3 bucket (p. 240)	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 Creating an NFS file share or Creating an SMB file share.	July 7, 2020
File Gateway local cache storage 4x increase (p. 240)	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 Recommended local disk sizes for your gateway in the *Storage Gateway User Guide*.	July 7, 2020
View Amazon CloudWatch alarms in the Storage Gateway console (p. 240)	You can now view CloudWatch alarms in the Storage Gateway console. For more information, see Understanding CloudWatch alarms.	May 29, 2020

Support for Federal Information Processing Standard (FIPS) endpoints (p. 240)	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 Choosing a service endpoint. To choose a FIPS endpoint for a Volume Gateway, see Choosing a service endpoint. To choose a FIPS endpoint for a Tape Gateway, see Choosing a service endpoint.	May 22, 2020
New AWS Regions (p. 240)	Storage Gateway is now available in the Africa (Cape Town) and Europe (Milan) Regions. For more information, see AWS Storage Gateway endpoints and quotas in the *AWS General Reference*.	May 7, 2020
Support for S3 Intelligent-Tiering storage class (p. 240)	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 Storage class for automatically optimizing frequently and infrequently accessed objects in the *Amazon Simple Storage Service User Guide*.	April 30, 2020
New AWS Region (p. 240)	Storage Gateway is now available in the AWS GovCloud (US-East) Region. For more information, see AWS Storage Gateway Endpoints and Quotas in the *AWS General Reference*.	March 12, 2020
Support for Linux Kernel-based Virtual Machine (KVM) hypervisor (p. 240)	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 Supported Hypervisors and Host Requirements in the *Storage Gateway User Guide*.	February 4, 2020

Support for VMware vSphere High Availability (p. 240)	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 Using VMware vSphere High Availability with Storage Gateway in the *Storage Gateway User Guide*. This release also includes performance improvements. For more information, see Performance in the *Storage Gateway User Guide*.	November 20, 2019
New AWS Region for Tape Gateway (p. 240)	Tape Gateway is now available in the South America (São Paulo) Region. For more information, see AWS Storage Gateway Endpoints and Quotas in the *AWS General Reference*.	September 24, 2019
Support for Amazon CloudWatch Logs (p. 240)	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 Getting Notified About Gateway Health and Errors With Amazon CloudWatch Log Groups in the *Storage Gateway User Guide.*	September 4, 2019
New AWS Region (p. 240)	Storage Gateway is now available in the Asia Pacific (Hong Kong) Region. For more information, see AWS Storage Gateway Endpoints and Quotas in the *AWS General Reference*.	August 14, 2019
New AWS Region (p. 240)	Storage Gateway is now available in the Middle East (Bahrain) Region. For more information, see AWS Storage Gateway Endpoints and Quotas in the *AWS General Reference*.	July 29, 2019
Support for activating a gateway in a virtual private cloud (VPC) (p. 240)	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 Activating a Gateway in a Virtual Private Cloud.	June 20, 2019

SMB file share support for Microsoft Windows ACLs (p. 240)	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 Using Microsoft Windows ACLs to Control Access to an SMB File Share.	May 8, 2019
File Gateway support for tag-based authorization (p. 240)	File Gateway now supports tag-based authorization. You can control access to File Gateway resources based on the tags on those resources. You can also control access based on the tags that can be passed in an IAM request condition. For more information, see Controlling Access to File Gateway Resources.	March 4, 2019
Availability of Storage Gateway Hardware Appliance in Europe (p. 240)	The Storage Gateway Hardware Appliance is now available in Europe. For more information, see AWS Storage Gateway Hardware Appliance Regions in the *AWS General Reference*. 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 Setting Up Your Hardware Appliance.	February 25, 2019
Support for Storage Gateway Hardware Appliance (p. 240)	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 Using the Storage Gateway Hardware Appliance.	September 18, 2018
Support for Server Message Block (SMB) protocol (p. 240)	File Gateways added support for the Server Message Block (SMB) protocol to file shares. For more information, see Creating a File Share.	June 20, 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 Create a file share (p. 35).	April 4, 2018
New AWS Region	Tape Gateway is now available in the Asia Pacific (Singapore) Region. For detailed information, see Supported AWS Regions (p. 17).	April 3, 2018
Support for refresh cache notification, Requester Pays, and canned ACLs for Amazon S3 buckets	With File Gateways, you can now be notified when the gateway finishes refreshing the cache for your Amazon S3 bucket. For more information, see RefreshCache.html in the *Storage Gateway API Reference*. For File Gateways, you can now specify that the requester or reader pays for access charges instead of the bucket owner. With File Gateways, you can now enable give full control to the owner of the S3 bucket that maps to the NFS file share. For more information, see Create a file share (p. 35).	March 1, 2018
New AWS Region	Storage Gateway is now available in the Europe (Paris) Region. For detailed information, see Supported AWS Regions (p. 17).	December 18, 2017
Support for file upload notification and guessing of the MIME type	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 NotifyWhenUploaded in the *Storage Gateway API Reference*. File Gateways now enable guessing of the MIME type for uploaded objects based on file extensions. For more information, see Create a file share (p. 35).	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 Supported hypervisors and host requirements (p. 16).	September 13, 2017
File Gateway support for Microsoft Hyper-V hypervisor	You can now deploy a File Gateway on a Microsoft Hyper-V hypervisor. For information, see Supported hypervisors and host requirements (p. 16).	June 22, 2017

Change	Description	Date Changed
New AWS Region	Storage Gateway is now available in the Asia Pacific (Mumbai) Region. For detailed information, see Supported AWS Regions (p. 17).	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 Create a file share (p. 35). 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 RefreshCache in the API Reference.	March 28, 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 Create and activate an Amazon S3 File Gateway (p. 30). For information about how to launch a File Gateway AMI, see Deploying a File Gateway on an Amazon EC2 host (p. 196). In addition, file gateway now supports HTTP proxy configuration. For more information, see Routing your gateway deployed on EC2 through an HTTP proxy (p. 110).	February 08, 2017
New AWS Region	Storage Gateway is now available in the Europe (London) Region. For detailed information, see Supported AWS Regions (p. 17).	December 13, 2016
New AWS Region	Storage Gateway is now available in the Canada (Central) Region. For detailed information, see Supported AWS Regions (p. 17).	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