AWS Storage Gateway

User Guide

API Version 2021-03-31

AWS Storage Gateway: User Guide

Table of Contents

What is Amazon FSx File Gateway?

Storage Gateway offers file gateway, volume gateway, and tape gateway storage solutions.

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

Benefits of using Amazon FSx File Gateway

FSx File provides the following benefits:

- Helps eliminate on-premises file servers and consolidates all their data in AWS to take advantage of the scale and economics of cloud storage.
- Provides options that you can use for all your file workloads, including those that require on-premises access to cloud data.
- Applications that need to stay on premises can now experience the same low latency and high performance that they have in AWS, without taxing your networks or impacting the latencies experienced by your most demanding applications.

How Amazon FSx File Gateway works

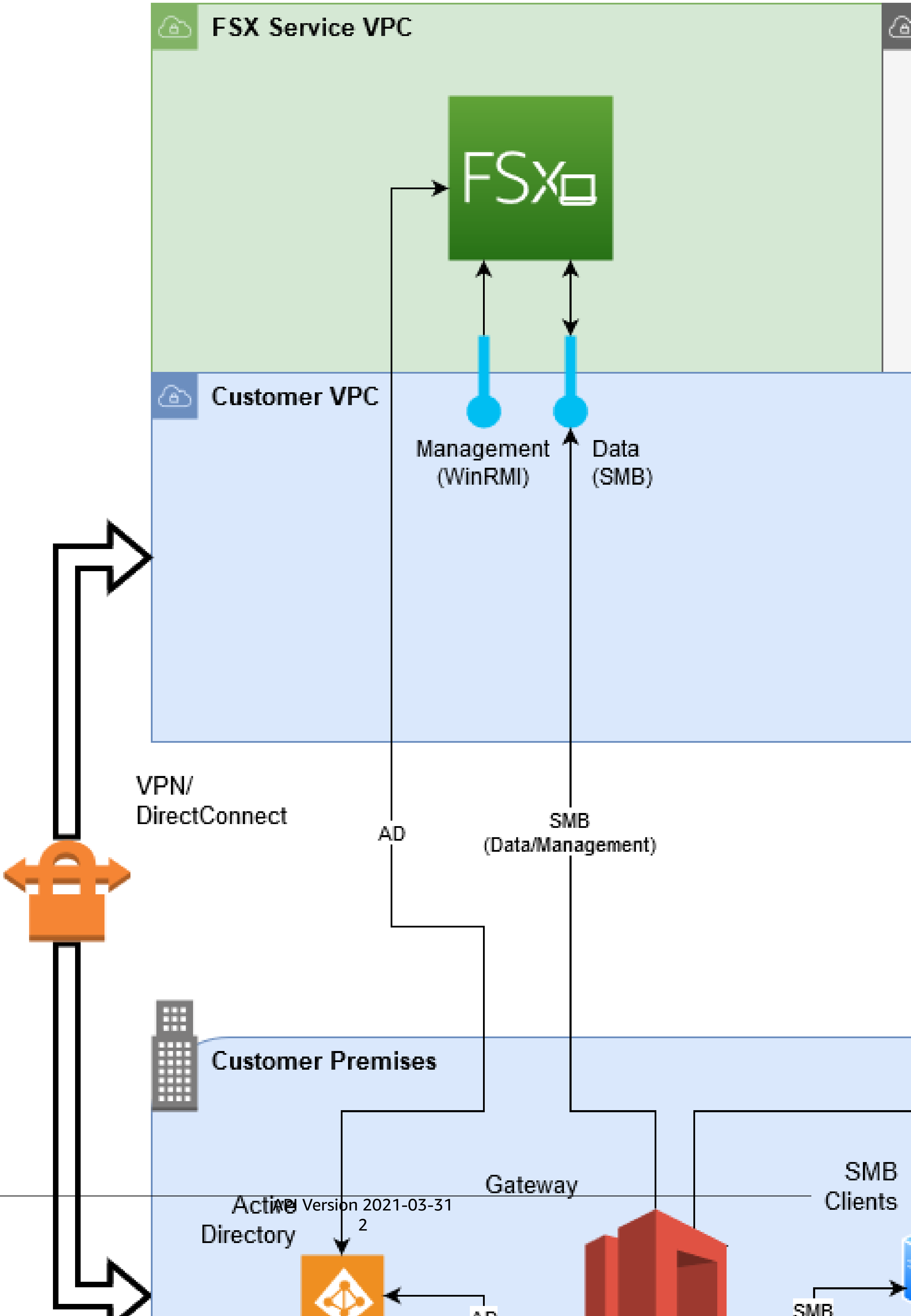
To use Amazon FSx File Gateway (FSx File), you must have at least one Amazon FSx for Windows File Server file system. You must also have on-premises access to FSx for Windows File Server, either through a VPN or through an AWS Direct Connect connection. For more information about using Amazon FSx file systems, see What is Amazon FSx for Windows File Server?

You download and deploy the FSx File VMware virtual appliance or an AWS Storage Gateway Hardware Appliance into your on-premises environment. After deploying your appliance, you activate the FSx File from the Storage Gateway console or through the Storage Gateway API. You can also create an FSx File using an Amazon Elastic Compute Cloud (Amazon EC2) image.

After the Amazon FSx File Gateway is activated and can access FSx for Windows File Server, use the Storage Gateway console to join it to your Microsoft Active Directory domain. After the gateway successfully joins a domain, you use the Storage Gateway console to attach the gateway to an existing FSx for Windows File Server. FSx for Windows File Server makes all the shares on the server available as shares on your Amazon FSx File Gateway. You can then use a client to browse and connect to the file shares on FSx File that correspond to the selected FSx File.

When the file shares are connected, you can read and write your files locally, while benefiting from all the features available on FSx for Windows File Server. FSx File maps local file shares and their contents to file shares stored remotely in FSx for Windows File Server. There is a 1:1 correspondence between the remote and locally visible files and their shares.

The following diagram provides an overview of file storage deployment for Storage Gateway.


FSX Service VPC
FSx
Customer VPC
Management
(WinRMI)
Data
(SMB)
VPN/
DirectConnect
AD
SMB
(Data/Management)
Customer Premises
Gateway
SMB
Clients
Active
Directory
AD
SMB

Note the following in the diagram:

- **AWS Direct Connect or a VPN** is needed to allow the FSx File to access the Amazon FSx file share using SMB and to allow the FSx for Windows File Server to join your on-premises Active Directory domain.
- **Amazon Virtual Private Cloud (Amazon VPC)** is needed to connect to the FSx for Windows File Server service VPC and the Storage Gateway service VPC using private endpoints. The FSx File can also connect to the public endpoints.

You can use Amazon FSx File Gateway in all AWS Regions where FSx for Windows File Server is available.

Setting up for Amazon FSx File Gateway

This section provides instructions for getting started with Amazon FSx 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

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 user**.
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 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

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

- Create and configure an FSx for Windows File Server file system. For instructions, see Step 1: Create Your File System in the *FSx for Windows File Server User Guide*.
- 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 FSx File.

- 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.

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

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*.

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.

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 FSx File 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

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 Storage Gateway access through firewalls and routers (p. 12).
TCP	80 (HTTP)	Inbound	The host from which you connect to the AWS	Storage Gateway	By local systems to obtain the storage gateway

Protocol	Port	Direction	Source	Destination	How used
			Management Console.		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 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.

Protocol	Port	Direction	Source	Destination	How used
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

For FSx File, you must use Microsoft Active Directory 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*.

FSx File requires the following ports.

Protocol	Port	Direction	Source	Destination	How used
UDP NetBIOS	137	Inbound and outbound		Microsoft Active Directory	For connecting to Microsoft Active Directory.
UDP NetBIOS	138	Inbound and outbound			For Datagram service
TCP LDAP	389	Inbound and outbound			For Directory System Agent (DSA) client connection
TCP v2/v3 data	445	Outbound			Storage data transfer between file gateway

Protocol	Port	Direction	Source	Destination	How used
					and FSx for Windows File Server
TCP (HTTPS)	443	Outbound		Storage Gateway service endpoints	Management control – Used for communication from an Storage Gateway VM to an AWS service endpoint
TCP HTTPS	443	Outbound		Amazon CloudFront	For gateway activation
TCP	443	Outbound		VPC endpoint usage	Management control – Used for communication from an Storage Gateway VM to an AWS service endpoint.
TCP	1026	Outbound			Used for control traffic
TCP	1027	Outbound			Used only during activation and can then be closed
TCP	1028	Outbound			Used for control traffic
TCP	1031	Outbound			Used only for software updates for file gateways
TCP	2222	Outbound			Used to open a support channel to the gateway when using VPC endpoints
TCP (HTTPS)	8080	Inbound			Required briefly for activation of a hardware appliance

Networking and firewall requirements for the Storage Gateway Hardware Appliance

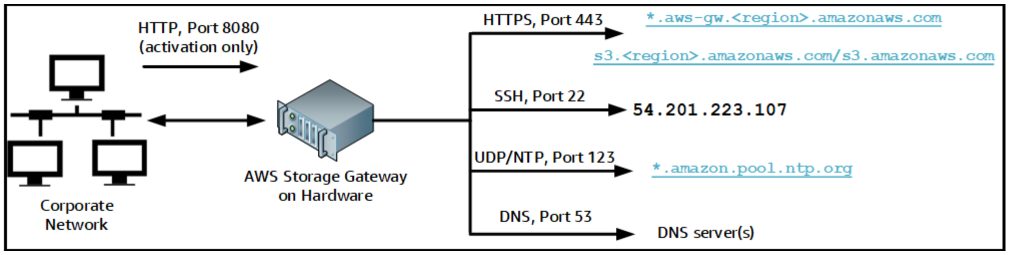
Each Storage Gateway Hardware Appliance requires the following network services:

- **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.

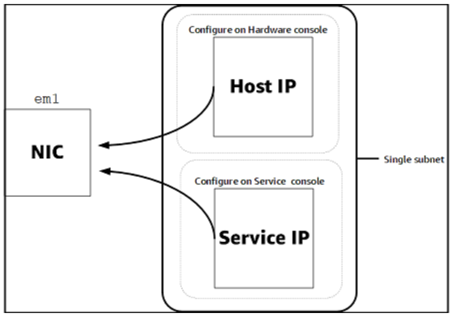
Protocol	Port	Direction	Source	Destination	How used
SSH	22	Outbound	Hardware appliance	`54.201.223.107`	Support channel
DNS	53	Outbound	Hardware appliance	DNS servers	Name resolution
UDP/NTP	123	Outbound	Hardware appliance	`*.amazon.pool.ntp.org`	Time synchronization
HTTPS	443	Outbound	Hardware appliance	`*.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. 21).

> **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. 18).

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. 16).

Allowing 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 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 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 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 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 port 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. 142).

Supported hypervisors and host requirements

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

Storage Gateway supports the following hypervisor versions and hosts:

- VMware ESXi Hypervisor (version 6.0, 6.5 or 6.7) – A free version of VMware is available on the VMware website. For this setup, you also need a VMware vSphere client to connect to the host.
- Microsoft Hyper-V Hypervisor (version 2012 R2 or 2016) – A free, standalone version of Hyper-V is available at the Microsoft Download Center. For this setup, you need a Microsoft Hyper-V Manager on a Microsoft Windows client computer to connect to the host.
- Linux Kernel-based Virtual Machine (KVM) – A free, open-source virtualization technology. KVM is included in all versions of Linux version 2.6.20 and newer. Storage Gateway is tested and supported for

the CentOS/RHEL 7.7, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS distributions. Any other modern Linux distribution may work, but function or performance is not guaranteed. We recommend this option if you already have a KVM environment up and running and you are already familiar with how KVM works.

- Amazon EC2 instance – Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image. For information about how to deploy a gateway on Amazon EC2, see Deploying a file gateway on an Amazon EC2 host (p. 157).
- 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. 150).
> Storage Gateway doesn't support dynamic memory and virtual memory ballooning.

Supported SMB clients for a file gateway

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

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

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

Supported file system operations for a file gateway

Your SMB client can write, read, delete, and truncate files. When clients send writes to Storage Gateway, it writes to local cache synchronously. Then it writes to Amazon FSx asynchronously through optimized transfers. Reads are first served through the local cache. If data is not available, it's fetched through Amazon FSx 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 files from Amazon FSx.

Accessing Storage Gateway

You can use the 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 Storage Gateway API to programmatically configure and manage your gateways. For more information about the API, see API Reference for Storage Gateway (p. 166).

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 Storage Gateway pricing.

Supported AWS Regions

Amazon FSx File Gateway stores file data in the AWS Region where your Amazon FSx file system is located. Before you start deploying your gateway, choose a Region in the upper-right corner of the Storage Gateway console.

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

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

To order a hardware appliance

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

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

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

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

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

Topics

- Launching a gateway (p. 27)
- Configuring an IP address for the gateway (p. 27)
- Configuring your gateway (p. 28)
- Removing a gateway from the hardware appliance (p. 29)
- Deleting your hardware appliance (p. 29)

Supported AWS Regions

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

Setting up your hardware appliance

After you receive your Storage Gateway Hardware Appliance, you use the hardware appliance console to configure networking to provide an always-on connection to AWS and activate your appliance. Activation associates your appliance with the 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. 18).
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. 21).
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. 23).
4. Install the Storage Gateway on your hardware appliance. For more information, see Configuring your gateway (p. 28).

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

Increasing the usable cache storage

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

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

1. Reset the hardware appliance to its factory settings. Contact 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

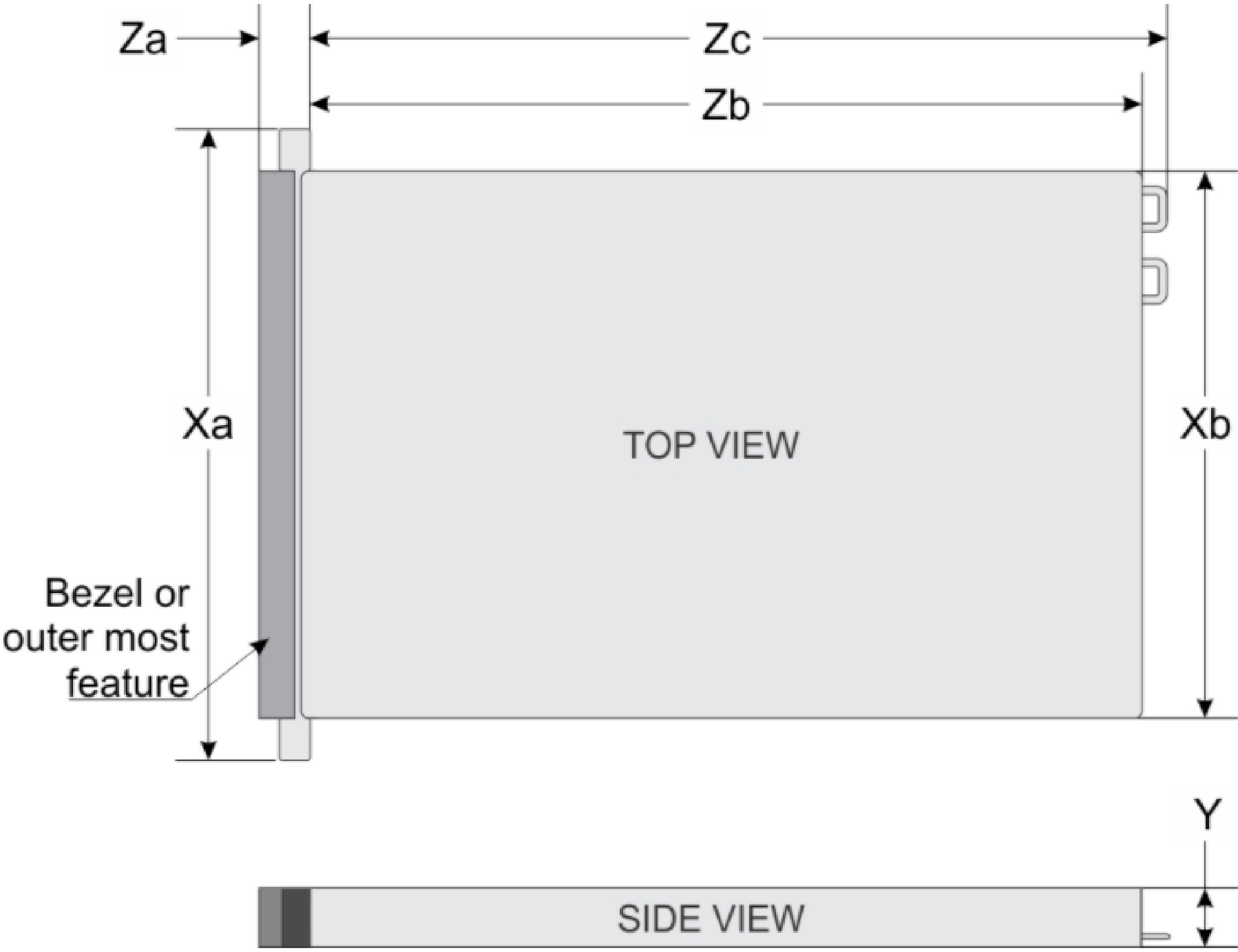
Rack-mounting your hardware appliance and connecting it to power

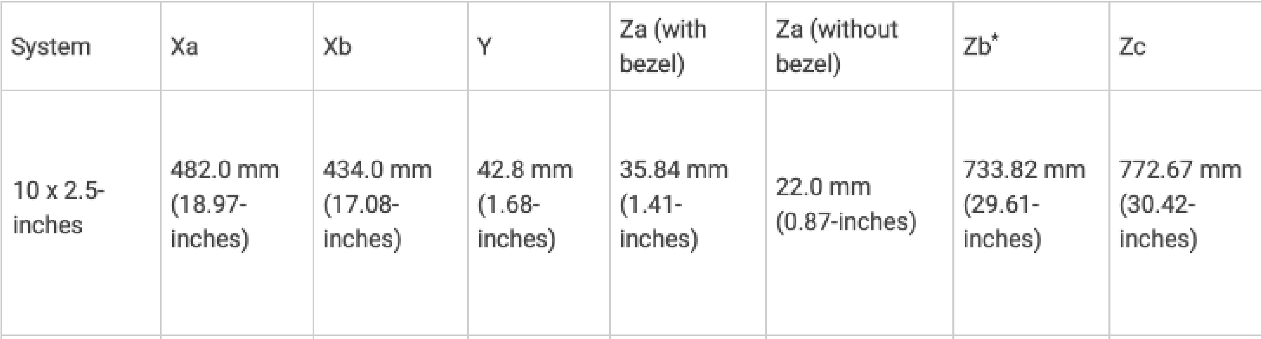
After you unbox your Storage Gateway Hardware Appliance, follow the instructions contained in the box to rack-mount the server. Your appliance has a 1U form factor and fits in a standard International Electrotechnical Commission (IEC) compliant 19-inch rack.

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





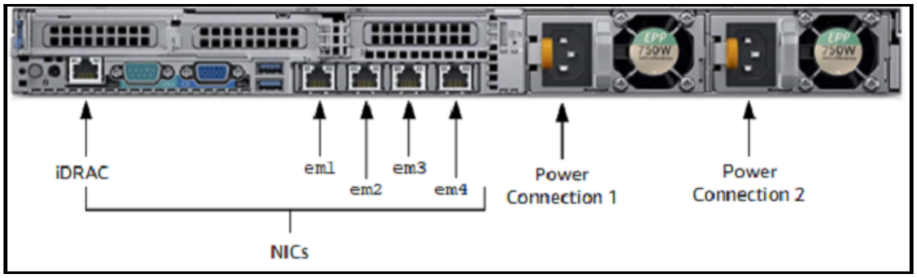
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

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. 11).

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.

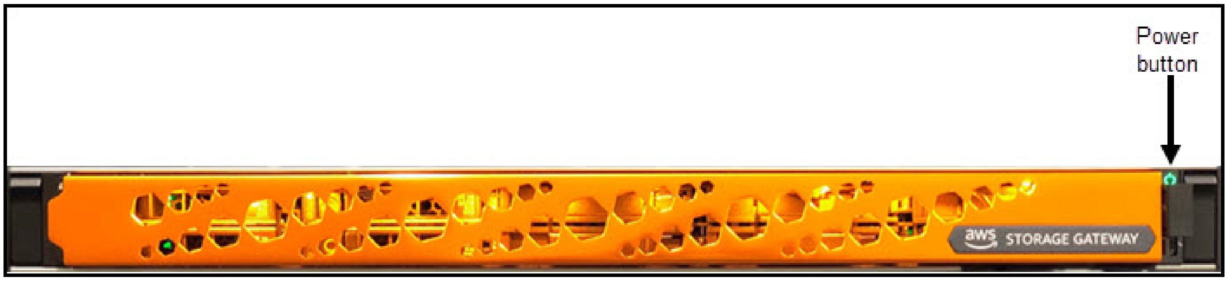
In the following image, you can see the hardware appliance with the different connections.



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.

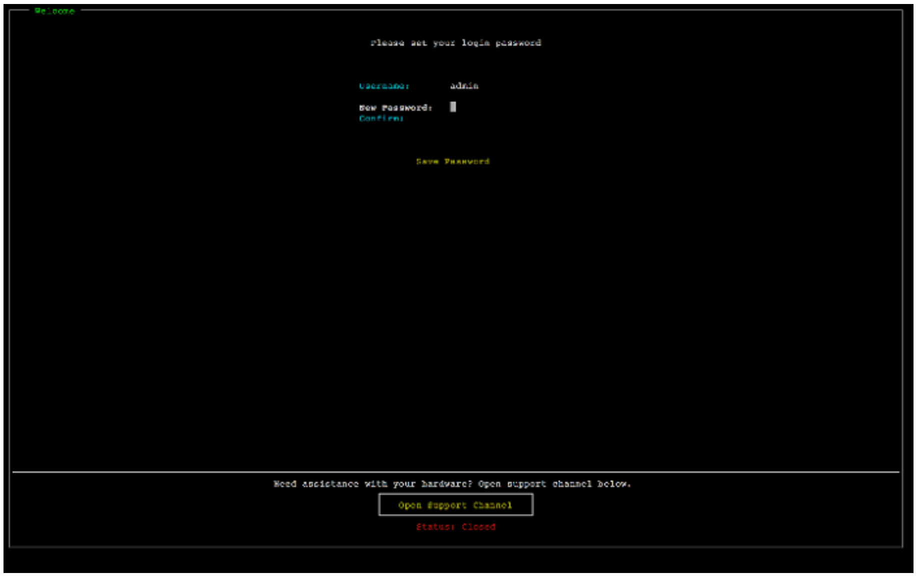


After the server boots up, the hardware console appears on the monitor. The hardware console presents a user interface specific to AWS that you can use to configure initial network parameters. You configure these parameters to connect the appliance to AWS and open up a support channel for troubleshooting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

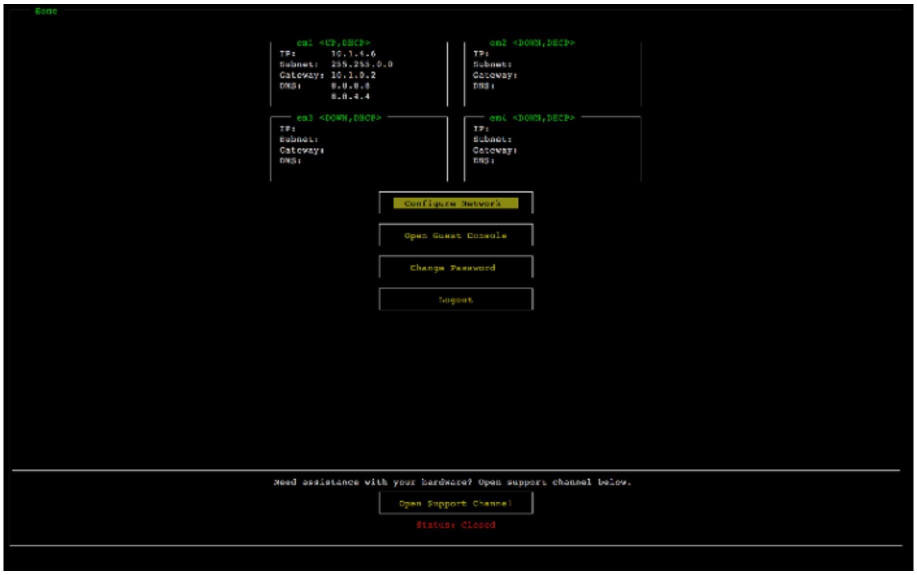
To set a password for the first time

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



```
Welcome

Please set your login password

Username:       admin

New Password:
Confirm:

Save Password

Need assistance with your hardware? Open support channel below.
Open Support Channel
Status: Closed
```

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



```
Home

em1 <UP,DHCP>                em2 <DOWN,DHCP>
IP:       10.1.4.6           IP:
Subnet:   255.255.0.0        Subnet:
Gateway:  10.1.0.2           Gateway:
DNS:      8.8.8.8            DNS:
          8.8.4.4

em3 <DOWN,DHCP>              em4 <DOWN,DHCP>
IP:                          IP:
Subnet:                      Subnet:
Gateway:                     Gateway:
DNS:                         DNS:

Configure Network
Open Guest Console
Change Password
Logout

Need assistance with your hardware? Open support channel below.
Open Support Channel
Status: Closed
```

Next step

Configuring network parameters (p. 21)

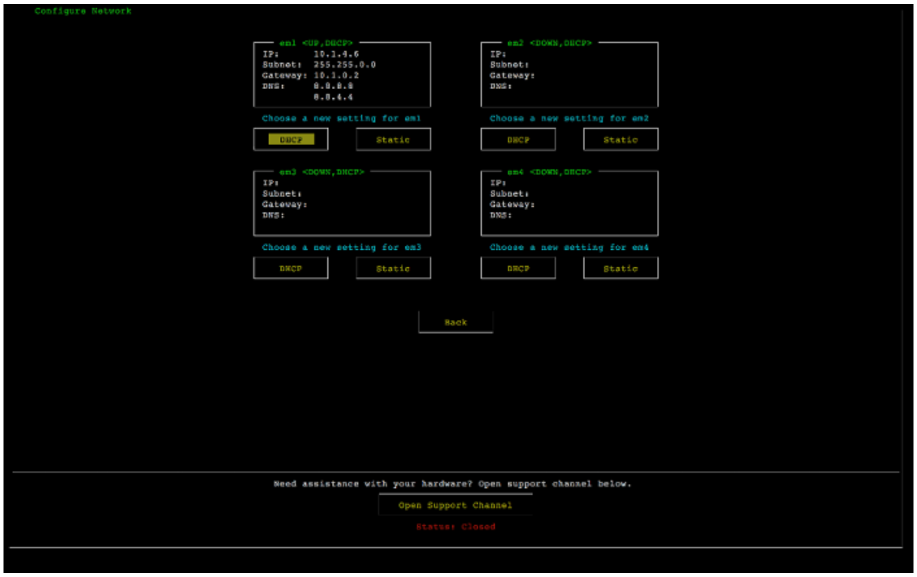
Configuring network parameters

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. 18).

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.



```
Configure Network

em1 <UP,DHCP>                 em2 <DOWN,DHCP>
IP:       10.1.4.6            IP:
Subnet:   255.255.0.0         Subnet:
Gateway:  10.1.0.2            Gateway:
DNS:      8.8.8.8             DNS:
          8.8.4.4
Choose a new setting for em1  Choose a new setting for em2

em3 <DOWN,DHCP>               em4 <DOWN,DHCP>
IP:                           IP:
Subnet:                       Subnet:
Gateway:                      Gateway:
DNS:                          DNS:
Choose a new setting for em3  Choose a new setting for em4

Need assistance with your hardware? Open support channel below.
Status: Closed
```

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

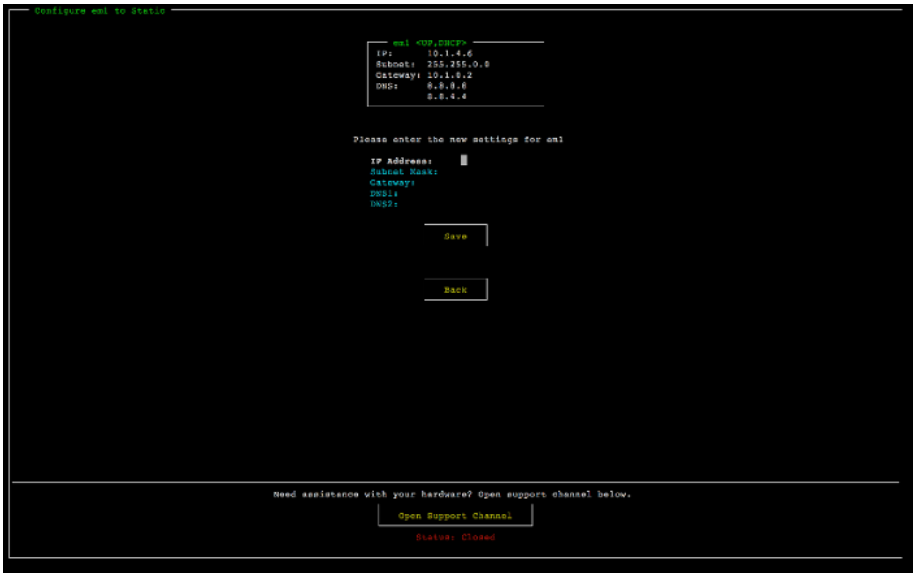
   - Use the IPv4 address assigned by your Dynamic Host Configuration Protocol (DHCP) server to your physical network port.

     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.



```
Configure em1 to Static

  em1 <UP,DHCP>
  IP:       10.1.4.6
  Subnet:   255.255.0.0
  Gateway:  10.1.0.2
  DNS:      8.8.8.8
            8.8.4.4

Please enter the new settings for em1

  IP Address:
  Subnet Mask:
  Gateway:
  DNS1:
  DNS2:

      Save

      Back

Need assistance with your hardware? Open support channel below.
      Open Support Channel
      Status: Closed
```

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. 23)

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*.

New console

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 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**.

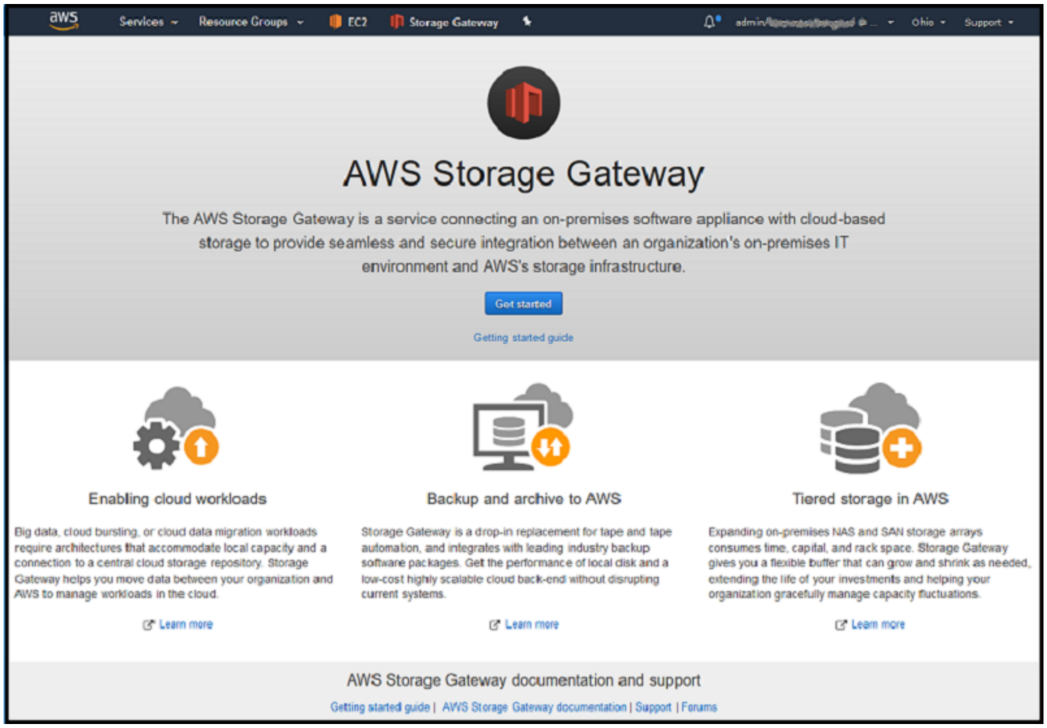
   ZFS is used as the RAID volume manager on the hardware appliance to provide better performance and data protection. ZFS is a software-based, open-source file system and logical volume manager. The hardware appliance is specifically tuned for ZFS RAID. For more information on ZFS RAID, see the ZFS Wikipedia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

Original console

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 Storage Gateway Management Console with the account credentials to use to activate your hardware.

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



AWS Storage Gateway

The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure.

Enabling cloud workloads

Big data, cloud bursting, or cloud data migration workloads require architectures that accommodate local capacity and a connection to a central cloud storage repository. Storage Gateway helps you move data between your organization and AWS to manage workloads in the cloud.

Backup and archive to AWS

Storage Gateway is a drop-in replacement for tape and tape automation, and integrates with leading industry backup software packages. Get the performance of local disk and a low-cost highly scalable cloud back-end without disrupting current systems.

Tiered storage in AWS

Expanding on-premises NAS and SAN storage arrays consumes time, capital, and rack space. Storage Gateway gives you a flexible buffer that can grow and shrink as needed, extending the life of your investments and helping your organization gracefully manage capacity fluctuations.

AWS Storage Gateway documentation and support

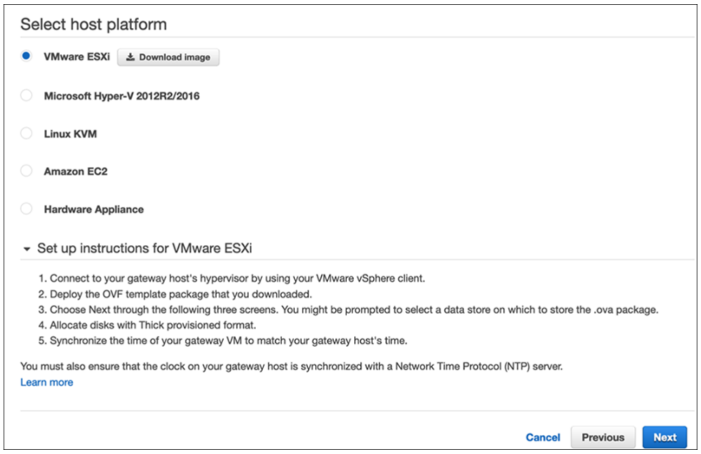
Getting started guide | AWS Storage Gateway documentation | Support | Forums

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.



Select host platform

● VMware ESXi

○ Microsoft Hyper-V 2012R2/2016

○ Linux KVM

○ Amazon EC2

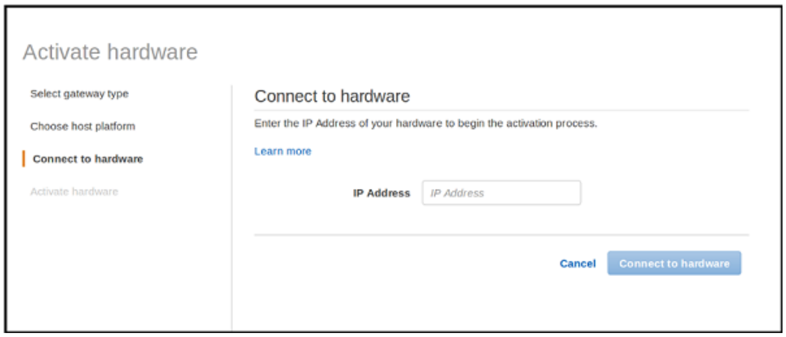
○ Hardware Appliance

Set up instructions for VMware ESXi

1. Connect to your gateway host's hypervisor by using your VMware vSphere client.
2. Deploy the OVF template package that you downloaded.
3. Choose Next through the following three screens. You might be prompted to select a data store on which to store the .ova package.
4. Allocate disks with Thick provisioned format.
5. Synchronize the time of your gateway VM to match your gateway host's time.

You must also ensure that the clock on your gateway host is synchronized with a Network Time Protocol (NTP) server.
Learn more

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



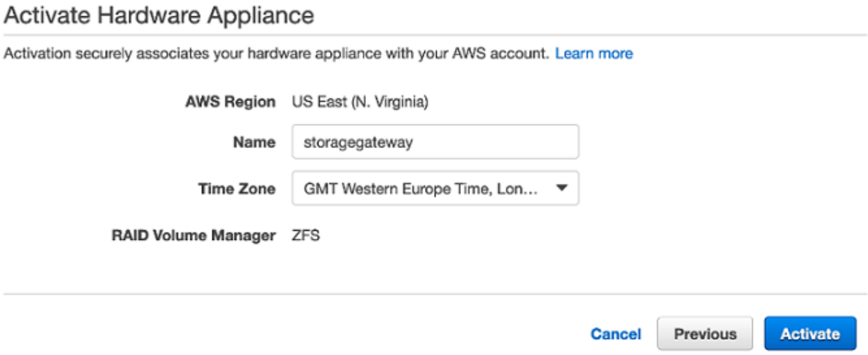
Activate hardware

Connect to hardware

Enter the IP Address of your hardware to begin the activation process.

IP Address: IP Address

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



Activate Hardware Appliance

Activation securely associates your hardware appliance with your AWS account. Learn more

AWS Region: US East (N. Virginia)

Name: storagegateway

Time Zone: GMT Western Europe Time, Lon...

RAID Volume Manager: ZFS

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

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

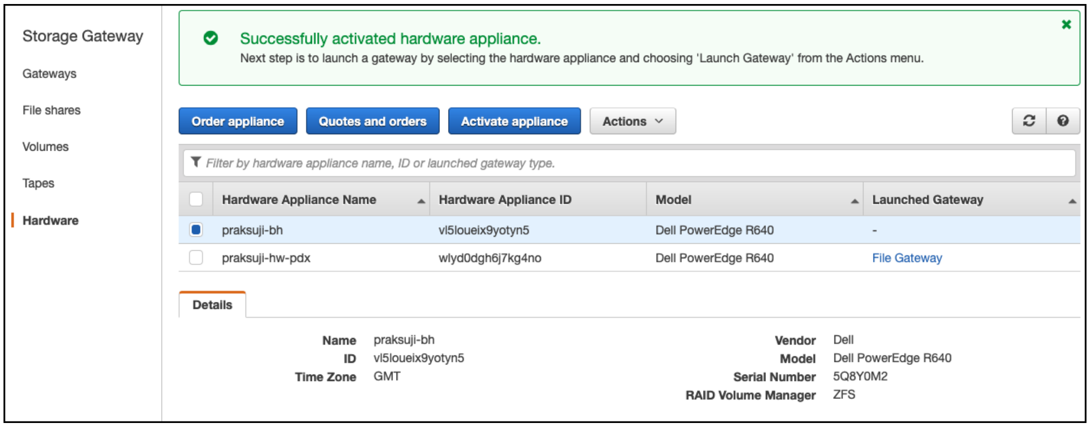
   > **Note**
   > We recommend setting the time zone for your appliance as this determines a standard update time that is out of the usual working day window.
7. (Optional) Keep the **RAID Volume Manager** set to **ZFS**.

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

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

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

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



Successfully activated hardware appliance.
Next step is to launch a gateway by selecting the hardware appliance and choosing 'Launch Gateway' from the Actions menu.

Filter by hardware appliance name, ID or launched gateway type.

	Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
☑	praksuji-bh	vl5loueix9yotyn5	Dell PowerEdge R640	-
□	praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Name praksuji-bh
ID vl5loueix9yotyn5
Time Zone GMT

Vendor Dell
Model Dell PowerEdge R640
Serial Number 5Q8Y0M2
RAID Volume Manager ZFS

Next step

Launching a gateway (p. 27)

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. 27)

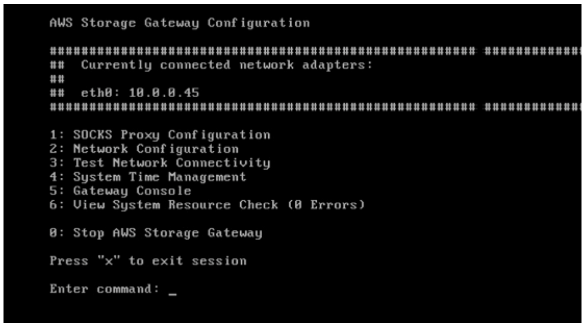
Configuring an IP address for the gateway

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

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

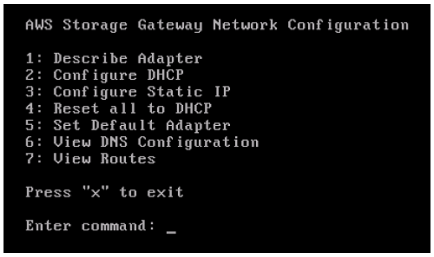
1. On the hardware console, choose **Open Service Console** to open a login screen for the gateway local console.
2. Enter the localhost **login** password, and then press `Enter`.

   The default account is `admin` and the default password is `password`.
3. Change the default password. Choose **Actions** then **Set Local Password** and enter your new credentials in the **Set Local Password** dialog box.
4. (Optional) Configure your proxy settings. See Rack-mounting your hardware appliance and connecting it to power (p. 18) for instructions.
5. Navigate to the Network Settings page of the gateway local console as shown following.



```
AWS Storage Gateway Configuration

###################################################### ############
##  Currently connected network adapters:
##
##  eth0: 10.0.0.45
###################################################### ############

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

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



```
AWS Storage Gateway Network Configuration

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

Press "x" to exit

Enter command: _
```

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

To exit the gateway local console

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

  Note

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

Next step

Configuring your gateway (p. 28)

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 local disks (p. 37).

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 Storage Gateway Console and Removing Associated Resources (p. 99).

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. 29).
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.

Getting started with Storage Gateway

In this section, you can find instructions about how to create and activate a file gateway in Storage Gateway. Before you get started, make sure that your setup meets the required prerequisites and other requirements described in Setting up for Amazon FSx File Gateway (p. 4).

Topics

Step 1: Create an FSx for Windows File Server file system

To create an Amazon FSx File Gateway in Storage Gateway, the first step is to create an Amazon FSx for Windows File Server file system. If you have already created an Amazon FSx file system, go to the next step, Step 2: (Optional) Create an Amazon VPC endpoint (p. 30).

> **Note**
> The following limitations apply when writing to an Amazon FSx file system from FSx File gateway:
>
> - Your Amazon FSx file system and your FSx File gateway must be owned by the same AWS account and located in the same AWS Region.
> - Each gateway can support 5 attached file systems. When attaching a file system, the Storage Gateway console notifies you if the selected gateway is at capacity, in which case you must choose a different gateway or detach a file system before you can attach another one.
> - FSx File gateway supports soft storage quotas (warning when users surpass their data limits), but does not support hard quotas (enforcing data limits by denying write access). Soft quotas are supported for all users except the Amazon FSx admin user. For more information on setting up storage quotas, see Storage quotas in the Amazon FSx User Guide.

To create an FSx for Windows File Server file system

1. Open the AWS Management Console at https://console.aws.amazon.com/fsx/home/, and choose the Region that you want to create your gateway in.
2. Follow the instructions in Getting Started with Amazon FSx in the *FSx for Windows File Server User Guide*

Step 2: (Optional) Create an Amazon VPC endpoint

This step is not required when you are creating an Amazon FSx File Gateway (FSx File) in Storage Gateway. However, we recommend that you create a virtual private cloud (VPC) endpoint for Storage

Gateway and activate the gateway in the VPC. This creates a private connection between your VPC and Storage Gateway.

If you already have a VPC endpoint for Storage Gateway, you can use it for your FSx File. A single VPC endpoint that can support multiple gateways allows gateways deployed in your VPC to connect to the Storage Gateway service VPC. Skip to the next step if you have already created a VPC endpoint for Storage Gateway.

To create an Amazon VPC endpoint

1. Open the AWS Management Console at https://console.aws.amazon.com/vpc/home/, and choose the AWS Region that you want to create your gateway in.
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**, search for `storagegateway`. The Region will default to the Region that you are signed in to—for example, `com.amazonaws.`*`region`*`.storagegateway`. So if you are signed in to US East (Ohio), you would see `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**, create a new security group to use with your VPC. Make sure that all of the following TCP ports are allowed in your security group:

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

   Note
   The gateway uses these ports to communicate back to the Storage Gateway managed service. When you are using a VPC endpoint, the following ports must be open for inbound access from the IP address of your gateway.
8. Choose **Create endpoint**. The initial state of the endpoint is **Pending**. When the endpoint is created, take note of the ID of the VPC endpoint that you just created.

   Note
   We recommend that you provide a name for this VPC endpoint, for example, **`StorageGatewayEndpoint`**.
9. When the endpoint is created, choose **Endpoints**, and 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 should look similar to this: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

    Note
    This DNS name will resolve to the Storage Gateway endpoint private IP addresses that are allocated in your VPC.
11. Review the list of ports that must be opened on your firewall.

Now that you have created a VPC endpoint, you can create your FSx File.

Next step

the section called “Step 3: Create and activate an FSx File gateway” (p. 32)

Step 3: Create and activate an Amazon FSx File Gateway

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

Topics

Note
A new console interface is available for gateway creation. Choose either the **New console** or **Original console** instructions based on the console that you are using.

Choose a gateway type

With an Amazon FSx File Gateway (FSx File), you store and retrieve files in FSx for Windows File Server with a local cache for low latency access to your most recently used data.

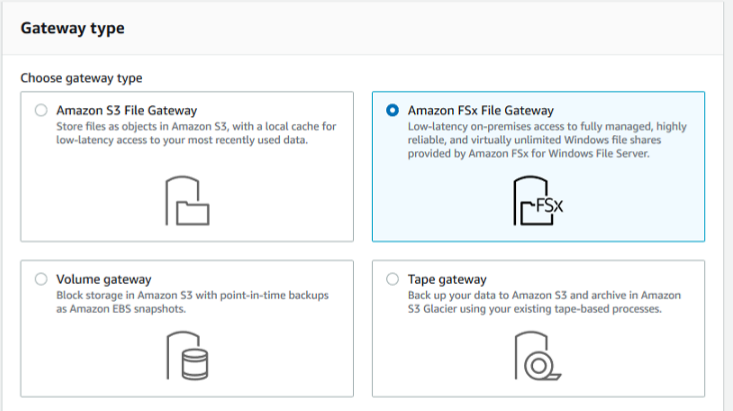
To choose a gateway type

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

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

2. Do one of the following:
   - If you haven't created a gateway in the Region that you chose, choose **Get started**.
   - If you already have a gateway in the Region that you chose, choose **Gateways** in the navigation pane, and then choose **Create gateway**.

3. For **Select gateway type**, choose **Amazon FSx File Gateway**, and then choose **Next**.



Gateway type

Choose gateway type

○ Amazon S3 File Gateway
Store files as objects in Amazon S3, with a local cache for low-latency access to your most recently used data.

● Amazon FSx File Gateway
Low-latency on-premises access to fully managed, highly reliable, and virtually unlimited Windows file shares provided by Amazon FSx for Windows File Server.

○ Volume gateway
Block storage in Amazon S3 with point-in-time backups as Amazon EBS snapshots.

○ Tape gateway
Back up your data to Amazon S3 and archive in Amazon S3 Glacier using your existing tape-based processes.

In the next step, you will Choose a host platform and download the VM (p. 33).

Choose a host platform and download the VM

If you create your gateway on premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see Supported hypervisors and host requirements (p. 13).

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

To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:
   - If you choose the hardware appliance, activate it by following the instructions in Activating your hardware appliance (p. 23).
   - If you choose one of the other options, choose **Download image** next to your virtualization platform to download a .zip file that contains the .ova file for your virtualization platform.

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

   For Amazon EC2, you create an instance from the provided AMI.
3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache during the deployment. A file gateway requires only one local disk for a cache. For information about local disk requirements, see Hardware and storage requirements (p. 6).

   Depending on your hypervisor, you can set specific options:

   - If you choose VMware, do the following:
     - Store your disk using the **Thick provisioned format** option. When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in thick-provisioned format.
   - If you choose Microsoft Hyper-V, do the following:
     - Configure the disk type using the **Fixed size** option. When you use fixed-size provisioning, the disk storage is allocated immediately, resulting in better performance. If you don't use fixed-size provisioning, the storage is allocated on demand. On-demand allocation can affect the functioning of Storage Gateway. For Storage Gateway to function properly, the VM disks must be stored in fixed-size provisioned format.
     - When allocating disks, choose **virtual hard disk (.vhd) file**. Storage Gateway supports the .vhdx file type. By using this file type, you can create larger virtual disks than with other file types. If you create a .vhdx type virtual disk, make sure that the size of the virtual disks that you create doesn't exceed the recommended disk size for your gateway.
   - If you choose Linux Kernel-based Virtual Machine (KVM), do the following:
     - Don't configure your disk to use `sparse` formatting. When you use fixed-size (nonsparse) provisioning, the disk storage is allocated immediately, resulting in better performance.
     - Use the parameter `sparse=false` to store your disk in nonsparse format when creating new virtual disks in the VM with the `virt-install` command for provisioning new virtual machines.

- Use virtio drivers for disk and network devices.
- We recommend that you don't set the current_memory option. If necessary, set it equal to the RAM provisioned to the gateway in the --ram parameter.

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

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

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

For information about deploying your gateway to an Amazon EC2 host, see Deploying a file gateway on an Amazon EC2 host (p. 157).

Choose a service endpoint

In this step, you choose a service endpoint for your gateway in Storage Gateway.

You can activate your gateway using:

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

New console

To choose a service endpoint

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

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

   This procedure assumes that you are activating your gateway with a public endpoint. For information about how to activate a gateway using a VPC endpoint, see Activating a gateway in a virtual private cloud (p. 47).
2. Choose **Next** to connect and activate your gateway.

Original console

To choose a service endpoint

1. For **Endpoint type**, choose one of the following:

   - To have your gateway access AWS services over the public internet using a public service endpoint, choose **Public**.
   - To have your gateway access AWS services over the public internet using a public service endpoint that complies with FIPS, choose **FIPS**.

     If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.
   - To have your gateway access AWS services over a private VPC endpoint connection using a public service endpoint, choose **VPC**.

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

   This procedure assumes that you are activating your gateway with a public endpoint. For information about how to activate a gateway using a VPC endpoint, see Activating a gateway in a virtual private cloud (p. 47).
2. Choose **Next** to connect and activate your gateway.

Connect to the gateway

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

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

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

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

1. Log on to your gateway VM local console. For detailed instructions, see the following:
   - VMware ESXi – Accessing the Gateway Local Console with VMware ESXi (p. 91).
   - Microsoft Hyper-V – Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - Linux KVM – Accessing the Gateway Local Console with Linux KVM (p. 89).
2. Get the IP address from the top of the menu page, and note it for later use.

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

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Instances**, and then choose the EC2 instance.

3. Choose the **Details** tab at the bottom, and then note the IP address or activation key. You use one of these to activate the gateway.

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

New console

To associate your gateway with your AWS account

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

Original console

To associate your gateway with your AWS account

1. If the **Connect to gateway** page isn't already open, open the console and navigate to that page.
2. Enter the IP address of your gateway for **IP address**, and then choose **Connect gateway**.

For detailed information about how to get a gateway IP address, see Connecting to Your Gateway (p. 161).

Activate the gateway

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

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

  Note
  You can also activate your gateway in a virtual private cloud to create a private connection between your on-premises software appliance and cloud-based storage infrastructure. You can then use the software appliance to transfer data to AWS storage without your gateway communicating with AWS storage services over the public internet. For instructions, see Activating a gateway in a virtual private cloud (p. 47).

New console

To activate your gateway

1. In **Activate gateway**, do the following:
   - For **Gateway time zone**, select a time zone to use for your gateway.

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

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

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

Original console

To activate your gateway

1. To complete the activation process, provide information on the activation page to configure your gateway setting:
   - **Gateway time zone** specifies the time zone to use for your gateway.
   - **Gateway name** identifies your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.
2. (Optional) In the **Add tags** section, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

If activation isn't successful, see Troubleshooting your gateway (p. 135) for possible solutions.

Configure local disks

When you deployed the VM, you allocated local disks for your gateway. Now you configure your gateway to use these disks. We recommend a minimum cache of 150 GiB and maximum cache size of 64 TiB.

To configure local disks

1. For **Configure local disks**, identify the disks that you added and decide which ones to allocate for cached storage. We recommend a minimum cache of 150 GiB and maximum cache size of 64 TiB.
2. For **Allocated to**, choose **Cache** for the disk that you want to configure as cache storage.

   If you don't see your disks, choose **Refresh**.
3. Choose **Save and continue** to save your configuration settings.

Configure Amazon CloudWatch logging

To notify you about the health of your file gateway and its resources in Storage Gateway, you can configure an Amazon CloudWatch log group. For more information, see Getting file gateway health logs with CloudWatch log groups (p. 58).

New console

To configure a CloudWatch log group for your file gateway

1. For **Configure logging - *optional***, choose one of the following:
   - **Disable logging** if you don't want to monitor your gateway using CloudWatch log groups.

- **Create a new log group** to create a new CloudWatch log group.
- **Use an existing log group** to use a CloudWatch log group that already exists.

  Choose a log group from the **Existing log group list**.

2. Choose **Save and continue** to save your configuration settings.

Original console

To configure a CloudWatch log group for your file gateway

1. In the **Gateway Log Group** wizard, choose the **Create new Log Group** link to create a new log group. You are directed to the CloudWatch console to create one. If you already have a CloudWatch log group that you want to use to monitor your gateway, choose that group for **Gateway Log Group**.
2. If you create a new log group, choose the refresh button to view the new log group in the list.
3. If your gateway is deployed on a VMware host that is enabled for VMware High Availability (HA) cluster, you're prompted to verify and test the VMware HA configuration. In this case, choose **Verify VMware HA**. Otherwise, choose **Save and Continue**.

Verify VMware High Availability (VMware HA clusters only)

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

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

New console

To test for VMware HA

1. For **Verify VMware High Availability configuration**, choose **Next**. Verification can take up to two minutes to complete.

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

Original console

To test for VMware HA

1. On the **Verify VMware High Availability Configuration** page, choose **Verify VMware HA**. This can take up to two minutes to complete.
2. If the test is successful, a message that indicates a successful test is displayed in the banner. If the test fails, a failed message is displayed. You can make changes in your vSphere configuration and repeat the test.
3. To repeat the test, for **Actions** choose **Verify VMware HA**.

For information about how to configure your gateway for VMware HA, see Using VMware vSphere High Availability with Storage Gateway (p. 103).

After you Amazon FSx File Gateway is activated and running you need to perform these a tasks before you can use your gateway.

- Configure Active Directory for your gateway to join a domain
- Attach an FSx for Windows File Server file system you created earlier to your FSx File gateway
- Mount your SMB file share on your client.

Next step

Configure Active Directory settings (p. 40)

Configure Active Directory settings

In this step, you configure your Amazon FSx File Gateway access settings in Storage Gateway to join a Microsoft Active Directory.

New console

To configure Active Directory settings

1. In the Storage Gateway console, choose **Attach FSx file system**.
2. On the **Confirm gateway** page, in the list of gateways, choose the Amazon FSx File Gateway that you want to use.

   If you don't have a gateway, you must create one. Make sure your gateway can resolve the name of your Active Directory Domain Controller. For information, see Required prerequisites (p. 5).
3. Enter values for the **Active Directory settings**:

   > **Note**
   > If your gateway is already joined to a domain, you don't need to join again. Go to the next step.

   - For **Domain name**, enter the domain name of the Active Directory that you want to use.
   - For **Domain user**, enter a user name for the Active Directory.
   - For **Domain password**, enter the password for the domain user.

     > **Note**
     > Your account must be able to join a server to a domain.
   - For **Organizational unit- optional**, you can specify an organizational unit the Active Directory belongs to.
   - Enter a value for **Domain controller(s) - optional**.
4. Choose **Next** to open the **Attach FSx File system** page.

Original console

To configure Microsoft Active Directory access settings

1. Choose **Gateways**, and on the Gateway page, select the check box next to the Amazon FSx file gateway that you want to join to a domain.

   If you don't have a gateway, you must create one. Make sure your gateway can resolve the name of your Active Directory Domain Controller. For information, see Required prerequisites (p. 5).
2. From **Actions**, choose **Edit SMB settings**.
3. Choose the pencil icon in the upper-right corner of the Active Directory settings section.
4. Enter the values for **Domain name**, **Domain user**, and **Domain password**. Optionally, you can specify an organizational unit, and domain controllers.
5. Choose **Save**, and then choose **Close**.

   > **Note**
   > If a file system is attached to a gateway, you can’t edit the domain information. You need to detach the file system and then you can change the domain information. The pencil icon for editing is not active, as seen following, if the gateway has one or more file systems attached.

Next step

Attach an Amazon FSx for Windows File Server file system (p. 42)

Attach an Amazon FSx for Windows File Server file system

The next step is to attach an Amazon FSx file system to the gateway. When you attach an Amazon FSx file system, all the file shares on the file system are made available to Amazon FSx File Gateway (FSx File) for you to mount.

> **Note**
> The following limitations apply when writing to an Amazon FSx file system from Amazon FSx File Gateway:
>
> - Your Amazon FSx file system and your FSx File must be owned by the same AWS account and located in the same AWS Region.
> - Each gateway can support up to five attached file systems. When you're attaching a file system, the Storage Gateway console notifies you if the selected gateway is at capacity. In that case, you must choose a different gateway or detach a file system before you can attach another one.
> - FSx File supports soft storage quotas (which warn you when users surpass their data limits), but does not support hard quotas (which enforce data limits by denying write access). Soft quotas are supported for all users except the Amazon FSx admin user. For more information about setting up storage quotas, see Storage quotas in the Amazon FSx User Guide.

New console

To attach an Amazon FSx file system

1. In the Storage Gateway console, on the **FSx file systems** > **Attach FSx file system** page, complete the following fields in the **FSx file system settings** section:

   - For **FSx file system name**, choose the file system that you want to attach from the dropdown list.
   - For **Local Endpoint IP address**, enter the gateway IP address that clients will use to browse file shares on the FSx file system.

     > **Note**
     >
     > - If you plan to attach only one file system to your gateway, you can leave this field blank to make shares on the file system available on all of the gateway's IP addresses. If you plan to attach multiple file systems, you must specify an IP address for each of them.
     > - If you attach a file system without an IP address and need to attach another file system later, you must detach the first file system and reattach it with an IP address.
     > - For Amazon EC2 gateways, you can specify the private IP address of the EC2 instance, unless it is already in use by a different file system, in which case you must add a new private address to the gateway, then restart it. For more information, see Multiple IP addresses in the *Amazon EC2 User Guide*.
     > - For on-premises gateways, you can specify the IP address of the primary network interface (static or DHCP), unless it is already in use by a different file system, in which case you must provide a different IP address from the same subnet as the primary interface, which will be made available as a virtual IP. Do not use an IP address assigned to any network interface other than the primary.

2. In the **Service account settings** section, provide the user name and password that is associated with the Amazon FSx file system.

   Note

   This user must have the backup administrator role from the Active Directory service that is associated with your Amazon FSx file systems.
   To ensure sufficient permissions to files, folders, and file metadata, we recommend that you make this user a member of the file system administrators group. If you are using AWS Directory Service for Microsoft Active Directory with Amazon FSx for Windows File Server, the user must be a member of the AWS Delegated FSx Administrators group.
   If you are using a self-managed Active Directory with Amazon FSx for Windows File Server, the user must be a member of one of two groups: the domain admins or the custom delegated file system administrators group you specified for the file system administration when you created your file system.
3. In the **Audit logs** section, choose **Existing log groups**, and choose the log that you want to use to monitor access to your Amazon FSx file system. You can create a new one. If you don't want to monitor your system, choose **Disable logging**.
4. For **Automated cache refresh setting**, if you want your cache to refresh automatically, choose **Set refresh interval** and specify an interval between 5 minutes and 30 days.
5. (Optional) In the **Tags** section, choose **Add new tag** to add one or more keys and a value for tagging your settings.
6. Choose **Next** and review the settings. To change your settings, you can choose **Edit** in each section.
7. When you are done, choose **Finish**.

Original console

To attach an Amazon FSx file system

1. From the top menus, choose **Attach FSx file system**. You are redirected to the **Configure settings** page.
2. For **Amazon FSx File System name**, choose the Amazon FSx file system that you want to attach. If you don't have an Amazon FSx file system, create one.
3. For **Gateway**, choose the FSx File that you want to associate the file system with.
4. For **User**, enter the user name that you use to access the file system.
5. For **Password**, enter the password for the file system.
6. For **Audit logs**, choose one of the options to use a log group. You can use an existing log group.
7. For **Automated cache refresh from FSx**, select the check box and set the time in days, hours, and minutes to refresh the file system's cache using Time To Live (TTL). TTL is the length of time since the last refresh. When the directory is accessed after that length of time, the file gateway refreshes that directory's contents from the Amazon FSx file system.
8. In the **Add tags** section, you can add one or more keys and a value for your settings.
9. Choose **Next**, review your choices, and choose **Attach file system.**.

Next step

Mount and use your file share (p. 44)

Mount and use your file share

Before mounting your file share on the client, wait for the status of the Amazon FSx file system to change to **Available**. After your file share is mounted, you can start using your Amazon FSx File Gateway (FSx File).

Topics

Mount your SMB file share on your client

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

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

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

> **Note**
> If you are a Microsoft Active Directory 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.
> Amazon FSx File Gateway doesn't support SMB locking or SMB extended attributes.

To mount an SMB file share for Active Directory users using the net use command

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

```
net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on
the FSx file system]
```

To mount an SMB file share on Windows using CmdKey

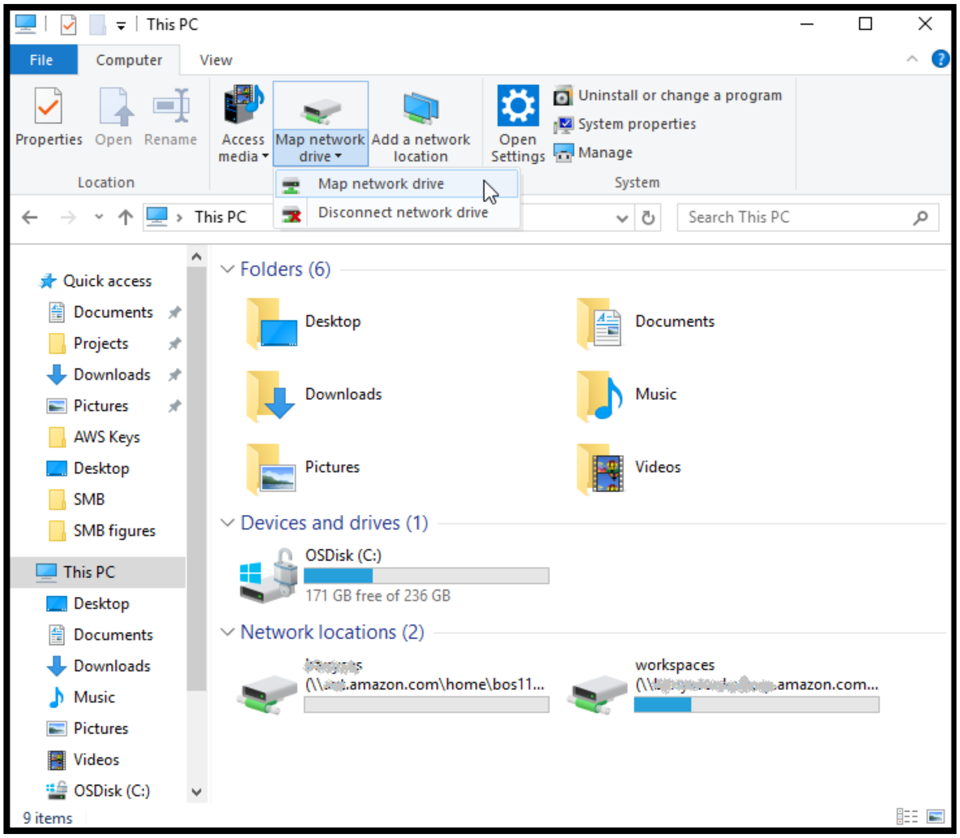
1. Press the Windows key and enter **cmd** to view the command prompt menu item.
2. Open the context (right-click) menu for **Command Prompt**, and choose **Run as administrator**.
3. Enter the following command:

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

Note
When mounting file shares, you might need to remount your file share after rebooting your client.

To mount an SMB file share using Windows File Explorer

1. Press the Windows key and enter `File Explorer` in the **Search Windows** box, or press `Win+E`.
2. In the navigation pane, choose **This PC**.
3. On the **Computer** tab, choose **Map network drive**, and then choose **Map network drive** again, as shown in the following screenshot.



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

Test your FSx File

You can copy files and directories to your mapped drive. The files automatically upload to your FSx for Windows File Server file system.

To upload files from your Windows client to Amazon FSx

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 file system name.
2. Copy files or a directory to the drive.

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

Activating a gateway in a virtual private cloud

You can create a private connection between your on-premises gateway and cloud-based storage infrastructure. You can then use the gateway to transfer data to AWS storage without your gateway communicating with AWS storage services over the public internet. Using the Amazon VPC service, you can launch AWS resources in a custom virtual network. You can use a virtual private cloud (VPC) to control your network settings, such as the IP address range, subnets, route tables, and network gateways. For more information about VPCs, see What is Amazon VPC? in the *Amazon VPC User Guide*.

To use a gateway with a Storage Gateway VPC endpoint in your VPC, do the following:

- Use the VPC console to create a VPC endpoint for Storage Gateway and get the VPC endpoint ID. You use this VPC endpoint ID to activate the gateway.

> **Note**
> Your gateway must be activated in the same region where your VPC endpoint was created.

Creating a gateway using a VPC endpoint

In this section, you can find instructions about how to download, deploy, and activate your file gateway using a VPC endpoint.

Topics

Creating a VPC endpoint for Storage Gateway

Follow these instructions to create a VPC endpoint. If you already have a VPC endpoint for Storage Gateway, you can use it.

To create a VPC endpoint for Storage Gateway

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Endpoints**, and then choose **Create Endpoint**.
3. On the **Create Endpoint** page, choose **AWS Services** for **Service category**.
4. For **Service Name**, choose `com.amazonaws.`*`region`*`.storagegateway`. For example `com.amazonaws.us-east-2.storagegateway`.

5. For **VPC**, choose your VPC and note its Availability Zones and subnets.
6. Verify that **Enable Private DNS Name** is not selected.
7. For **Security group**, choose the security group that you want to use for your VPC. You can accept the default security group. Verify that all of the following TCP ports are allowed in your security group:

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Choose **Create endpoint**. The initial state of the endpoint is **pending**. When the endpoint is created, note the ID of the VPC endpoint that you just created.
9. When the endpoint is created, choose **Endpoints**, then choose the new VPC endpoint.
10. In the **DNS Names** section, use the first DNS name that doesn't specify an Availability Zone. Your DNS name look similar to this: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Now that you have a VPC endpoint, you can create your gateway.

Choosing a gateway type

To choose a gateway type

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

   If you have previously created a gateway in this AWS Region, the console shows your gateway. Otherwise, the service homepage appears.
2. If you haven't created a gateway in the AWS Region that you chose, choose **Get started**. If you already have a gateway in the AWS Region that you chose, choose **Gateways** from the navigation pane, and then choose **Create gateway**.
3. For **Select gateway type**, choose a gateway type, and then choose **Next**.

Choosing a host platform and downloading the VM

If you create your gateway on premises, you deploy the hardware appliance, or download and deploy a gateway VM, and then activate the gateway. If you create your gateway on an Amazon EC2 instance, you launch an Amazon Machine Image (AMI) that contains the gateway VM image and then activate the gateway. For information about supported host platforms, see Supported hypervisors and host requirements (p. 13).

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

To choose a host platform and download the VM

1. For **Select host platform**, choose the virtualization platform that you want to run your gateway on.
2. Do one of the following:

   - If you choose the hardware appliance, activate it by following the instructions in Activating your hardware appliance (p. 23).

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

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

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

3. If you choose a hypervisor option, deploy the downloaded image to your hypervisor. Add at least one local disk for your cache during the deployment. A file gateway requires only one local disk for a cache. For information about local disk requirements, see Hardware and storage requirements (p. 6).

   Depending on your hypervisor, you can set specific options:

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

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

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

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

For information about deploying your gateway to an Amazon EC2 host, see Deploy your gateway to an Amazon EC2 host (p. 157).

Choosing a service endpoint

You can activate your gateway using a private VPC endpoint. If you use a VPC endpoint, all communication from your gateway to AWS services occurs through the VPC endpoint in your VPC in AWS.

New Console

To choose a service endpoint

1. For **Select service endpoint**, choose **VPC**.
2. If you don't have a VPC endpoint, choose **Create a VPC endpoint** to create one in the Amazon VPC console. For instructions on the creating a VPC endpoint, see Creating a VPC endpoint for Storage Gateway (p. 47). A VPC endpoint allows your gateway to communicate with AWS services only through your VPC in AWS without going over the public internet.
3. In **VPC endpoint**, enter the DNS name or the IP address of the VPC endpoint for Storage Gateway. The DNS name looks similar to this: `vpce-1234567e1c11a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`.
4. If you already have a VPC endpoint, choose **Amazon VPC endpoints**. You can identify an existing VPC endpoint by it's DNS name, IP address or VCP endpoint ID.
5. To identify the VPC endpoint by DNS name, choose **DNS name (recommended) or IP address**, provide the DNS name or the IP address. The DNS name looks similar to this: `vpce-1234567e1c11a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`.
6. To identify the VPC endpoint by VPC endpoint ID, choose **VPC endpoint ID** and choose the ID you want from the list.
7. Choose **Next** to connect and activate your gateway.

Original Console

To choose a service endpoint

1. In the console, you can select a service endpoint for your gateway after selecting the host platform. For **Endpoint type**, choose **VPC**. If you don't have a VPC endpoint, choose **Create a VPC endpoint** to create one. A VPC endpoint allows your gateway to communicate with AWS services only through your VPC in AWS without going over the public internet.

   This procedure assumes that you are activating your gateway using a VPC endpoint. For more information about how to activate a gateway using a public endpoint, see the following topics:

   - Getting started with Storage Gateway (p. 30)
2. Enter the VPC endpoint DNS name for Storage Gateway that you created in the Creating a VPC endpoint for Storage Gateway (p. 47) section. Your DNS name looks similar to this: `vpce-1234567e1c11a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`.
3. Choose **Next** to connect to your gateway and activate your gateway.

Connecting to your gateway

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

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

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

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

1. Log on to your gateway VM local console. For detailed instructions, see the following:
   - VMware ESXi – .
   - Microsoft Hyper-V – .
   - Linux KVM – .
2. Get the IP address from the top of the menu page, and note it for later use.

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

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

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

New Console

To associate your gateway with your Amazon Web Services account

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

Original Console

To associate your gateway with your Amazon Web Services account

1. If the **Connect to gateway** page isn't already open, open the console and navigate to that page.
2. Type the IP address of your gateway for **IP address**, and then choose **Connect gateway**.

For detailed information about how to get a gateway IP address, see Connecting to Your Gateway (p. 161).

Activate your gateway in a VPC

Activating a file gateway requires additional setup.

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

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

New Console

To activate your gateway

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

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

     Note
     The gateway name must be between 2 and 255 characters in length.
2. (Optional) For **Add tags**, enter a key and value to add tags to your gateway. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your gateway.
3. Choose **Activate gateway**.

Original Console

To activate your gateway

1. To complete the activation process, provide information on the activation page to configure your gateway setting:

   - **Gateway Time Zone** specifies the time zone to use for your gateway.
   - **Gateway Name** identifies your gateway. You use this name to manage your gateway in the console; you can change it after the gateway is activated. This name must be unique to your account.
2. Choose **Activate gateway**.

If activation isn't successful, see Troubleshooting your gateway (p. 135) for possible solutions.

To associate your gateway with your Amazon Web Services account

If you don’t have internet access and private network access from your browser, you can still do the following.

1. Enter the fully qualified DNS name of the VPC endpoint or elastic network interface to get the activation key from the gateway. You can use curl with the following URL, or just enter this URL into your web browser.

   An example curl command follows.

   An example activation key follows.

   ```
   BME11-LQPTD-DF11P-BLLQ0-111V1
   ```

2. Use the AWS CLI to activate the gateway by specifying the activation key you received in previous step, for example:

   ```
   aws --region us-east-1 storagegateway activate-gateway --activation-key
   BME11-LQPTD-DF11P-BLLQ0-111V1 --gateway-type FILE_S3 --gateway-name user-
   ec2-iad-pl-fgw2 --gateway-timezone GMT-4:00 --gateway-region us-east-1 --
   endpoint-url https://vpce-12345678e91c24a1fe9-62qntt8k.storagegateway.us-
   east-1.vpce.amazonaws.com
   ```

   Following is an example response.

   ```
   {"GatewayARN": "arn:aws:storagegateway:us-east-1:123456789012:gateway/sgw-FFF12345"}
   ```

Configure local disks

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

To configure local disks

1. For **Configure local disks**, identify the disks you added and decide which ones you want to allocate for cached storage. We recommend minimum cache size of 150 GiB and Maximum 64 TiB.
2. For **Allocated to**, choose **Cache** for the disk that you want to configure as cache storage.

   If you don't see your disks, choose **Refresh**.
3. Choose **Save and continue** to save your configuration settings.

Allowing traffic to required ports in your HTTP proxy

Using an HTTP proxy is optional. If you use an HTTP proxy, make sure that you allow traffic from Storage Gateway to the destinations and ports listed following.

When Storage Gateway is communicating through the public endpoints, it communicates with the following Storage Gateway services.

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
> Depending on your gateway's AWS Region, replace *`region`* in the endpoint with the corresponding region string. For example, if you create a gateway in the US West (Oregon) region, the endpoint looks like this: `storagegateway.us-west-2.amazonaws.com:443`.

When Storage Gateway is communicating through the VPC endpoint, it communicates with the AWS services through multiple ports on the Storage Gateway VPC endpoint and port 443 on the Amazon S3 private endpoint.

- TCP ports on Storage Gateway VPC endpoint.
  - 443, 1026, 1027, 1028, 1031, and 2222
- TCP port on S3 private endpoint

- 443

You are now ready to create resources for your gateway.

Next Step

S3 File Create a file share

Managing your Amazon FSx File Gateway resources

The following sections provide information about how to manage your Amazon FSx File Gateway (FSx File) resources, including attaching and detaching Amazon FSx file systems, and configuring Microsoft Active Directory settings.

Topics

Attaching an Amazon FSx file system

You must have an FSx for Windows File Server file system before you can attach it to an FSx File. If you don't have a file system, you must create one. For instructions, see Step 1: Create Your File System in the *FSx for Windows File Server User Guide*.

The next step is to activate an FSx File and configure your gateway to join an Active Directory domain. For instructions, see Configure Active Directory settings (p. 40).

> **Note**
> When your gateway has joined a domain, you don't have to configure it to join the domain again.

Each gateway can support up to five attached file systems. For instructions on how to attach a file system, see Attach an Amazon FSx for Windows File Server file system (p. 42).

Configuring Active Directory for your FSx File

To use FSx File, you are required to configure your gateway to join an Active Directory domain. For instructions, see Configure Active Directory settings (p. 40).

Configuring Active Directory settings

After you configure your gateway to join an Active Directory domain, you can edit the Active Directory settings.

To edit Active Directory settings

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 whose Active Directory settings you want to edit.
3. For **Actions**, choose **Edit SMB settings**, and then choose **Active Directory settings**.
4. Provide the information requested in the Active Directory settings section, and then choose **Save changes**.

Editing FSx File settings

After the gateway is activated, you can edit your gateway settings.

To edit your gateway settings

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 whose settings you want to edit.
3. For **Actions**, choose **Edit gateway information**.
4. For **Gateway name**, edit the name of your gateway that you selected.
5. For **Gateway time zone**, choose a time zone.
6. For **Gateway health log group**, choose one of the options to monitor your gateway using Amazon CloudWatch log groups.

   If you choose **Use an existing log group**, choose a log group from the **Existing log group list**, and then choose **Save changes**.

Editing Amazon FSx for Windows File Server file system settings

After creating an Amazon FSx for Windows File Server file system, you can edit the file system settings.

New console

To edit Amazon FSx file system settings

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. In the navigation pane, choose **File system**, and choose the file system whose settings you want to edit.
3. For **Actions**, choose **Edit file system settings**.
4. In the file system settings section, verify the gateway, Amazon FSx location, and IP address information.

   > **Note**
   > You cannot edit a file system's IP address after it is attached to a gateway. To change the IP address, you must detach and reattach the file system.

5. In the **Audit logs** section, choose an option to use CloudWatch log groups to monitor access to Amazon FSx file systems. You can use an existing log group.
6. For **Automated cache refresh settings**, choose an option. If you choose **Set refresh interval**, set the time in days, hours, and minutes to refresh the file system's cache using Time To Live (TTL).

   TTL is the length of time since the last refresh. When the directory is accessed after that length of time, the file gateway refreshes that directory's contents from the Amazon FSx file system.

> **Note**
> Valid refresh interval values are between 5 minutes and 30 days.

7. In the **Service account settings - optional** section, enter a user name and a **Password**. These credentials are for a user that has the Backup Administrator role from the Active Directory service associated with your Amazon FSx file systems.
8. Choose **Save changes**.

Original console

To edit Amazon FSx file system settings

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. In the navigation pane, choose **File system**, and then choose the file system whose settings you want to edit.
3. For **Actions**, choose **Edit file system settings**.
4. Verify the name of your file system.
5. For **User**, enter a user name. For **Password**, enter a password.
6. For **Automated cache refresh from FSx after**, select the check box and set the time in days, hours, and minutes to refresh the file system's cache using Time To Live (TTL).

   TTL is the length of time since the last refresh. When the directory is accessed after that length of time, the file gateway refreshes that directory's contents from the Amazon FSx file system.
7. In the **Audit logs** section, choose an option to use CloudWatch log groups to monitor access to Amazon FSx file systems. You can use an existing log group.
8. Choose **Save**.

Detaching an Amazon FSx file system

Detaching a file system doesn't delete your data in FSx for Windows File Server. Data that is written to the file shares on these the file systems before you delete the file system will still be uploaded to your FSx for Windows File Server.

To detach an Amazon FSx file system

1. Open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. In the left navigation pane, choose **File system**, and then choose the file system that you want to detach. You can delete multiple file systems.
3. For **Actions**, choose **Detach file system**.
4. Enter `detach` in the box to confirm, and choose **Detach**.

Monitoring your file gateway

You can monitor your file gateway and associated resources in 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. 58).

Topics

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 FSx file system. 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 Amazon CloudWatch logging (p. 37). 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.

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. 145).
- `"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 and fix these types of errors, see Troubleshooting file gateway issues (p. 145).

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.

New 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. 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.

Original 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. 145).

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

Understanding file system 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. 60).

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 FSx File Gateway (FSx File) audit logs provide you with details about user access to files and folders within a file system association. You can use audit logs to monitor user activities and take action if inappropriate activity patterns are identified. The logs are formatted similar to Windows Server security log events, to support compatibility with existing log processing tools for Windows security events.

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 FSx File audit log file access attributes.

Attribute	Definition
`securityDescriptor`	Shows the discretionary access control list (DACL) set on an object, in SDDL format.

Attribute	Definition
sourceAddress	The IP address of file share client machine.
SubjectDomainName	The Active Directory (AD) domain that the client's account belongs to.
SubjectUserName	The Active Directory user name of the client.
source	The ID of the Storage Gateway `FileSystemAssociation` that is being audited.
mtime	This time that the object's content was modified, set by the client.
version	The version of the audit log format.
ObjectType	Defines whether the object is a file or folder.
locationDnsName	The FSx File system DNS name.
objectName	The full path to the object.
ctime	The time that the object's content or metadata was modified, set by the client.
shareName	The name of the share that is being accessed.
operation	The name of the object access operation.
newObjectName	The full path to the new object after it has been renamed.
gateway	The Storage Gateway ID.
status	The status of the operation. Only success is logged (failures are logged with the exception of failures arising from permissions denied).
fileSizeInBytes	The size of the file in bytes, set by the client at file creation time.

Attributes logged per operation

The following table describes the FSx File 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)	Write attributes (chown)	Write attributes (chmod)	Write attributes (chgrp)
securityDescriptor							X			
sourceAddress	X	X	X	X	X	X	X	X	X	X
SubjectDomainName	X	X	X	X	X	X	X	X	X	X
SubjectUserName	X	X	X	X	X	X	X	X	X	X
source	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)	Write attributes (chown)	Write attributes (chmod)	Write attributes (chgrp)
`mtime`			X	X						
`version`	X	X	X	X	X	X	X	X	X	X
`objectType`	X	X	X	X	X	X	X	X	X	X
`locationDnsName`	X	X	X	X	X	X	X	X	X	X
`objectName`	X	X	X	X	X	X	X	X	X	X
`ctime`			X	X						
`shareName`	X	X	X	X	X	X	X	X	X	X
`operation`	X	X	X	X	X	X	X	X	X	X
`newObjectName`					X					
`gateway`	X	X	X	X	X	X	X	X	X	X
`status`	X	X	X	X	X	X	X	X	X	X
`fileSizeInBytes`				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

- Gateway VM local console—see Performing Maintenance Tasks on the Local Console (p. 67).
- 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

The number and size of disks that you want to allocate for your gateway is up to you. The gateway requires the following additional storage:

File gateways require at least one disk to use as a cache. The following table recommends sizes for local disk storage for your deployed gateway. You can add more local storage later after you set up the gateway, and as your workload demands increase.

Local storage	Description	Gateway type
Cache storage	The cache storage acts as the on-premises durable store for data that is pending upload to Amazon S3 or file system.	• File gateways

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.

After the initial configuration and deployment of your gateway, you can adjust the local storage by adding disks for cache storage.

Determining the size of cache storage to allocate

You can initially use this approximation to provision disks for the cache storage. You can then use Amazon CloudWatch operational metrics to monitor the cache storage usage and provision more storage as needed using the console. For information on using the metrics and setting up alarms, see Performance (p. 102).

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.

FSx File doesn't support ephemeral storage.

Managing Gateway Updates Using the Storage Gateway Console

Storage Gateway periodically releases important software updates for your gateway. Either you can manually apply updates on the Storage Gateway Management Console, or 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.

Before any update is applied to your gateway, AWS notifies you with a message on the Storage Gateway console and your AWS Personal Health Dashboard. For more information, see AWS Personal Health Dashboard. The VM doesn't reboot, but the gateway is unavailable for a short period while it's being updated and restarted.

When you deploy and activate your gateway, a default weekly maintenance schedule is set. You can modify the maintenance schedule at any time. When updates are available, the **Details** tab displays a maintenance message. You can see the date and time that the last successful update was applied to your gateway on the **Details** tab.

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

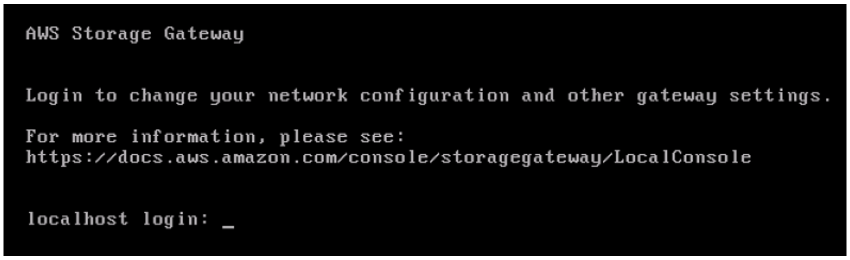
Performing tasks on the VM local console (file gateway)

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

When the VM is ready for you to log in, the login screen is displayed. If this is your first time logging in to the local console, you use the default user name and password to log in. These default login credentials give you access to menus where you can configure gateway network settings and change the password from the local console. Storage Gateway enables you to set your own password from the 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 Logging in to the file gateway local console (p. 68).



```
AWS Storage Gateway


Login to change your network configuration and other gateway settings.

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


localhost login: _
```

To log in to the gateway's local console

- If this is your first time logging in to the local console, log in to the VM with the default credentials. The default user name is `admin` and the password is `password`. Otherwise, use your credentials to log in.

  Note
  We recommend changing the default password. You do this by running the `passwd` command from the local console menu (item 6 on the main menu). For information about how to run the command, see Running storage gateway commands on the local console (p. 77). You can also set the password from the Storage Gateway console. For more information, see Logging in to the file gateway local console (p. 68).

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 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

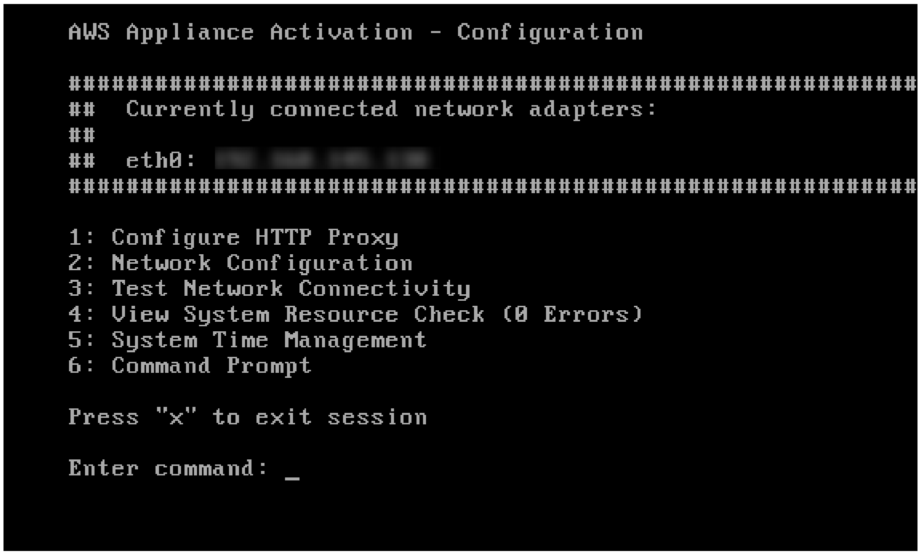
File gateways support configuration of an HTTP proxy.

> **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. 7).

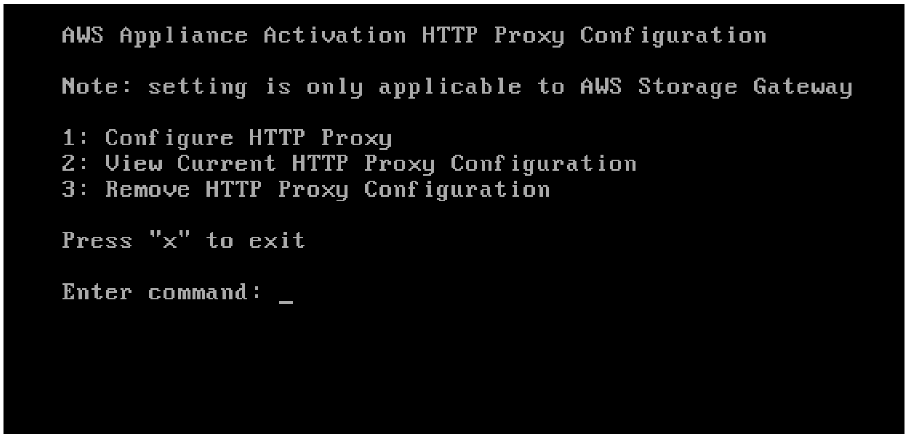
To configure an HTTP proxy for a file gateway

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. 91).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - 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. 89).
2. On the **AWS Appliance Activation - Configuration** main menu, enter `1` to begin configuring the HTTP proxy.



```
AWS Appliance Activation - Configuration

##########################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
##########################################################

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

Press "x" to exit session

Enter command: _
```

3. On the **HTTP Proxy Configuration menu**, enter **1** and provide the host name for the HTTP proxy server.



```
AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: _
```

You can configure other HTTP settings from this menu as shown following.

To	Do this
Configure an HTTP proxy	Enter **1**. You need to supply a host name and port to complete configuration.
View the current HTTP proxy configuration	Enter **2**. If an HTTP proxy isn't 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	Enter **3**. The message `HTTP Proxy Configuration Removed` is displayed.

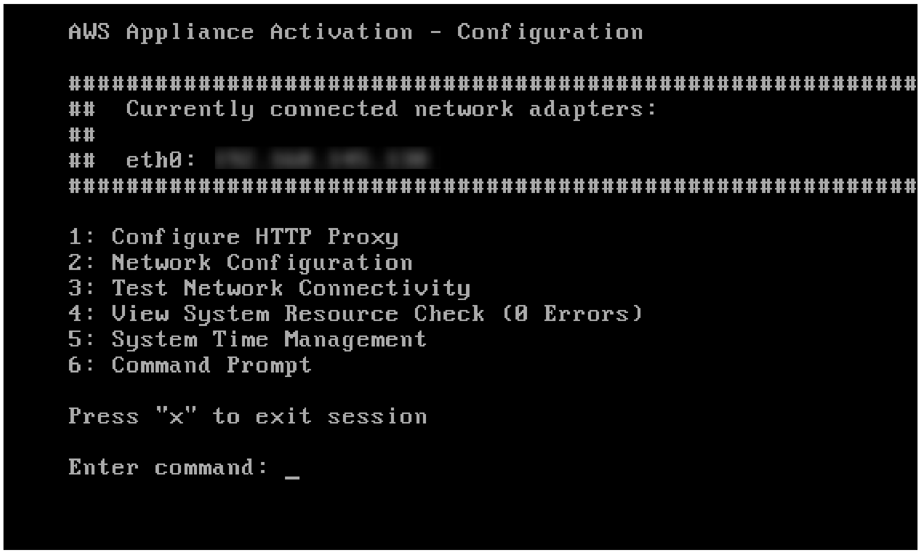
4. Restart your VM to apply your HTTP configuration settings.

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.

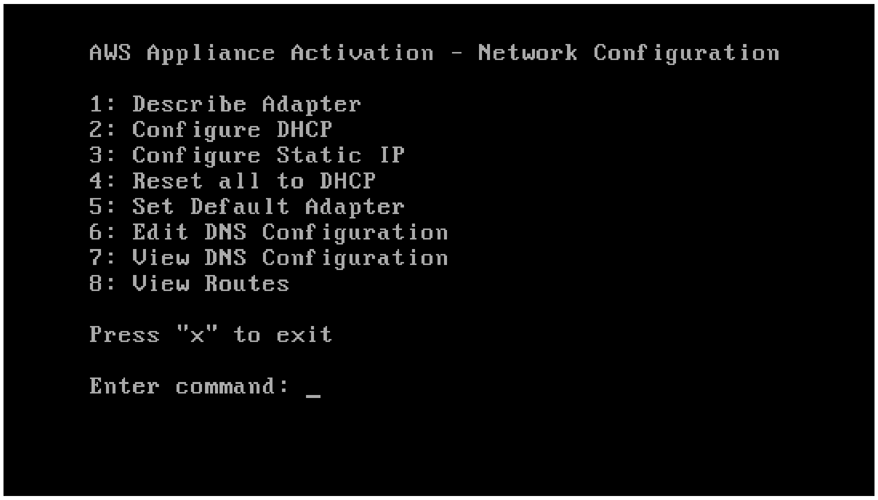
To configure your gateway to use static IP addresses

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. 91).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 89).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **2** to begin configuring your network.



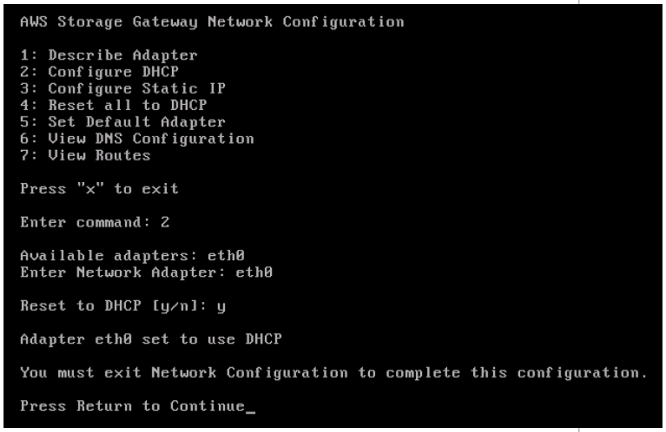
```
    AWS Appliance Activation - Configuration

    ###########################################################
    ##  Currently connected network adapters:
    ##
    ##  eth0: [redacted]
    ###########################################################

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

    Press "x" to exit session

    Enter command: _
```

3. On the **Network Configuration** menu, choose one of the following options.



```
AWS Appliance Activation - Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: Edit DNS Configuration
7: View DNS Configuration
8: View Routes

Press "x" to exit

Enter command: _
```

To	Do this
Get information about your network adapter	Enter `1`. 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 same adapter name when you configure a static IP address (option **3**) as when you set your gateway's default route adapter (option **5**).

To	Do this
Configure DHCP	Enter **2**. You are prompted to configure the network interface to use DHCP.  AWS Storage Gateway Network Configuration 1: Describe Adapter 2: Configure DHCP 3: Configure Static IP 4: Reset all to DHCP 5: Set Default Adapter 6: View DNS Configuration 7: View Routes Press "x" to exit Enter command: 2 Available adapters: eth0 Enter Network Adapter: eth0 Reset to DHCP [y/n]: y Adapter eth0 set to use DHCP You must exit Network Configuration to complete this configuration. Press Return to Continue_
Configure a static IP address for your gateway	Enter **3**. 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. 65). 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.

To	Do this
Reset all your gateway's network configuration to DHCP	Enter **4**. 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. 65).
Set your gateway's default route adapter	Enter **5**. 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 **6**. 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 **7**. 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 **8**. The default route of your gateway is displayed.

Testing your FSx File gateway connection to gateway endpoints

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

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.

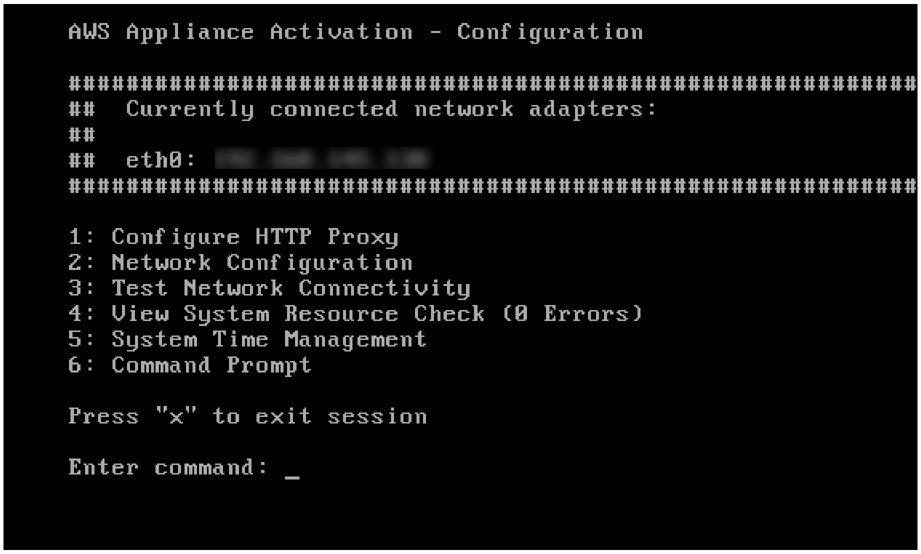
To view the status of a system resource check

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. 91).

- For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
- For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 89).

2. In the **AWS Appliance Activation - Configuration** main menu, enter **4** to view the results of a system resource check.



```
AWS Appliance Activation - Configuration

############################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
############################################################

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

Press "x" to exit session

Enter command: _
```

The console displays an **[OK**], **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
[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

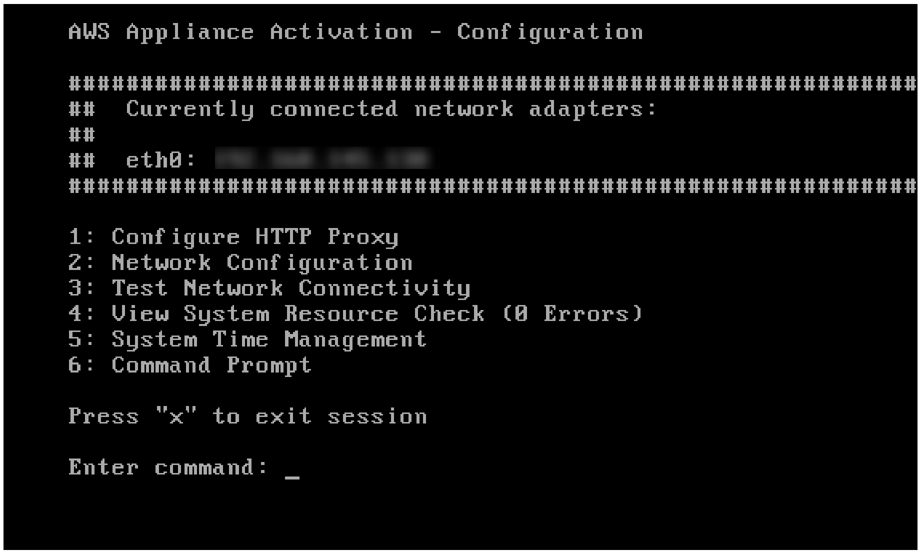
You can view and edit Network Time Protocol (NTP) server configurations and synchronize the VM time on your gateway with your hypervisor host.

To manage system time

1. Log in to your gateway's local console:

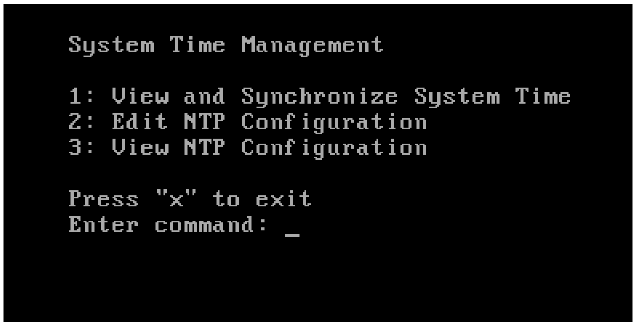
   - For more information on logging in to the VMware ESXi local console, see Accessing the Gateway Local Console with VMware ESXi (p. 91).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 89).

2. In the **AWS Appliance Activation - Configuration** main menu, enter **5** to manage your system's time.



```
    AWS Appliance Activation - Configuration

    ###########################################################
    ##  Currently connected network adapters:
    ##
    ##  eth0: [redacted]
    ###########################################################

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

    Press "x" to exit session

    Enter command: _
```

3. In the **System Time Management** menu, choose one of the following options.



```
    System Time Management

    1: View and Synchronize System Time
    2: Edit NTP Configuration
    3: View NTP Configuration

    Press "x" to exit
    Enter command: _
```

To	Do this
View and synchronize your VM time with NTP server time.	Enter **1**. 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.

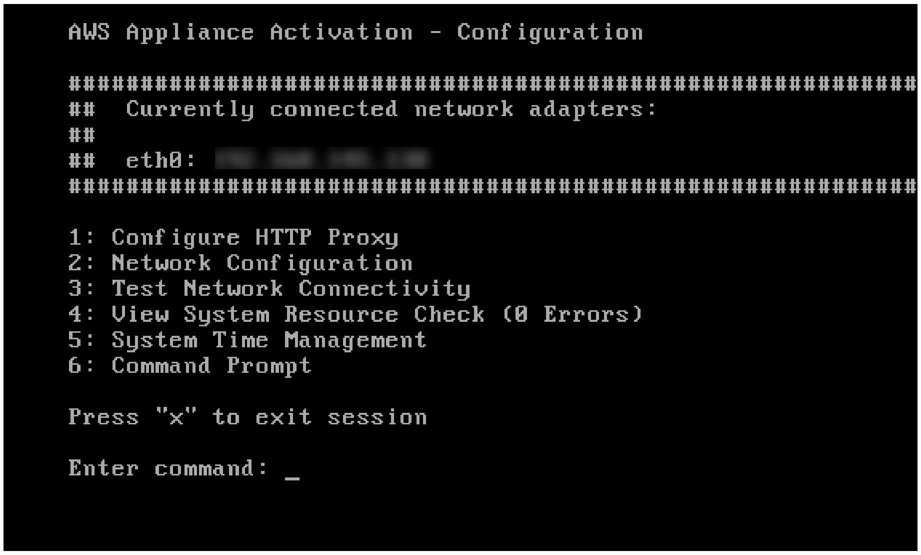
To	Do this
	For example, suppose that there is a prolonged network outage and your hypervisor host and gateway don't get time updates. In this case, the gateway VM's time is different from the true time. When there is a time drift, a discrepancy occurs between the stated times when operations such as 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. 152). 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. 156). 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 **2**. You are prompted to provide a preferred and a secondary NTP server.
View your NTP server configuration	Enter **3**. 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 Amazon Web Services Support, and so on.

To run a configuration or diagnostic command

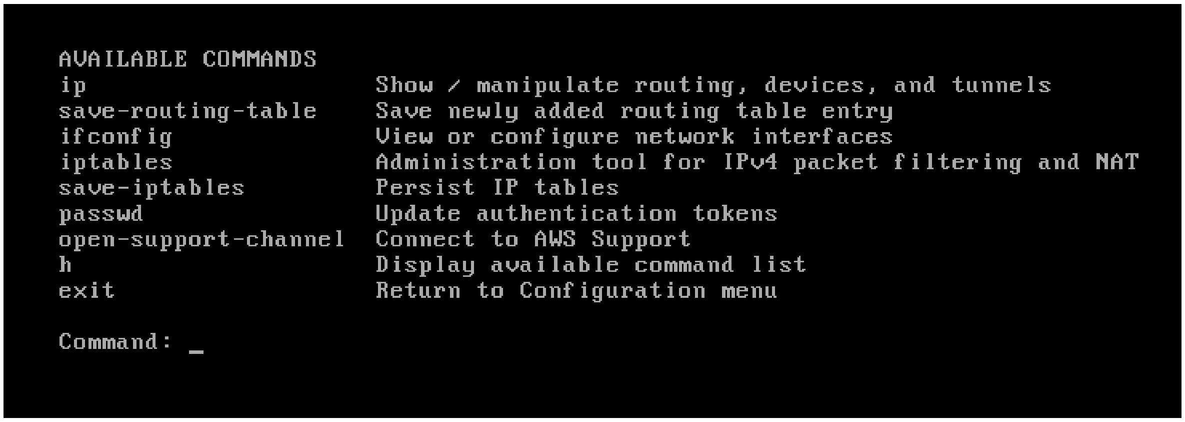
1. Log in to your gateway's local console:
   - For more information on logging in to the VMware ESXi local console, see Accessing the Gateway Local Console with VMware ESXi (p. 91).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - For more information on logging in to the KVM local console, see Accessing the Gateway Local Console with Linux KVM (p. 89).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **6** for **Command Prompt**.



```
AWS Appliance Activation - Configuration

###########################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
###########################################################

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

Press "x" to exit session

Enter command: _
```

3. On the **AWS Appliance Activation - Command Prompt** console, enter `h`, and then press the **Return** key.

   The console displays the **AVAILABLE COMMANDS** menu with what the commands do, as shown in the following screenshot.



```
AVAILABLE COMMANDS
ip                      Show / manipulate routing, devices, and tunnels
save-routing-table      Save newly added routing table entry
ifconfig                View or configure network interfaces
iptables                Administration tool for IPv4 packet filtering and NAT
save-iptables           Persist IP tables
passwd                  Update authentication tokens
open-support-channel    Connect to AWS Support
h                       Display available command list
exit                    Return to Configuration menu

Command: _
```

4. At the command prompt, enter the command that you want to use and follow the instructions.

To learn about a command, enter the command name at the command prompt.

Configuring network adapters for your gateway

By default, Storage Gateway is configured to use the E1000 network adapter type, but you can reconfigure your gateway to use the VMXNET3 (10 GbE) network adapter. You can also configure Storage Gateway so it can be accessed by more than one IP address. You do this by configuring your gateway to use more than one network adapter.

Topics

Configuring your gateway to use the VMXNET3 network adapter

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**.

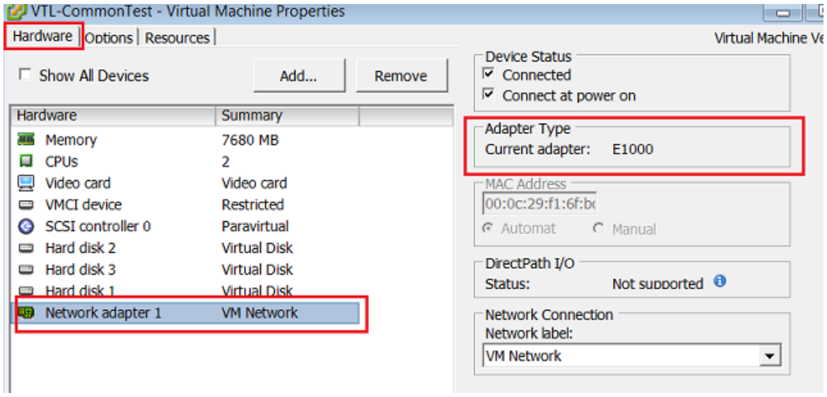
Following are the steps you take to configure your gateway to use the VMXNET3 adapter:

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.



VTL-CommonTest - Virtual Machine Properties

Hardware	Summary
Memory	7680 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	Paravirtual
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 1	Virtual Disk
Network adapter 1	VM Network

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:0c:29:f1:6f:bc
● Automat ○ Manual

DirectPath I/O
Status: Not supported

Network Connection
Network label:
VM Network

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.

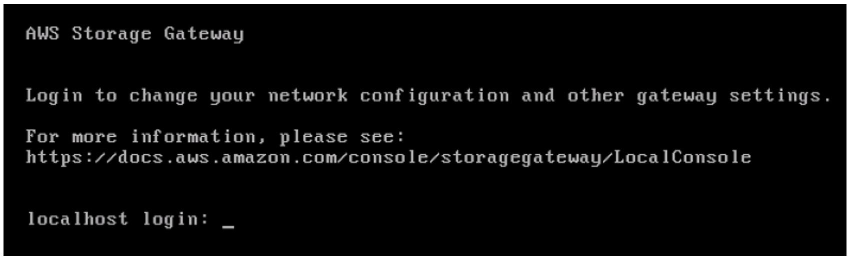
5. Choose **Add** to open the Add Hardware wizard.
6. Choose **Ethernet Adapter**, and then choose **Next**.
7. In the Network Enter wizard, select **`VMXNET3`** for **Adapter Enter**, and then choose **Next**.
8. In the Virtual Machine properties wizard, verify in the **Adapter Enter** section that **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.

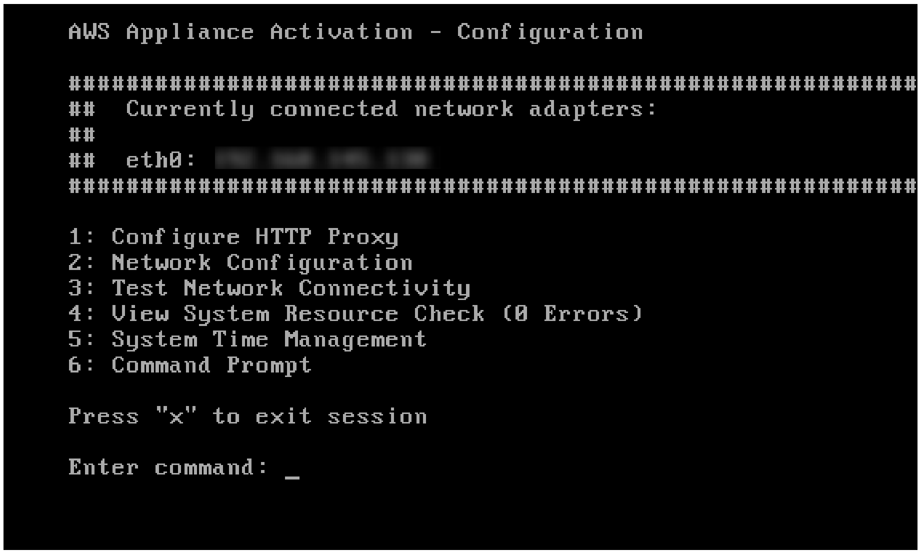
After your gateway restarts, reconfigure the adapter you just added to make sure that network connectivity to the internet is established.

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. 68).

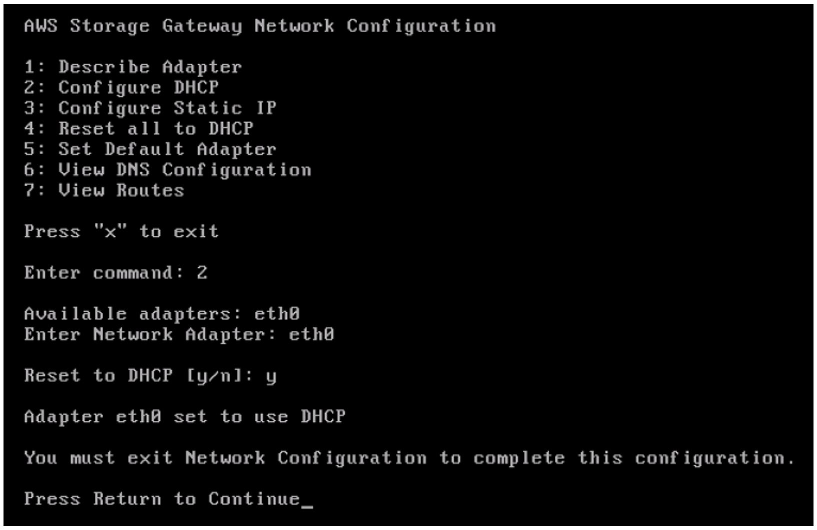


```
AWS Storage Gateway


Login to change your network configuration and other gateway settings.

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


localhost login: _
```



```
AWS Appliance Activation - Configuration

##############################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
##############################################################

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

Press "x" to exit session

Enter command: _
```

2. At the prompt, enter **`2`** to select **Network Configuration**, and then press **`Enter`** to open the network configuration menu.
3. At the prompt, enter **`4`** to select **Reset all to DHCP**, and then enter **`y`** (for yes) at the prompt to set all adapters to use Dynamic Host Configuration Protocol (DHCP). All available adapters are set to use DHCP.



```
AWS Storage Gateway Network Configuration

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

Press "x" to exit

Enter command: 2

Available adapters: eth0
Enter Network Adapter: eth0

Reset to DHCP [y/n]: y

Adapter eth0 set to use DHCP

You must exit Network Configuration to complete this configuration.

Press Return to Continue_
```

If your gateway is already activated, you must shut it down and restart it from the Storage Gateway Management Console. After the gateway restarts, you must test network connectivity to the internet. For information about how to test network connectivity, see Testing your FSx File gateway connection to gateway endpoints (p. 74).

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

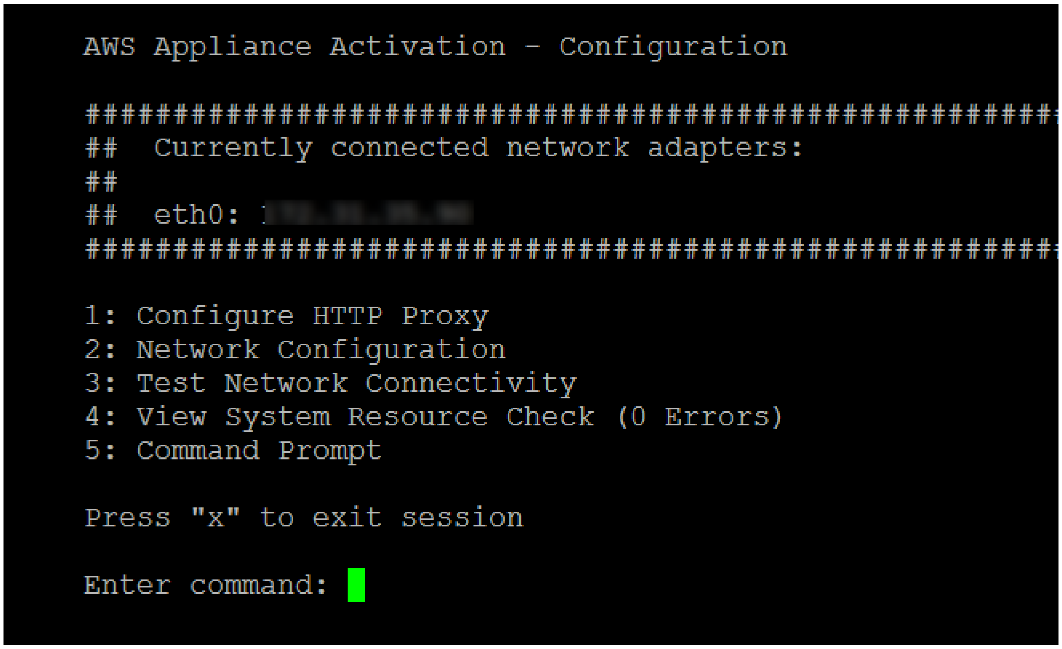
- Logging in to your Amazon EC2 gateway local console (p. 81)
- Routing your gateway deployed on EC2 through an HTTP proxy (p. 82)
- Configuring your gateway network settings (p. 84)
- Testing your gateway connectivity to the internet (p. 85)
- Viewing your gateway system resource status (p. 87)
- Running Storage Gateway commands on the local console (p. 88)

Logging in to your Amazon EC2 gateway local console

You can connect to your Amazon EC2 instance by using a Secure Shell (SSH) client. For detailed information, see Connect to your instance in the *Amazon EC2 User Guide*. To connect this way, you need the SSH key pair that you specified when you launched your instance. For information about Amazon EC2 key pairs, see Amazon EC2 key pairs in the *Amazon EC2 User Guide.*

To log in to the gateway local console

1. Log in to your local console. If you are connecting to your EC2 instance from a Windows computer, log in as *admin*.
2. After you log in, you see the **AWS Appliance Activation - Configuration** main menu, as shown in the following screenshot.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

To Learn About This	See This Topic
Configure an HTTP proxy for your gateway	Routing your gateway deployed on EC2 through an HTTP proxy (p. 82)
Configure network settings for your gateway	Testing your gateway connectivity to the internet (p. 85)
Test network connectivity	Testing your gateway connectivity to the internet (p. 85)
View a system resource check	Logging in to your Amazon EC2 gateway local console (p. 81).
Run Storage Gateway console commands	Running Storage Gateway commands on the local console (p. 88)

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

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

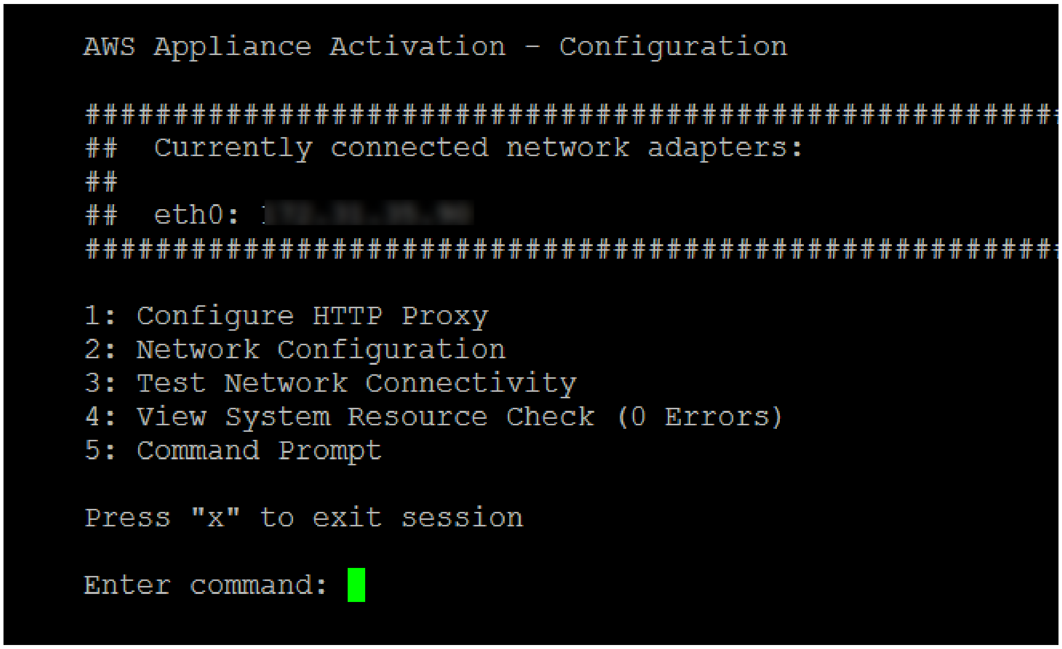
Routing your gateway deployed on EC2 through an HTTP proxy

Storage Gateway supports the configuration of a Socket Secure version 5 (SOCKS5) proxy between your gateway deployed on Amazon EC2 and AWS.

If your gateway must use a proxy server to communicate to the internet, then you need to configure the HTTP proxy settings for your gateway. You do this by specifying an IP address and port number for the host running your proxy. After you do so, Storage Gateway routes all AWS endpoint traffic through your proxy server. Communications between the gateway and endpoints is encrypted, even when using the HTTP proxy.

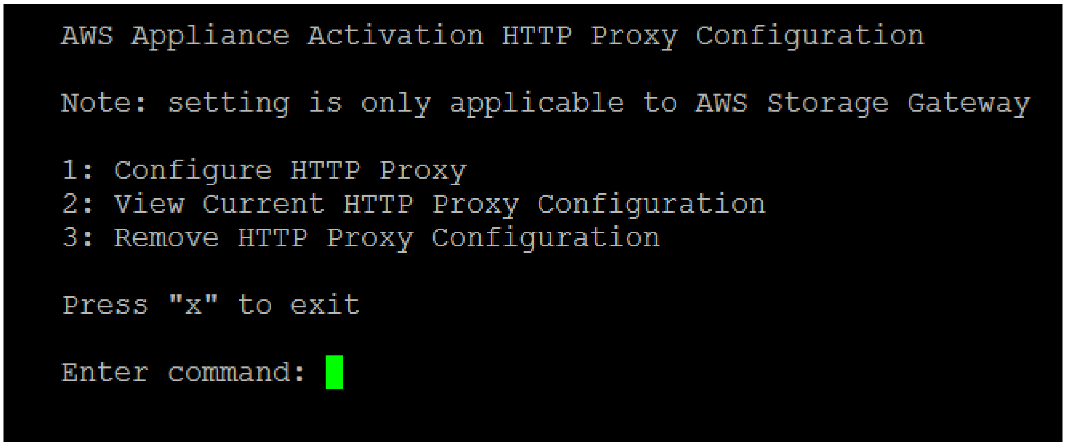
To route your gateway internet traffic through a local proxy server

1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 81).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **1** to begin configuring the HTTP proxy.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

3. Choose one of the following options in the **AWS Appliance Activation - Configuration HTTP Proxy Configuration** menu.



```
AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command:
```

To	Do This
Configure an HTTP proxy	Enter **1**. You need to supply a host name and port to complete configuration.
View the current HTTP proxy configuration	Enter **2**.

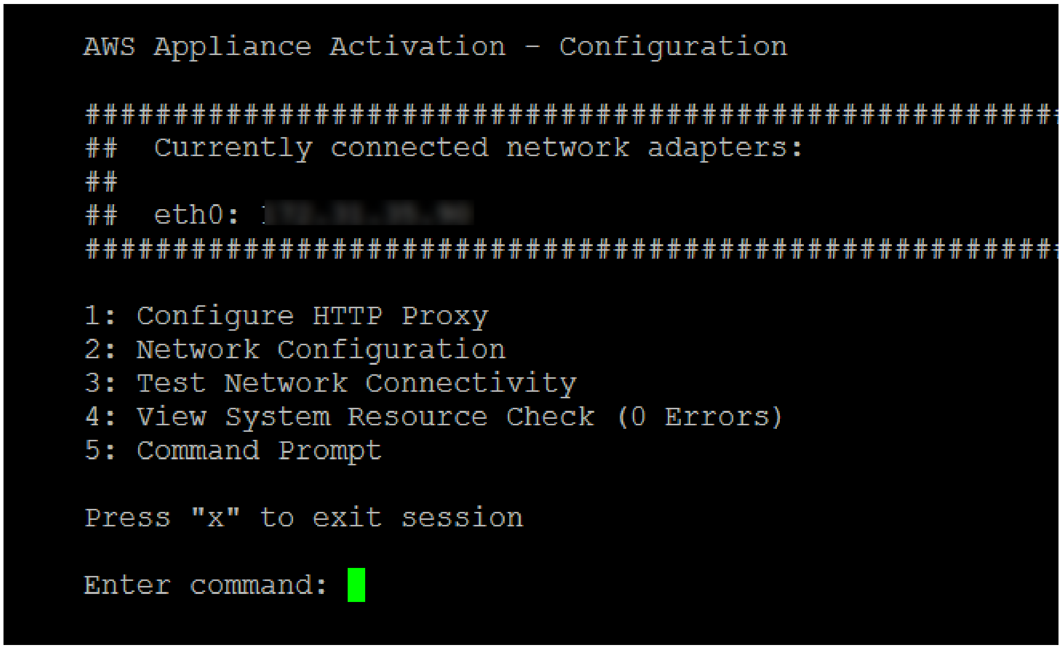
To	Do This
	If an HTTP proxy is not configured, the message `HTTP Proxy not configured` is displayed. If an HTTP proxy is configured, the host name and port of the proxy are displayed.
Remove an HTTP proxy configuration	Enter **3**. The message `HTTP Proxy Configuration Removed` is displayed.

Configuring your gateway network settings

You can view and configure your Domain Name Server (DNS) settings through the local console.

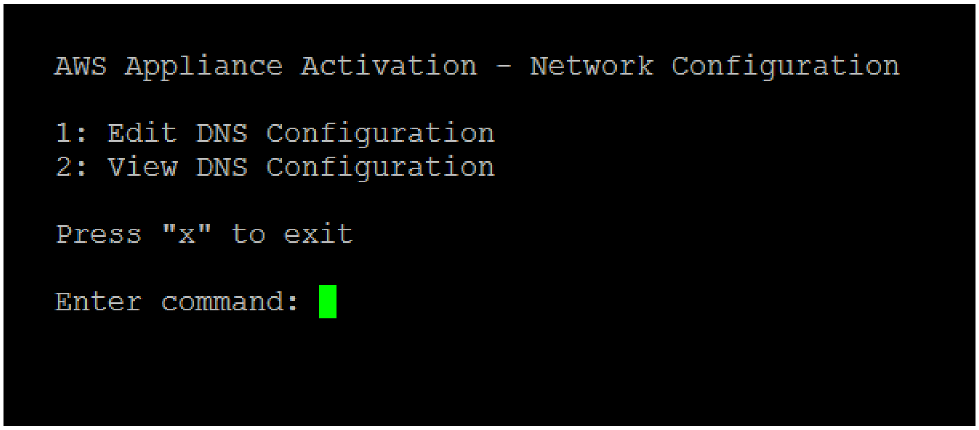
To configure your gateway to use static IP addresses

1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 81).
2. On the **AWS Appliance Activation - Configuration** main menu, enter **2** to begin configuring your DNS server.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

3. On the **Network Configuration** menu, choose one of the following options.



```
AWS Appliance Activation - Network Configuration

1: Edit DNS Configuration
2: View DNS Configuration

Press "x" to exit

Enter command:
```

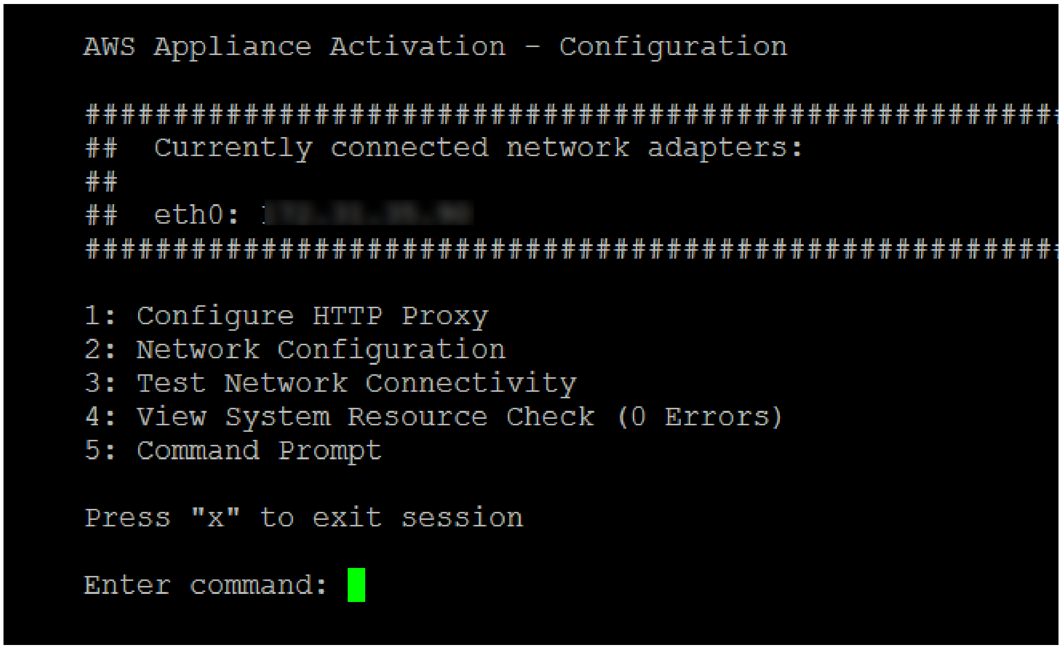
To	Do This
Edit your gateway's DNS configuration	Enter **1**. The available adapters of the primary and secondary DNS servers are displayed. You are prompted to provide the new IP address.
View your gateway's DNS configuration	Enter **2**. The available adapters of the primary and secondary DNS servers are displayed.

Testing your gateway connectivity to the internet

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

To test your gateway's connection to the internet

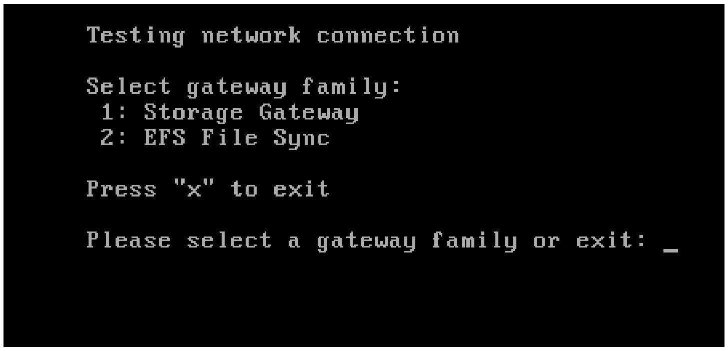
1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 81).
2. In the **Storage Gateway Configuration** main menu, enter **3** to begin testing network connectivity.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

The console displays the available AWS Regions.

3. Choose option **1** for Storage Gateway.



```
Testing network connection

Select gateway family:
 1: Storage Gateway
 2: EFS File Sync

Press "x" to exit

Please select a gateway family or exit: _
```

The console displays the available AWS Regions for Storage Gateway.

4. Choose the AWS Region that you want to test. For example, us-east-2. For supported AWS Regions and a list of AWS service endpoints you can use with Storage Gateway, see Storage Gateway endpoints and quotas in the *AWS General Reference*.

   Each endpoint in the AWS Region that you choose displays either a **[PASSED]** or **[FAILED]** message, as shown following.

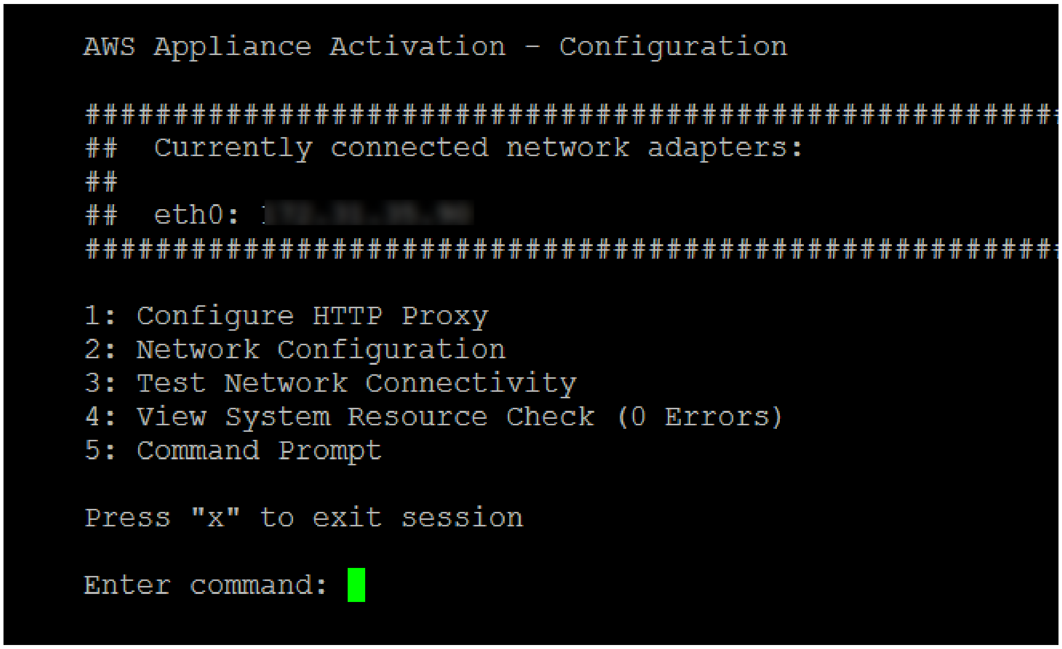
Message	Description
[PASSED]	Storage Gateway has internet connectivity.
[FAILED]	Storage Gateway does not have internet connectivity.

Viewing your gateway system resource status

When your gateway starts, it checks its virtual CPU cores, root volume size, and RAM. It then determines whether these system resources are sufficient for your gateway to function properly. You can view the results of this check on the gateway's local console.

To view the status of a system resource check

1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 81).
2. In the **Storage Gateway Configuration** main menu, enter **4** to view the results of a system resource check.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

The console displays an **[OK**], **[WARNING]**, or **[FAIL]** message for each resource as described in the table following.

Message	Description
[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.

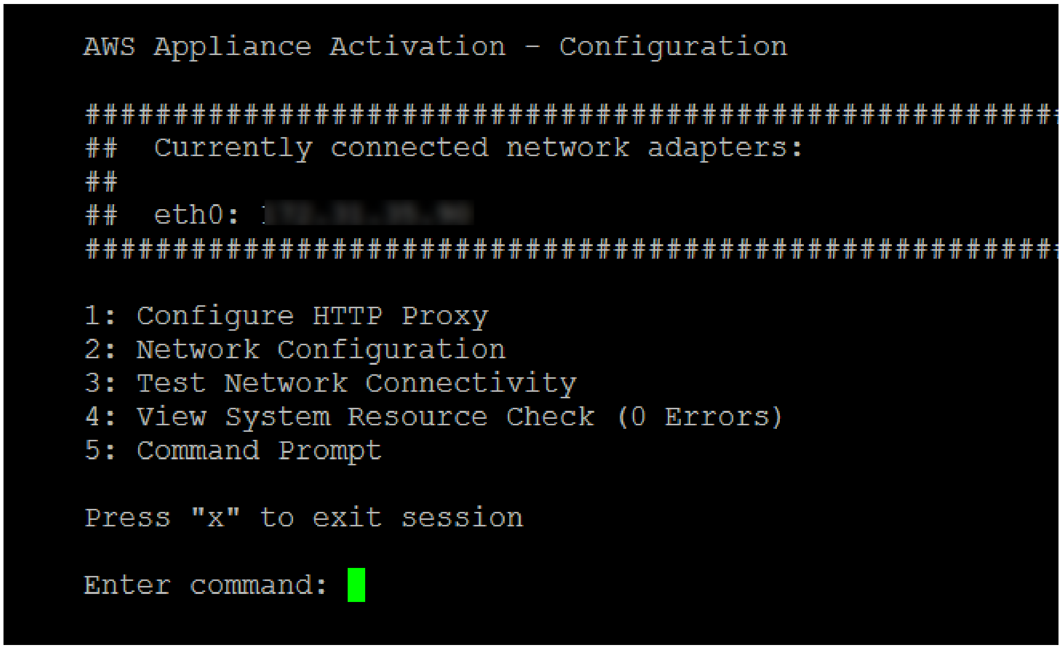
The console also displays the number of errors and warnings next to the resource check menu option.

Running Storage Gateway commands on the local console

The 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 Amazon Web Services Support.

To run a configuration or diagnostic command

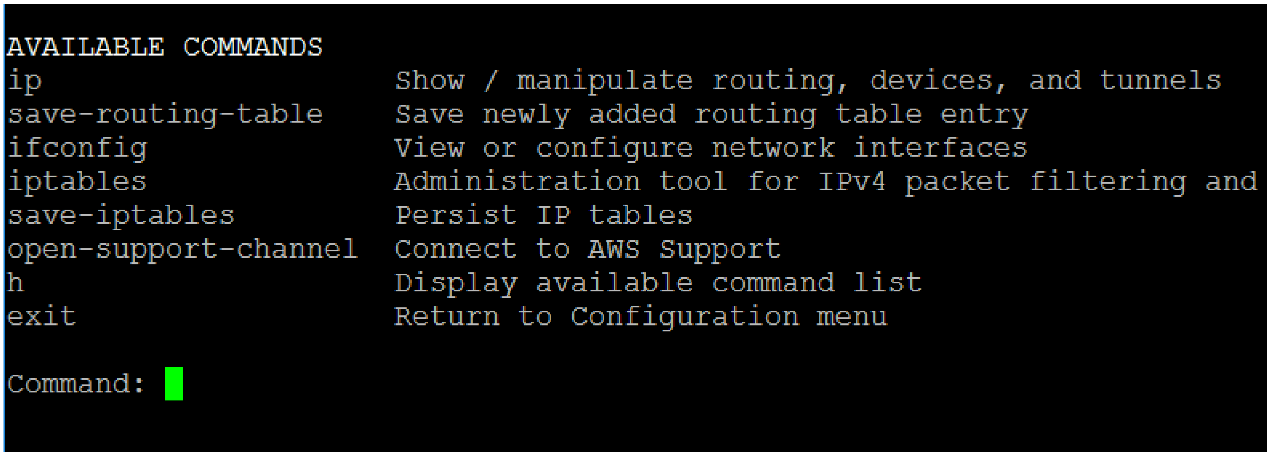
1. Log in to your gateway's local console. For instructions, see Logging in to your Amazon EC2 gateway local console (p. 81).
2. In the **AWS Appliance Activation Configuration** main menu, enter **5** for **Gateway Console**.



```
AWS Appliance Activation - Configuration

#######################################################
##  Currently connected network adapters:
##
##  eth0: [redacted]
#######################################################

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command:
```

3. In the command prompt, enter **h**, and then press the **Return** key.

   The console displays the **AVAILABLE COMMANDS** menu with the available commands. After the menu, a gateway console prompt appears, as shown in the following screenshot.



```
AVAILABLE COMMANDS
ip                      Show / manipulate routing, devices, and tunnels
save-routing-table      Save newly added routing table entry
ifconfig                View or configure network interfaces
iptables                Administration tool for IPv4 packet filtering and
save-iptables           Persist IP tables
open-support-channel    Connect to AWS Support
h                       Display available command list
exit                    Return to Configuration menu

Command:
```

4. At the command prompt, enter the command that you want to use and follow the instructions.

To learn about a command, enter the command name at the command prompt.

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

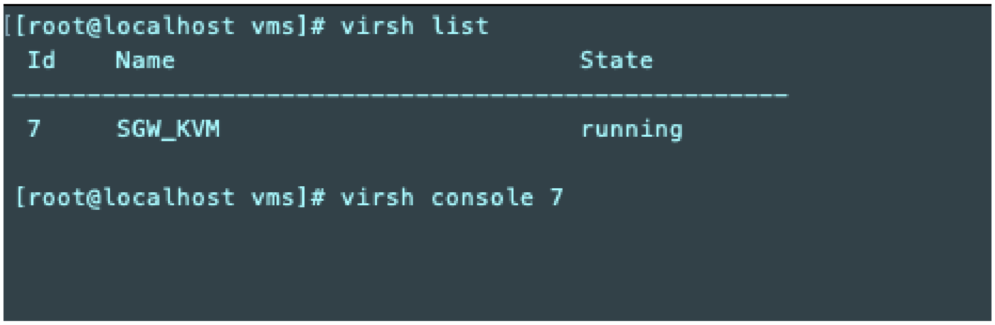
There are different ways to configure virtual machines running on KVM, depending on the Linux distribution being used. Instructions for accessing KVM configuration options from the command line follow. Instructions might differ depending on your KVM implementation.

To access your gateway's local console with KVM

1. Use the following command to list the VMs that are currently available in KVM.

```
# virsh list
```

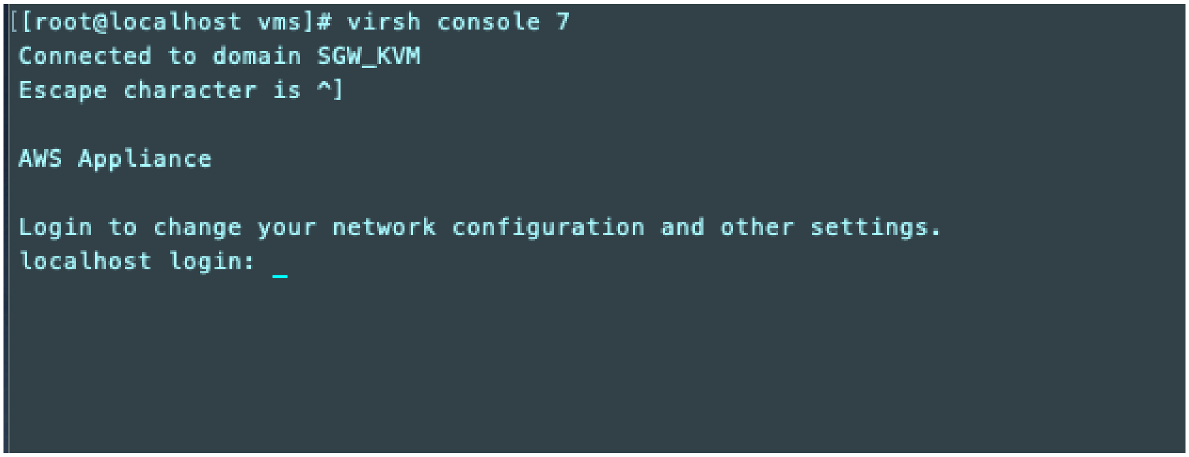
   You can choose available VMs by `Id`.



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

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

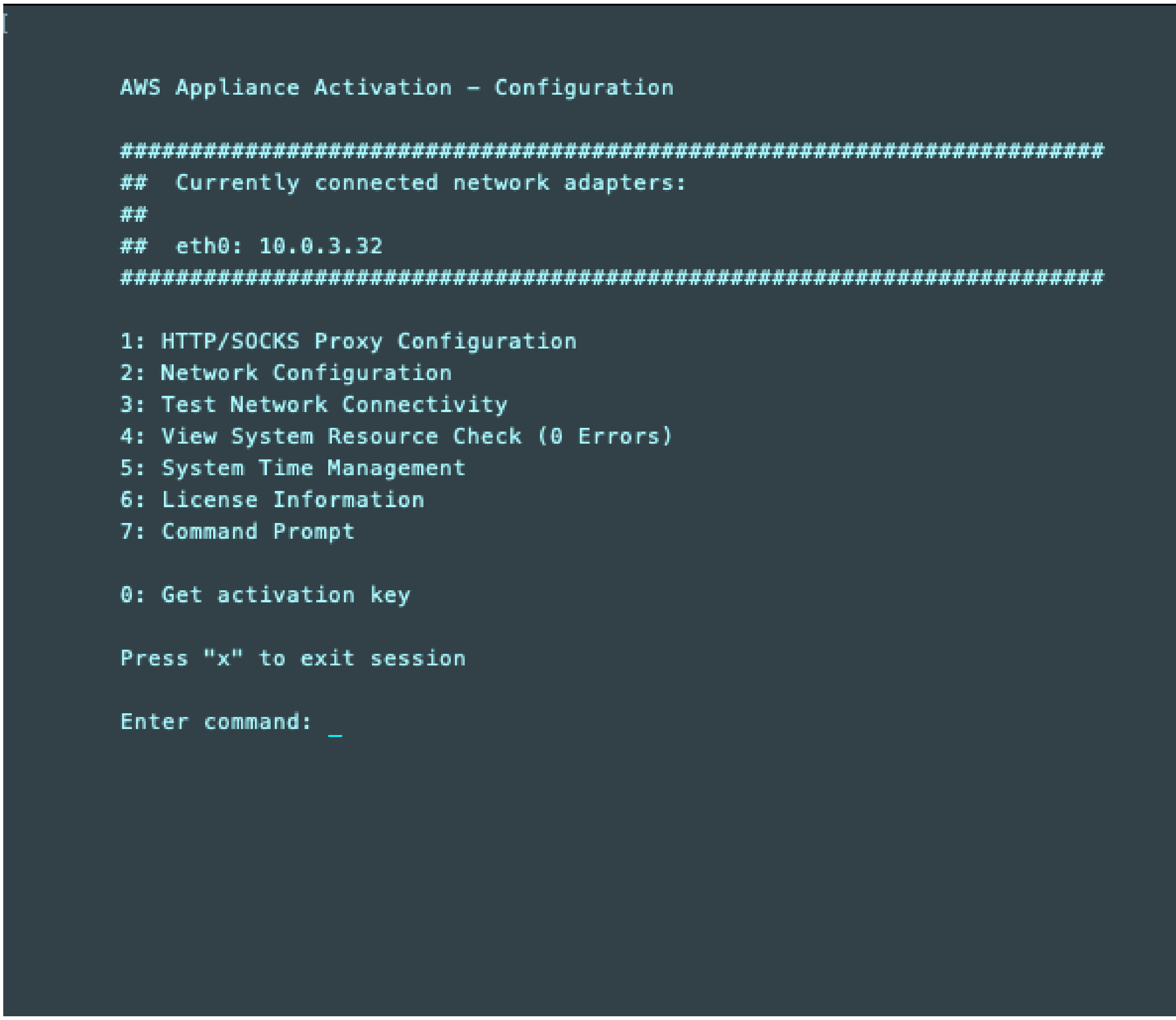
2. Use the following command to access the local console.

```
# virsh console VM_Id
```



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

 AWS Appliance

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

3. To get default credentials to log in to the local console, see Logging in to the file gateway local console (p. 68).
4. After you have logged in, you can activate and configure your gateway.



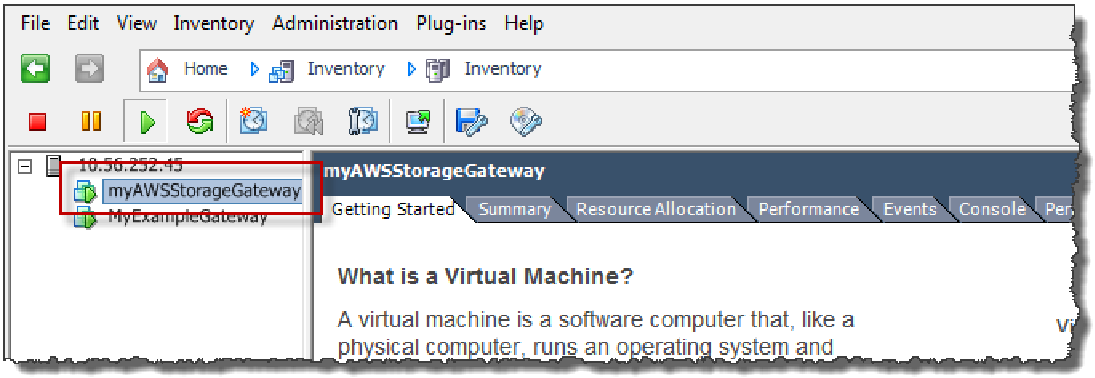
```
[


        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.

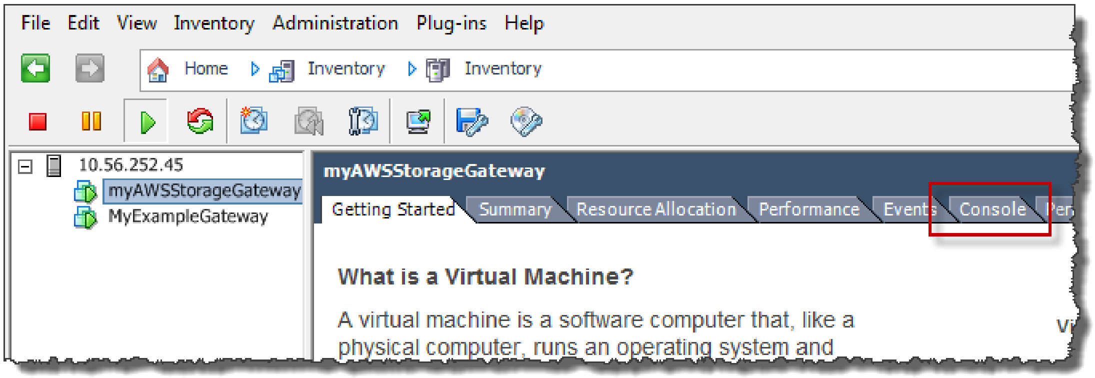
   Note
   If your gateway VM is turned on, a green arrow icon appears with the VM icon, as shown in the following screenshot. If your gateway VM is not turned on, you can turn it on by choosing the green **Power On** icon on the **Toolbar** menu.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and

3. Choose the **Console** tab.

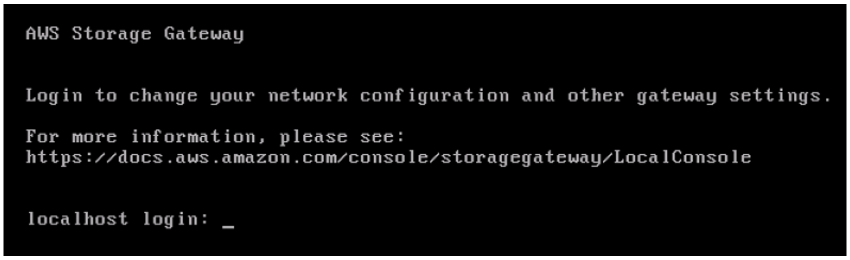


What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and

After a few moments, the VM is ready for you to log in.

Note
To release the cursor from the console window, press **Ctrl+Alt**.



```
AWS Storage Gateway


Login to change your network configuration and other gateway settings.

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


localhost login: _
```

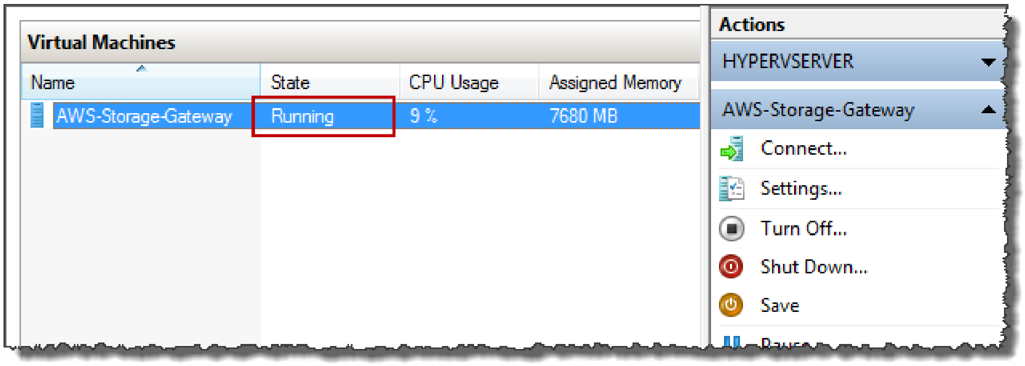
4. To log in using the default credentials, continue to the procedure Logging in to the file gateway local console (p. 68).

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.

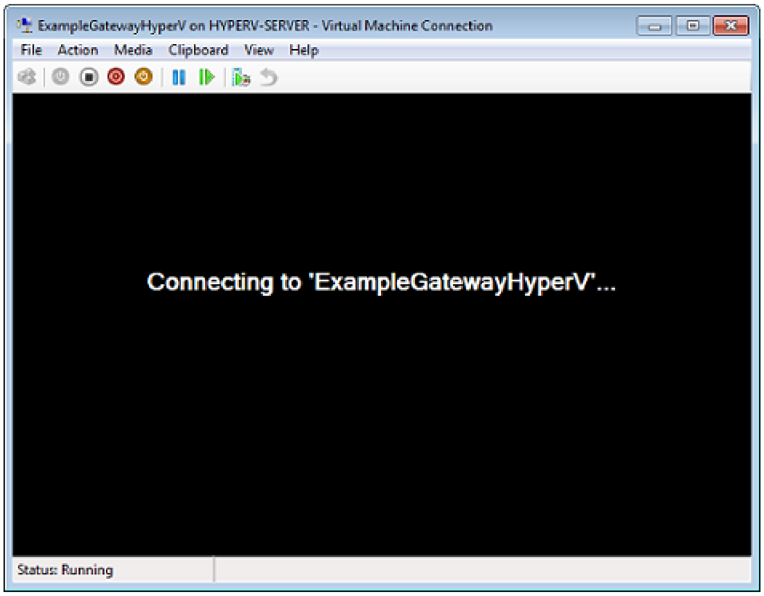


Virtual Machines

Name	State	CPU Usage	Assigned Memory
AWS-Storage-Gateway	Running	9 %	7680 MB

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.

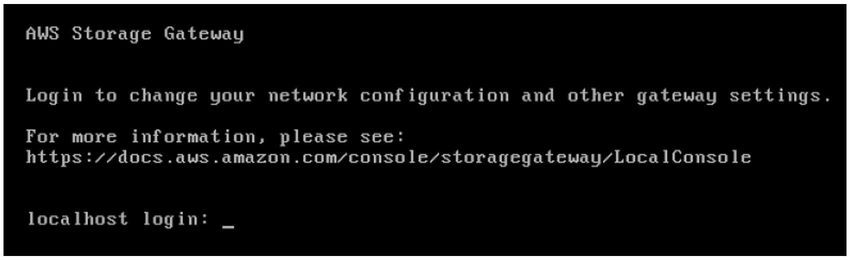


ExampleGatewayHyperV on HYPERV-SERVER - Virtual Machine Connection

Connecting to 'ExampleGatewayHyperV'...

Status: Running

After a few moments, the VM is ready for you to log in.



```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

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


localhost login: _
```

4. To log in using the default credentials, continue to the procedure Logging in to the file gateway local console (p. 68).

Configuring Network Adapters for Your Gateway

In this section you can find information about how configure multiple network adapters for your gateway.

Topics

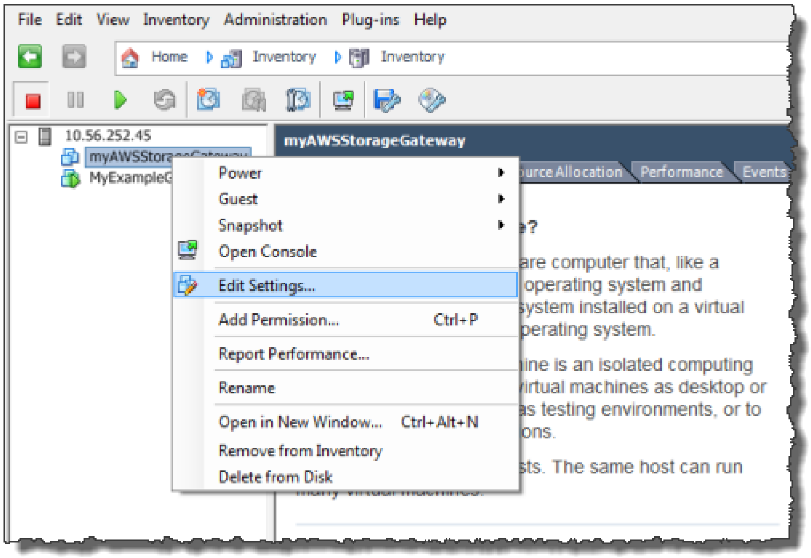
Configuring Your Gateway for Multiple NICs in a VMware ESXi Host

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.

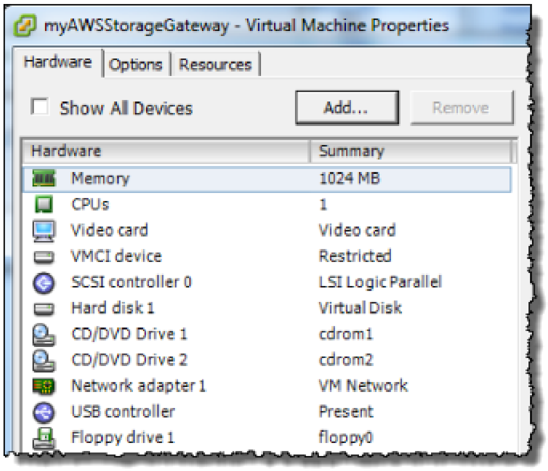
To configure your gateway to use an additional network adapter in VMware ESXi host

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**.



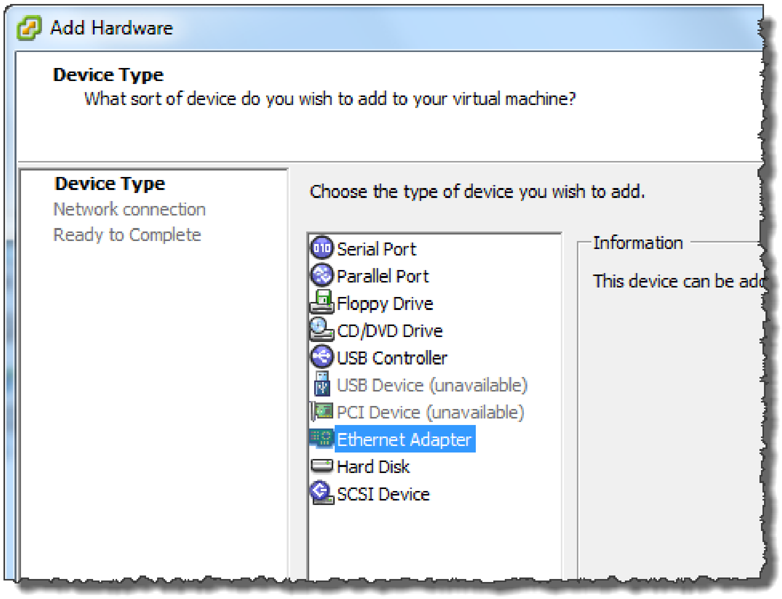
4. On the **Hardware** tab of the **Virtual Machine Properties** dialog box, choose **Add** to add a device.



Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD Drive 1	cdrom1
CD/DVD Drive 2	cdrom2
Network adapter 1	VM Network
USB controller	Present
Floppy drive 1	floppy0

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**.



Add Hardware

Device Type
What sort of device do you wish to add to your virtual machine?

Device Type
Network connection
Ready to Complete

Choose the type of device you wish to add.

Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device

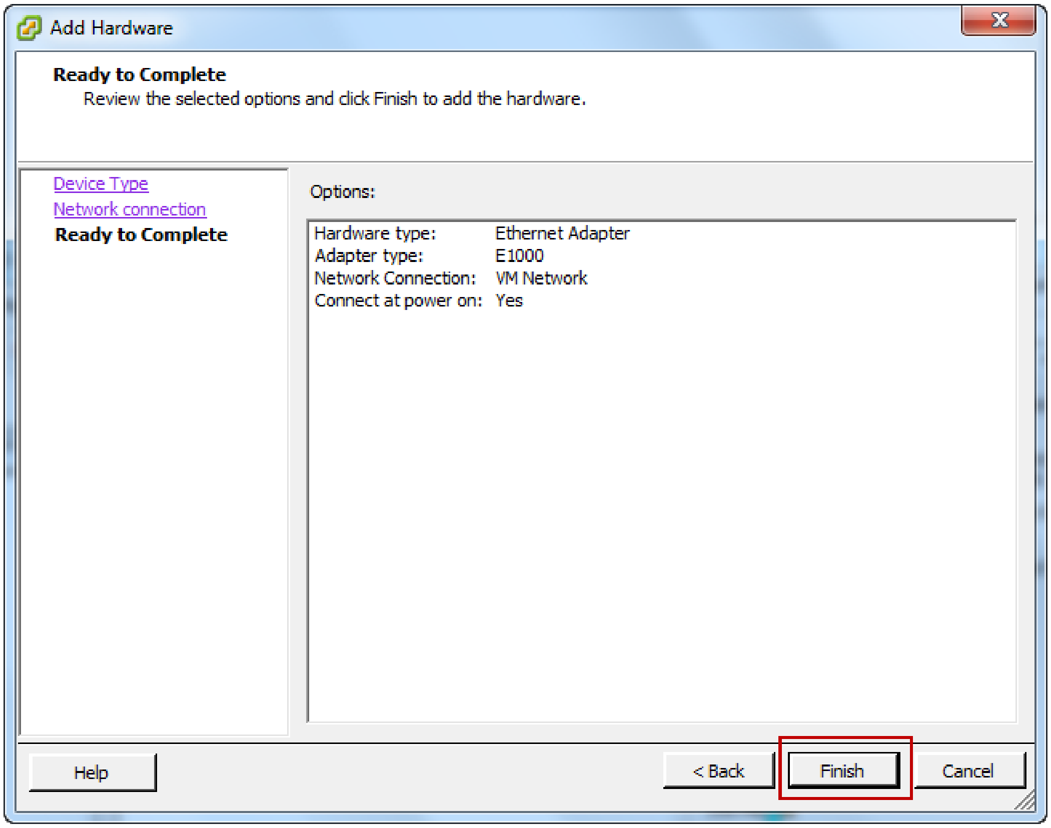
Information

This device can be add

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**.



Add Hardware

Ready to Complete

Review the selected options and click Finish to add the hardware.

Options:

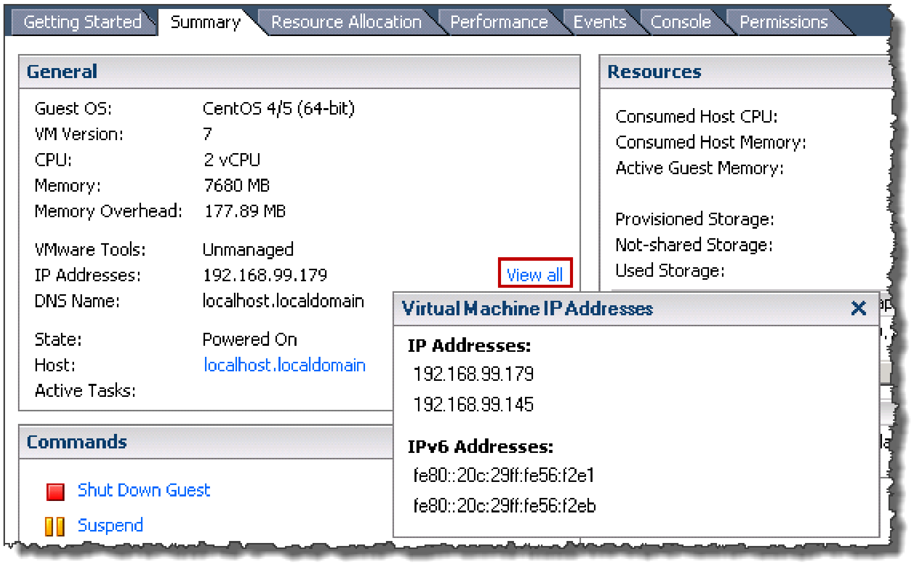
Hardware type: Ethernet Adapter
Adapter type: E1000
Network Connection: VM Network
Connect at power on: Yes

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.



General

Guest OS: CentOS 4/5 (64-bit)
VM Version: 7
CPU: 2 vCPU
Memory: 7680 MB
Memory Overhead: 177.89 MB

VMware Tools: Unmanaged
IP Addresses: 192.168.99.179
DNS Name: localhost.localdomain

State: Powered On
Host: localhost.localdomain
Active Tasks:

Commands

Resources

Consumed Host CPU:
Consumed Host Memory:
Active Guest Memory:

Provisioned Storage:
Not-shared Storage:
Used Storage:

Virtual Machine IP Addresses

IP Addresses:
192.168.99.179
192.168.99.145

IPv6 Addresses:
fe80::20c:29ff:fe56:f2e1
fe80::20c:29ff:fe56:f2eb

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.

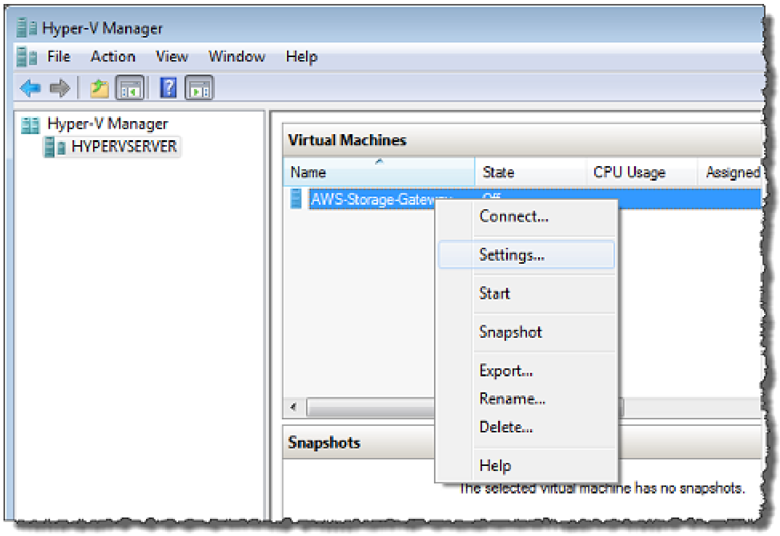
For information about local console tasks common to VMware, Hyper-V, and KVM hosts, see Performing tasks on the VM local console (file gateway) (p. 67)

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**.

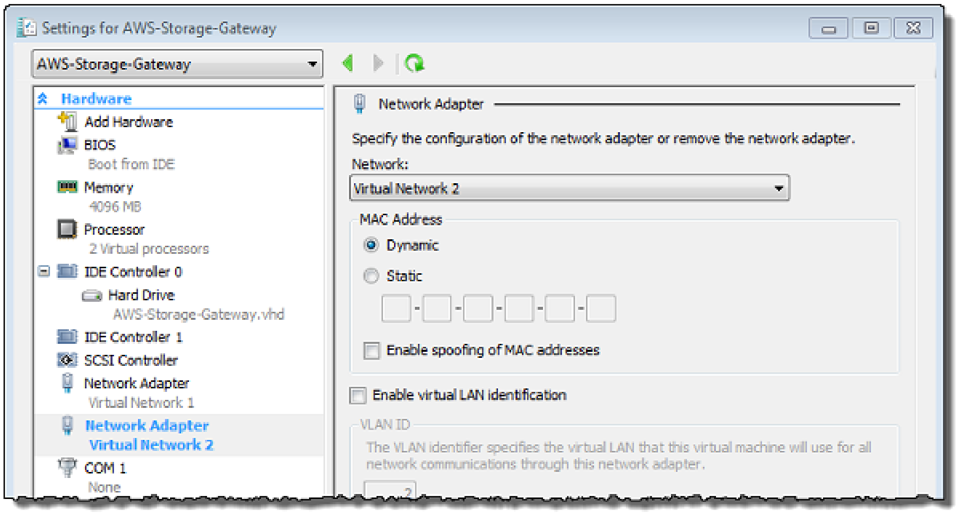


The selected virtual machine has no snapshots.

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.



Specify the configuration of the network adapter or remove the network adapter.

Network: Virtual Network 2

MAC Address

● Dynamic

○ Static

□ Enable spoofing of MAC addresses

□ Enable virtual LAN identification

VLAN ID

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network 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.

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. 67)

Deleting Your Gateway by Using the 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 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 *Storage Gateway API Reference*.

Topics

Deleting Your Gateway by Using the Storage Gateway Console

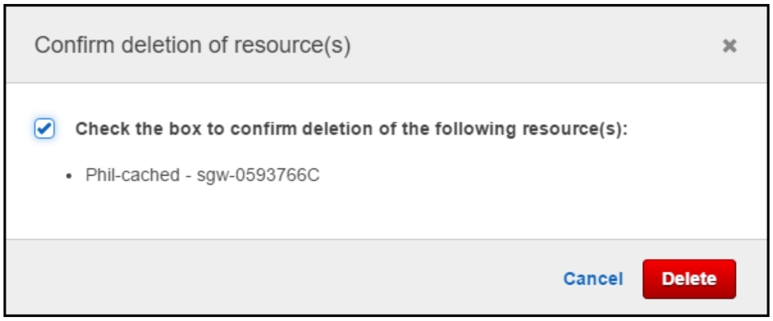
The procedure for deleting a gateway is the same for all gateway types. However, depending on the type of gateway you want to delete and the host the gateway is deployed on, you might have to perform additional tasks to remove resources associated with the gateway. Removing these resources helps you 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**.



Confirm deletion of resource(s)

☑ Check the box to confirm deletion of the following resource(s):

- Phil-cached - sgw-0593766C

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. 99).
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*.

Performance

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

Topics

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. 66).

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. 58).

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

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.

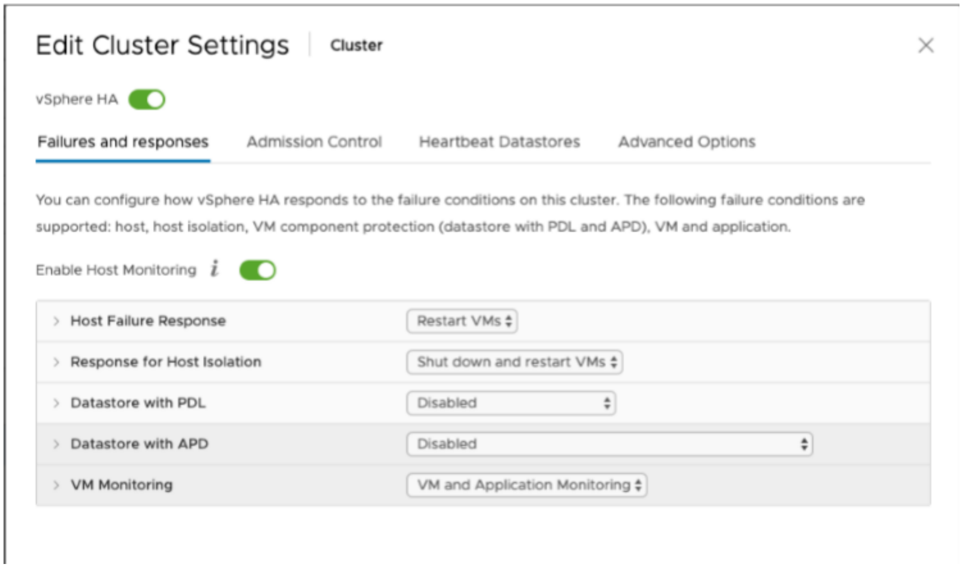
Next, configure your VMware cluster to work with Storage Gateway.

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.



You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring

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

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. 105).

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

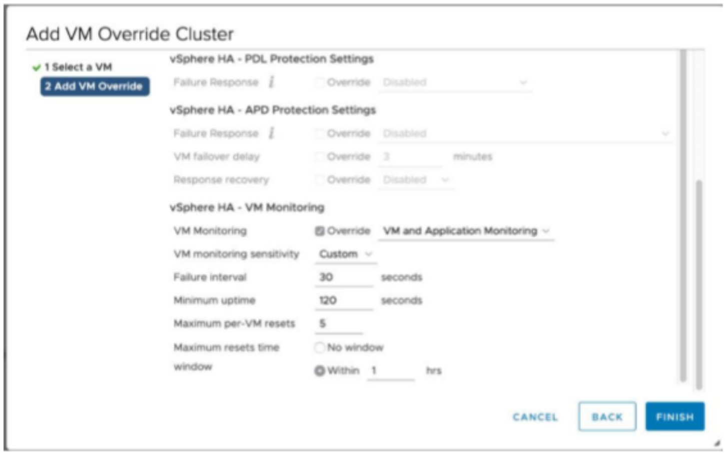
If you have other VMs running on your cluster, you might want to set the cluster values specifically for each VM.

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.



Add VM Override Cluster

✓ 1 Select a VM
2 Add VM Override

vSphere HA - PDL Protection Settings

Failure Response □ Override Disabled

vSphere HA - APD Protection Settings

Failure Response □ Override Disabled

VM failover delay □ Override 3 minutes

Response recovery □ Override Disabled

vSphere HA - VM Monitoring

VM Monitoring ☑ Override VM and Application Monitoring

VM monitoring sensitivity Custom

Failure interval 30 seconds

Minimum uptime 120 seconds

Maximum per-VM resets 5

Maximum resets time window ○ No window ● Within 1 hrs

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. 58).

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

The AWS shared responsibility model applies to data protection in AWS Storage Gateway. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.

- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Storage Gateway or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Data encryption using AWS KMS

Storage Gateway uses SSL/TLS (Secure Socket Layers/Transport Layer Security) to encrypt data that is transferred between your gateway appliance and AWS storage. By default, Storage Gateway uses Amazon S3-Managed encryption keys (SSE-S3) to server-side encrypt all data it stores in Amazon S3. You have an option to use the Storage Gateway API to configure your gateway to encrypt data stored in the cloud using server-side encryption with AWS Key Management Service (SSE-KMS) customer master keys (CMKs).

> **Important**
> When you use an AWS KMS CMK for server-side encryption, you must choose a symmetric CMK. Storage Gateway does not support asymmetric CMKs. For more information, see Using symmetric and asymmetric keys in the *AWS Key Management Service Developer Guide*.

Encrypting a file share

For a file share, you can configure your gateway to encrypt your objects with AWS KMS–managed keys by using SSE-KMS. For information on using the Storage Gateway API to encrypt data written to a file share, see CreateNFSFileShare in the *Storage Gateway API Reference*.

Encrypting a file system

For information see, Data Encryption in Amazon FSxin the *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 CMK or revoke the grant token, you can't access the data on the volume or tape. For more information, see Deleting customer master keys in the *AWS Key Management Service Developer Guide*.
- If you create a snapshot from a volume that is KMS-encrypted, the snapshot is encrypted. The snapshot inherits the volume's KMS key.
- If you create a new volume from a snapshot that is KMS-encrypted, the volume is encrypted. You can specify a different KMS key for the new volume.

  > **Note**
  > Storage Gateway doesn't support creating an unencrypted volume from a recovery point of a KMS-encrypted volume or a KMS-encrypted snapshot.

For more information about AWS KMS, see What is AWS Key Management Service?

Authentication and access control for Storage Gateway

Access to 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

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. 111)
- Identity-based policies (IAM policies) (p. 112)

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

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 system ARN	`arn:aws:fsx:region:account-id:file-system/filesystem-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 *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. 122).

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)

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. 114). 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. 122)), 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. 111).
- **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. 122).

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. 111).

The sections in this topic cover the following:

- Permissions required to use the Storage Gateway console (p. 115)
- AWS managed policies for Storage Gateway (p. 116)
- Customer managed policy examples (p. 116)

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. 117).

  > **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. 122).

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. 117).

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 Storage Gateway resources.
- **AWSStorageGatewayFullAccess** – Grants full access to 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 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. 115).

> **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

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 Storage Gateway console, you must also grant permissions to allow the `ListGateways` action, as shown in the following example.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/
volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Example 5: Allow all actions on gateways with a specific prefix

The following policy allows a user to perform all Storage Gateway actions on gateways with names that start with `DeptX`. The policy also allows the `DescribeSnapshots` Amazon EC2 action which is required if you plan to describe snapshots.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

The preceding policy works if the user to whom the policy is attached uses either the API or an AWS SDK to access the gateway. However, if this user plans to use the Storage Gateway console, you must grant additional permissions as described in Example 3: Allow access to a specific gateway (p. 118).

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"
            }
         }
      }
   ]
}
```

Storage Gateway API permissions: Actions, resources, and conditions reference

When you set up access control (p. 110) 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. 111).

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. 110)
- Customer managed policy examples (p. 116)

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 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.

Security best practices for Storage Gateway

AWS Storage Gateway provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions. For more information, see AWS Security Best Practices.

Troubleshooting your gateway

Following, you can find information about troubleshooting issues related to gateways, file shares, volumes, virtual tapes, and snapshots. The on-premises gateway troubleshooting information covers gateways deployed on both the VMware ESXi and Microsoft Hyper-V clients. The troubleshooting information for file shares applies to the Amazon S3 File Gateway type. The troubleshooting information for volumes applies to the volume gateway type. The troubleshooting information for tapes applies to the tape gateway type. The troubleshooting information for gateway issues applies to using CloudWatch metrics. The troubleshooting information for high availability issues covers gateways running on VMware vSphere High Availability (HA) platform.

Topics

Troubleshooting on-premises gateway issues

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

Issue	Action to Take
	endpoints for outbound communication to AWS. For more information about network and firewall requirements, see Network and firewall requirements (p. 7).
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 FSx File gateway connection to gateway endpoints (p. 74). • 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. 75). • 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. 5).
You need to remove a disk allocated as upload buffer space. For example, you might want to reduce the amount of upload buffer space for a gateway, or you might need to replace a disk used as an upload buffer that has failed.	
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. 102). 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. 65). 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 FSx File gateway connection to gateway endpoints (p. 74). • 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. 78) 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. 102).
You are having trouble importing (deploying) Storage Gateway on Microsoft Hyper-V.	See Troubleshooting Microsoft Hyper-V setup (p. 139), 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

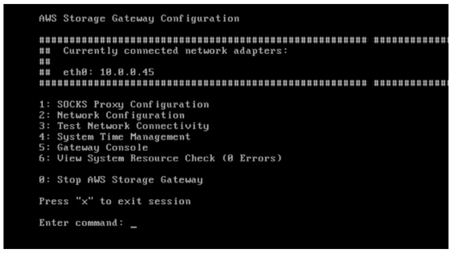
Storage Gateway provides a local console you can use to perform several maintenance tasks, including enabling AWS Support to access your gateway to assist you with troubleshooting gateway issues. By default, AWS Support access to your gateway is disabled. You enable this access through the host's local 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. 91).
- Microsoft Hyper-V – for more information, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).

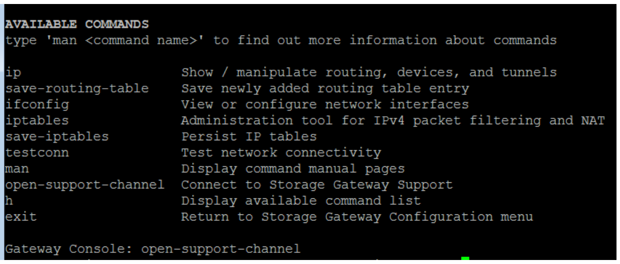
The local console looks like the following.



```
AWS Storage Gateway Configuration

########################################################## #############
##  Currently connected network adapters:
##
##  eth0: 10.0.0.45
########################################################## #############

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

2. At the prompt, enter **`5`** to open the AWS Support Channel console.
3. Enter **`h`** to open the **AVAILABLE COMMANDS** window.
4. Do one of the following:

   - If your gateway is using a public endpoint, in the **AVAILABLE COMMANDS** window, enter **`open-support-channel`** to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.
   - If your gateway is using a VPC endpoint, in the **AVAILABLE COMMANDS** window, enter **`open-support-channel`**. If your gateway is not activated, provide the VPC endpoint or IP address to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.



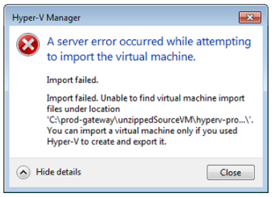
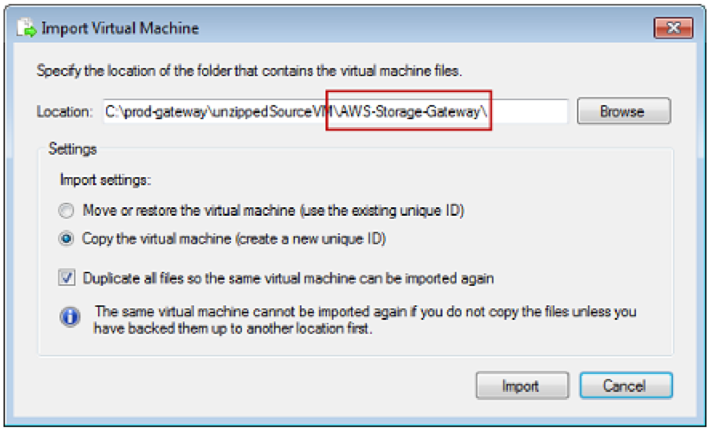
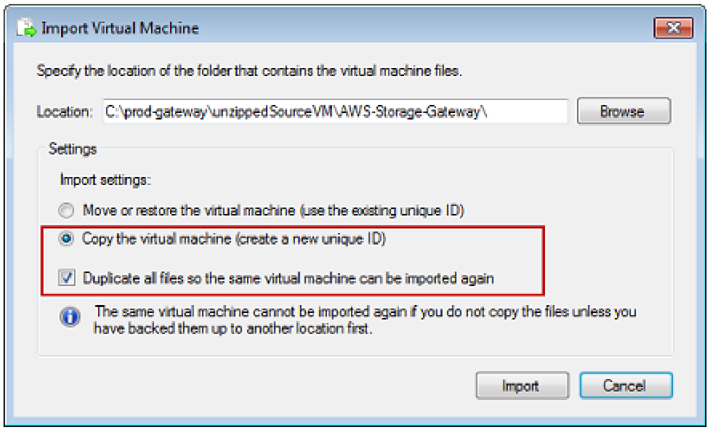
```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands

ip                      Show / manipulate routing, devices, and tunnels
save-routing-table      Save newly added routing table entry
ifconfig                View or configure network interfaces
iptables                Administration tool for IPv4 packet filtering and NAT
save-iptables           Persist IP tables
testconn                Test network connectivity
man                     Display command manual pages
open-support-channel    Connect to Storage Gateway Support
h                       Display available command list
exit                    Return to Storage Gateway Configuration menu

Gateway Console: open-support-channel
```

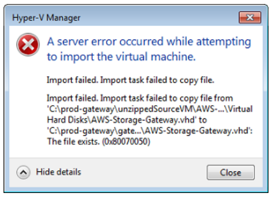
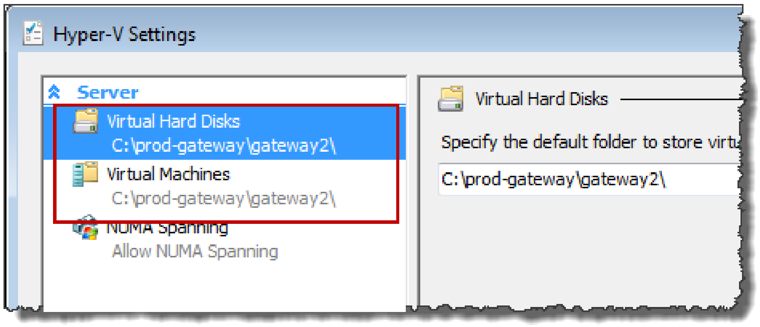
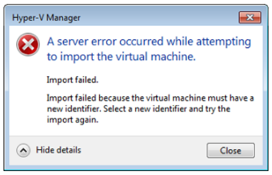
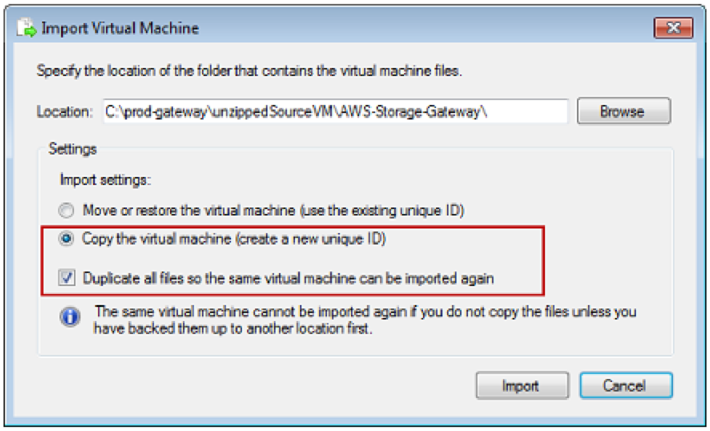
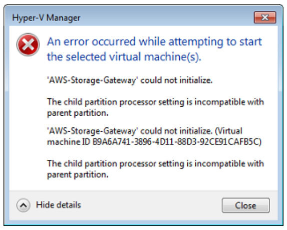
> **Note**
> The channel number is not a Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number. Instead, the gateway makes a Secure Shell (SSH) (TCP 22) connection to Storage Gateway servers and provides the support channel for the connection.

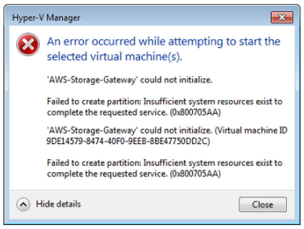
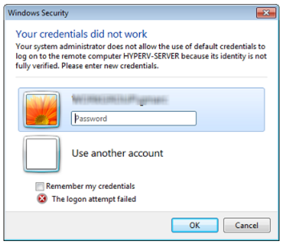
5. After the support channel is established, provide your support service number to AWS Support so AWS Support can provide troubleshooting assistance.
6. When the support session is completed, enter **`q`** to end it. Don't close the session until Amazon Web Services Support notifies you that the support 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 ...".  Hyper-V Manager A server error occurred while attempting to import the virtual machine. Import failed. Import failed. Unable to find virtual machine import files under location 'C:\prod-gateway\unzippedSourceVM\hyperv-pro...\'. You can import a virtual machine only if you used Hyper-V to create and export it. 	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:  Import Virtual Machine Specify the location of the folder that contains the virtual machine files. Location: C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ Settings Import settings: ○ Move or restore the virtual machine (use the existing unique ID) ● Copy the virtual machine (create a new unique ID) ☑ Duplicate all files so the same virtual machine can be imported again The same virtual machine cannot be imported again if you do not copy the files unless you have backed them up to another location first. • 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.  Import Virtual Machine Specify the location of the folder that contains the virtual machine files. Location: C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ Settings Import settings: ○ Move or restore the virtual machine (use the existing unique ID) ● Copy the virtual machine (create a new unique ID) ☑ Duplicate all files so the same virtual machine can be imported again The same virtual machine cannot be imported again if you do not copy the files unless you have backed them up to another location first.
You try to import a gateway and receive the error	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

Issue	Action to Take
message: "Import failed. Import task failed to copy file."  Hyper-V Manager A server error occurred while attempting to import the virtual machine. Import failed. Import task failed to copy file. Import failed. Import task failed to copy file from 'C:\prod-gateway\unzippedSourceVM\AWS-...\Virtual Hard Disks\AWS-Storage-Gateway.vhd' to 'C:\prod-gateway\gate...\AWS-Storage-Gateway.vhd': The file exists. (0x80070050) Hide details Close	configuration files, then this error will occur. To fix this problem, specify new locations in the **Hyper-V Settings** dialog box.  Hyper-V Settings Server Virtual Hard Disks C:\prod-gateway\gateway2\ Virtual Machines C:\prod-gateway\gateway2\ NUMA Spanning Allow NUMA Spanning Virtual Hard Disks Specify the default folder to store virtu C:\prod-gateway\gateway2\
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."  Hyper-V Manager A server error occurred while attempting to import the virtual machine. Import failed. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again. Hide details Close	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.  Import Virtual Machine Specify the location of the folder that contains the virtual machine files. Location: C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ Browse Settings Import settings: ○ Move or restore the virtual machine (use the existing unique ID) ● Copy the virtual machine (create a new unique ID) ☑ Duplicate all files so the same virtual machine can be imported again The same virtual machine cannot be imported again if you do not copy the files unless you have backed them up to another location first. Import Cancel
You try to start a gateway VM and receive an error message "The child partition processor setting is incompatible with parent partition."  Hyper-V Manager An error occurred while attempting to start the selected virtual machine(s). 'AWS-Storage-Gateway' could not initialize. The child partition processor setting is incompatible with parent partition. 'AWS-Storage-Gateway' could not initialize. (Virtual machine ID B9A6A741-3896-4D11-88D3-92CE91CAFB5C) The child partition processor setting is incompatible with parent partition. Hide details Close	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. 5).

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."  Hyper-V Manager An error occurred while attempting to start the selected virtual machine(s). 'AWS-Storage-Gateway' could not initialize. Failed to create partition: Insufficient system resources exist to complete the requested service. (0x800705AA) 'AWS-Storage-Gateway' could not initialize. (Virtual machine ID 9DE14579-8474-40F0-9EEB-8BE47750DD2C) Failed to create partition: Insufficient system resources exist to complete the requested service. (0x800705AA) 	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. 5).
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. 75).
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.  Windows Security Your credentials did not work Your system administrator does not allow the use of default credentials to log on to the remote computer HYPERV-SERVER because its identity is not fully verified. Please enter new credentials. [redacted] Password Use another account □ Remember my credentials The logon attempt failed 	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. 157).

Topics

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. 6).

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

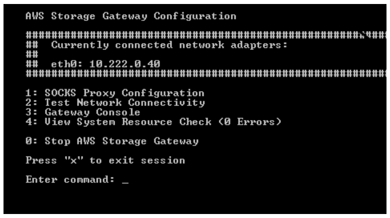
1. Log in to the local console for your Amazon EC2 instance. For instructions, go to Connect to your instance in the *Amazon EC2 User Guide*.

   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.

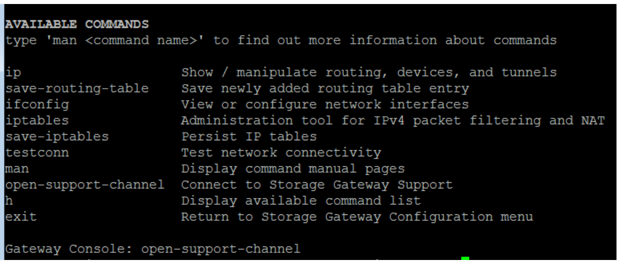
The local console looks like the following.



```
AWS Storage Gateway Configuration

################################################################
##  Currently connected network adapters:
##
##  eth0: 10.222.0.40
################################################################

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

2. At the prompt, enter **`3`** to open the AWS Support Channel console.
3. Enter **`h`** to open the **AVAILABLE COMMANDS** window.
4. Do one of the following:

   - If your gateway is using a public endpoint, in the **AVAILABLE COMMANDS** window, enter **`open-support-channel`** to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.
   - If your gateway is using a VPC endpoint, in the **AVAILABLE COMMANDS** window, enter **`open-support-channel`**. If your gateway is not activated, provide the VPC endpoint or IP address to connect to customer support for Storage Gateway. Allow TCP port 22 so you can open a support channel to AWS. When you connect to customer support, Storage Gateway assigns you a support number. Make a note of your support number.



```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands

ip                      Show / manipulate routing, devices, and tunnels
save-routing-table      Save newly added routing table entry
ifconfig                View or configure network interfaces
iptables                Administration tool for IPv4 packet filtering and NAT
save-iptables           Persist IP tables
testconn                Test network connectivity
man                     Display command manual pages
open-support-channel    Connect to Storage Gateway Support
h                       Display available command list
exit                    Return to Storage Gateway Configuration menu

Gateway Console: open-support-channel
```

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

5. After the support channel is established, provide your support service number to AWS Support so AWS Support can provide troubleshooting assistance.
6. When the support session is completed, enter **`q`** to end it. Don't close the session until 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.

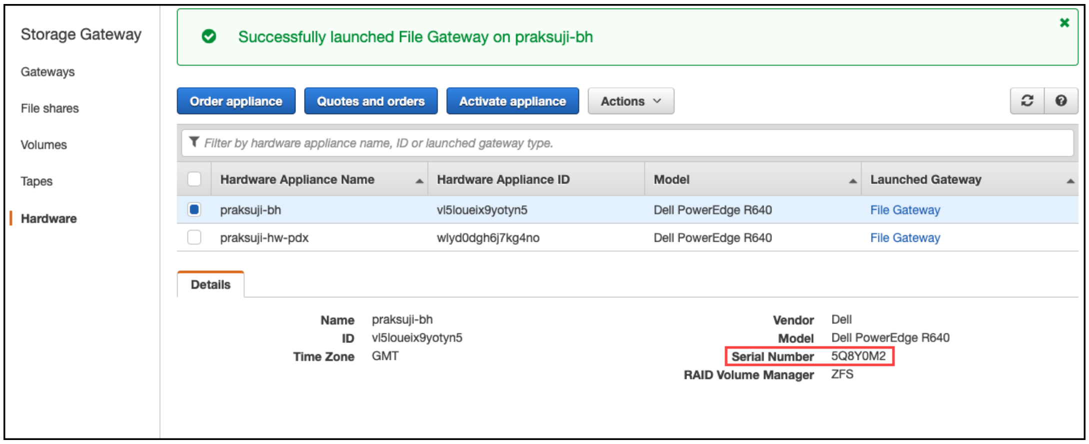
Where do you obtain Dell iDRAC support?

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.



Successfully launched File Gateway on praksuji-bh

	Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
■	praksuji-bh	vl5loueix9yotyn5	Dell PowerEdge R640	File Gateway
□	praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Name praksuji-bh
ID vl5loueix9yotyn5
Time Zone GMT

Vendor Dell
Model Dell PowerEdge R640
Serial Number 5Q8Y0M2
RAID Volume Manager ZFS

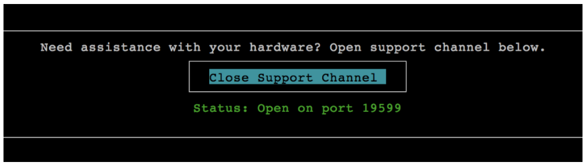
Where to obtain hardware appliance support

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.

   ```
   Need assistance with your hardware? Open support channel below.
                        Close Support Channel
                     Status: Open on port 19599
   ```

   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: ObjectMissing

You can get an `ObjectMissing` error when a writer other than the specified file gateway deletes the specified file from the Amazon FSx. Any subsequent uploads to Amazon FSx or retrievals from Amazon FSx for the object fail.

To resolve an ObjectMissing error

1. Save the latest copy of the file to the local file system of your SMB client (you need this file copy in step 3).
2. Delete the file from the file gateway using your SMB client.
3. Copy the latest version of the file that you saved in step 1 Amazon FSx using your SMB 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. 66), 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. 106) 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

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 Amazon FSx file system 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 FSx

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.

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.

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. 148).

Troubleshooting high availability issues

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

Topics

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

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. 66), 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. 106) of the Availability and application monitoring system in VMware.

Metrics

The `AvailabilityNotifications` metric is available on all gateways. This metric is a count of the number of availability-related health notifications generated by the gateway. Use the `Sum` statistic to observe whether the gateway is experiencing any availability-related events. Consult with your configured CloudWatch log group for details about the events.

Best practices for recovering your data

Although it is rare, your gateway might encounter an unrecoverable failure. Such a failure can occur in your virtual machine (VM), the gateway itself, the local storage, or elsewhere. If a failure occurs, we recommend that you follow the instructions in the appropriate section following to recover your data.

> **Important**
> Storage Gateway doesn’t support recovering a gateway VM from a snapshot that is created by your hypervisor or from your Amazon EC2 Amazon Machine Image (AMI). If your gateway VM malfunctions, activate a new gateway and recover your data to that gateway using the instructions following.

Topics

Recovering from an unexpected virtual machine shutdown

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 FSx File gateway connection to gateway endpoints (p. 74).
- 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. 150).

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. 157).
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

Topics

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

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.

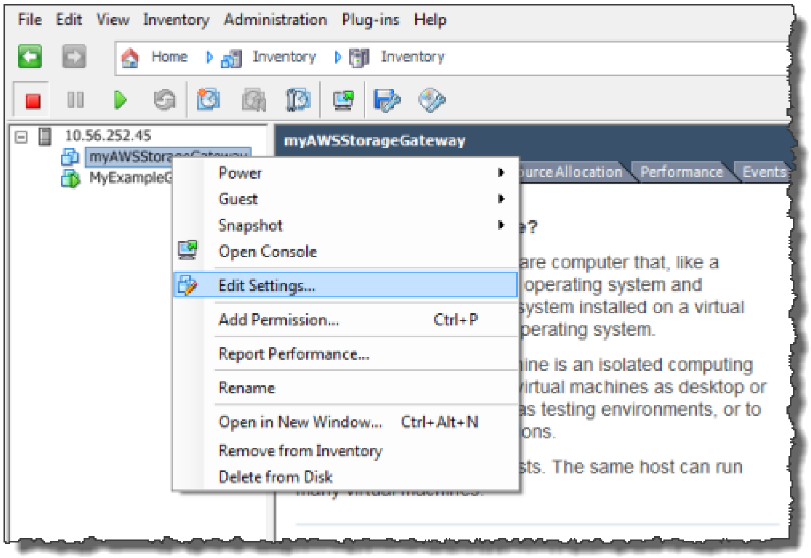
> **Important**
> Synchronizing the VM time with the host time is required for successful gateway activation.

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**.

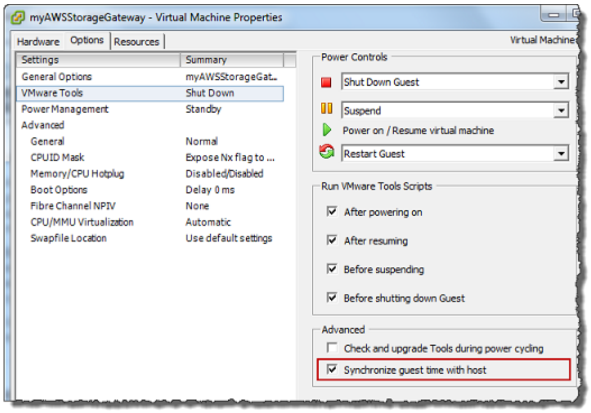
      The **Virtual Machine Properties** dialog box opens.



   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.



myAWSStorageGateway - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine

Settings	Summary
General Options	myAWSStorageGat...
VMware Tools	Shut Down
Power Management	Standby
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Delay 0 ms
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Power Controls

Shut Down Guest

Suspend

Power on / Resume virtual machine

Restart Guest

Run VMware Tools Scripts

☑ After powering on

☑ After resuming

☑ Before suspending

☑ Before shutting down Guest

Advanced

☐ Check and upgrade Tools during power cycling

☑ Synchronize guest time with host

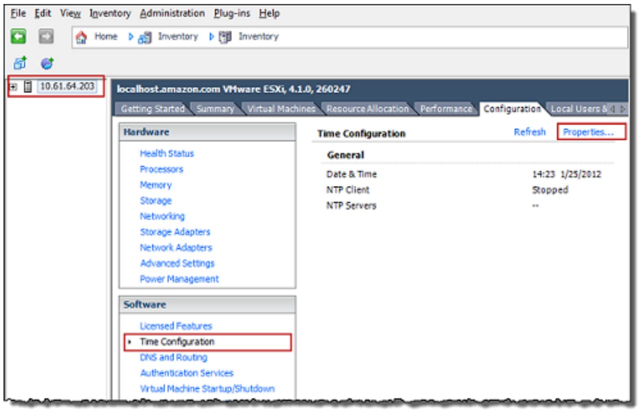
2. Configure the host time.

   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.



Time Configuration

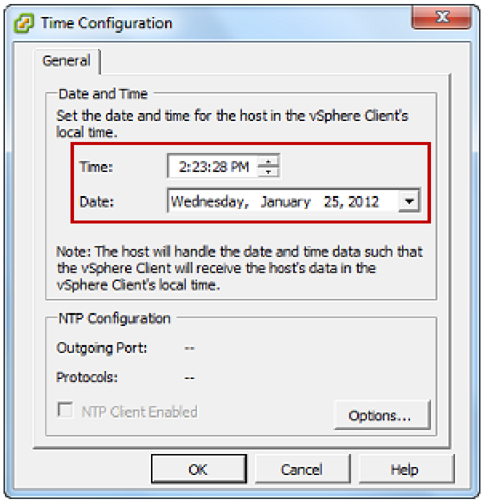
General

Date & Time 14:23 1/25/2012

NTP Client Stopped

NTP Servers --

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



Date and Time

Set the date and time for the host in the vSphere Client's local time.

Time: 2:23:28 PM

Date: Wednesday, January 25, 2012

Note: The host will handle the date and time data such that the vSphere Client will receive the host's data in the vSphere Client's local time.

NTP Configuration

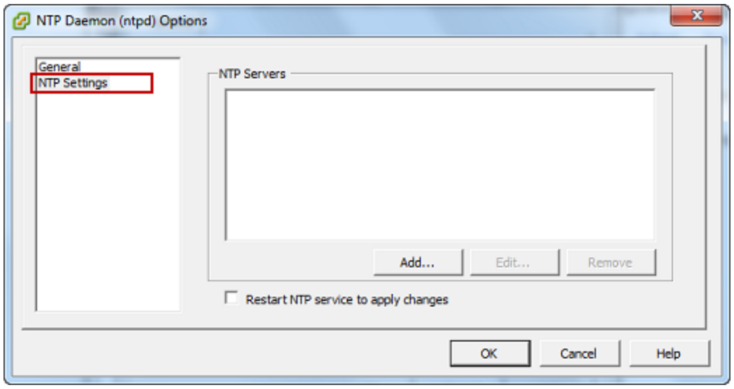
Outgoing Port: --

Protocols: --

□ NTP Client Enabled

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.

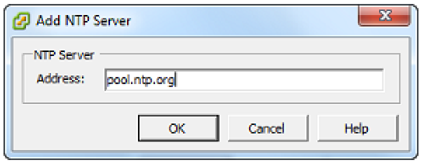


□ Restart NTP service to apply changes

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.



Add NTP Server

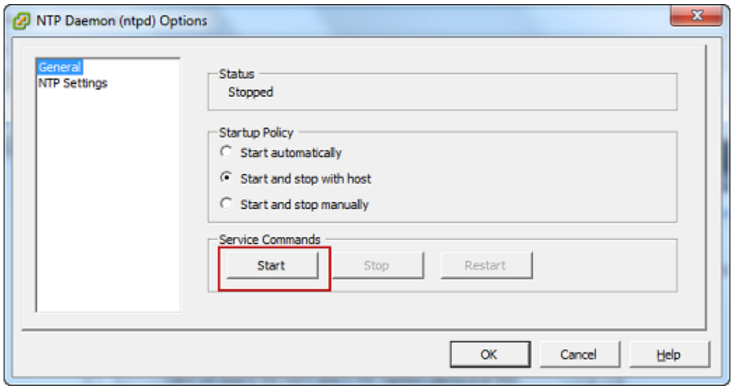
NTP Server

Address: pool.ntp.org

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.



NTP Daemon (ntpd) Options

Status: Stopped

Startup Policy
- ○ Start automatically
- ● Start and stop with host
- ○ Start and stop manually

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

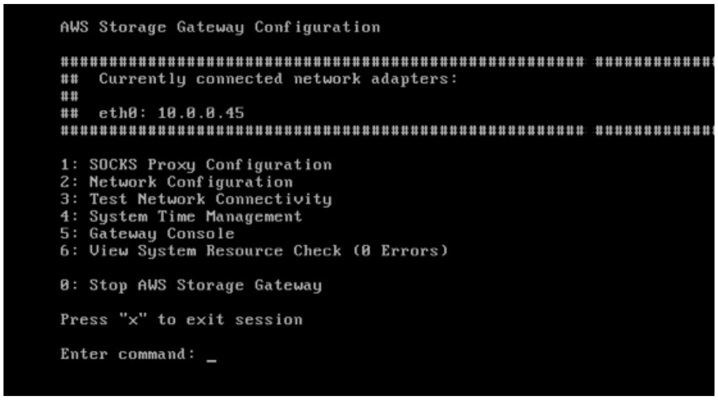
For a gateway deployed on VMware ESXi, setting the hypervisor host time and synchronizing the VM time to the host is sufficient to avoid time drift. For more information, see Synchronizing VM Time with Host Time (p. 152). For a gateway deployed on Microsoft Hyper-V, you should periodically check your 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:

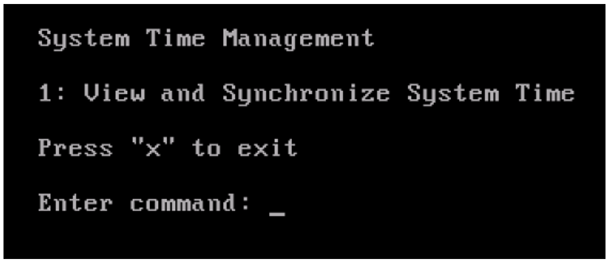
   - For more information on logging in to the VMware ESXi local console, see Accessing the Gateway Local Console with VMware ESXi (p. 91).
   - For more information on logging in to the Microsoft Hyper-V local console, see Access the Gateway Local Console with Microsoft Hyper-V (p. 92).
   - For more information on logging in to the local console for Linux Kernel-based Virtuam Machine (KVM), see Accessing the Gateway Local Console with Linux KVM (p. 89).

2. On the **Storage Gateway Configuration** main menu, enter **4** for **System Time Management**.



```
AWS Storage Gateway Configuration

###################################################### ############
##  Currently connected network adapters:
##
##  eth0: 10.0.0.45
###################################################### ############

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

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

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

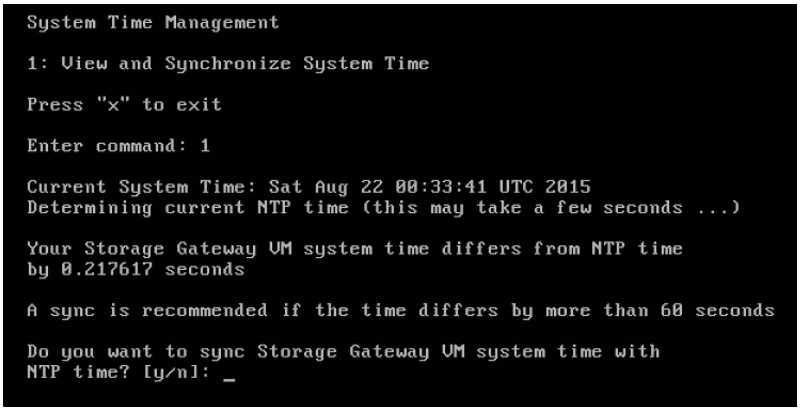


```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

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

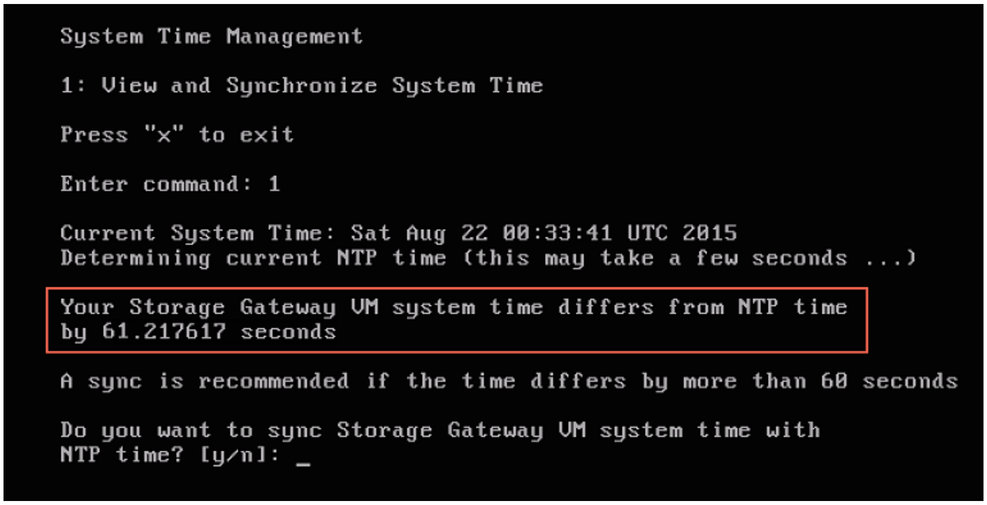
   If you enter **y** to synchronize, the synchronization might take a few moments.

   The following screenshot shows a VM that doesn't require time synchronization.



```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: 1

Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)

Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds

A sync is recommended if the time differs by more than 60 seconds

Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

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



```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: 1

Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)

Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds

A sync is recommended if the time differs by more than 60 seconds

Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Deploying a 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. 6).

   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. 6).

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. 7).
11. Choose **Review and Launch** to review your configuration.
12. On the **Step 7: Review Instance Launch** page, choose **Launch**.
13. In the **Select an existing key pair or create a new key pair** dialog box, choose **Choose an existing key pair**, and then select the key pair that you created when getting set up. When you are ready, choose the acknowledgment box, and then choose **Launch Instances**.

    A confirmation page tells you that your instance is launching.
14. Choose **View Instances** to close the confirmation page and return to the console. On the **Instances** screen, you can view the status of your instance. It takes a short time for an instance to launch. When you launch an instance, its initial state is **pending**. After the instance starts, its state changes to **running**, and it receives a public DNS name
15. Select your instance, note the public IP address in the **Description** tag, and return to the Connect to gateway (p. 35) page on the Storage Gateway console to continue your gateway setup.

You can determine the AMI ID to use for launching a file gateway by using the Storage Gateway console or by querying the AWS Systems Manager parameter store.

To determine the AMI ID

1. Sign in to the AWS Management Console and open the Storage Gateway console at https://console.aws.amazon.com/storagegateway/home.
2. Choose **Create gateway**, choose **File gateway**, and then choose **Next**.
3. On the **Choose host platform** page, choose **Amazon EC2**.

4. Choose **Launch instance** to launch a Storage Gateway EC2 AMI. You are redirected to the EC2 community AMI page, where you can see the AMI ID for your AWS Region in the URL.

   Or you can query the Systems Manager parameter store. You can use the AWS CLI or Storage Gateway API to query the Systems Manager public parameter under the namespace `/aws/service/storagegateway/ami/FILE_S3/latest`. For example, using the following CLI command returns the ID of the current AMI in the current AWS Region.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
FILE_S3/latest
```

   The CLI command returns output similar to the following.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX/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. The request you make to the gateway VM contains the AWS Region in which activation occurs.

The URL returned by the redirect in the response contains a query string parameter called `activationkey`. This query string parameter is your activation key. The format of the query string looks like the following: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*.

Topics

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 -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

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*.

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. 91)
- HyperV host: Access the Gateway Local Console with Microsoft Hyper-V (p. 92)
- Linux Kernel-based Virtual Machine (KVM) host: Accessing the Gateway Local Console with Linux KVM (p. 89)
- EC2 host: Getting an IP Address from an Amazon EC2 Host (p. 161)

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`

Resource Type	ARN Format
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. 120).

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. 120)

Working with open-source components for 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

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 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 FSx File Gateway

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

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

- For Amazon FSx File Gateway 2021-07-07 Release: sgw-file-fsx-smb-open-source.tgz
- For Amazon FSx File Gateway 2021-04-06 Release: sgw-file-fsx-smb-20210406-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 the following links:

- For Amazon FSx File Gateway 2021-07-07 Release: Third-Party License.
- For Amazon FSx File Gateway 2021-04-06 Release: Third-Party License.

API Reference for Storage Gateway

In addition to using the console, you can use the Storage Gateway API to programmatically configure and manage your gateways. This section describes the Storage Gateway operations, request signing for authentication and the error handling. For information about the regions and endpoints available for Storage Gateway, see 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

Storage Gateway Required Request Headers

This section describes the required headers that you must send with every POST request to Storage Gateway. You include HTTP headers to identify key information about the request including the operation you want to invoke, the date of the request, and information that indicates the authorization of you as the sender of the request. Headers are case insensitive and the order of the headers is not important.

The following example shows headers that are used in the ActivateGateway operation.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

The following are the headers that must include with your POST requests to Storage Gateway. Headers shown below that begin with "x-amz" are AWS-specific headers. All other headers listed are common header used in HTTP transactions.

Header	Description
`Authorization`	The authorization header contains several of pieces of information about the request that enable Storage Gateway to determine if the request is a valid action for the requester. The format of this header is as follows (line breaks added for readability):

Header	Description

	`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. 167).

`Content-Type`	Use `application/x-amz-json-1.1` as the content type for all requests to Storage Gateway. `Content-Type: application/x-amz-json-1.1`
`Host`	Use the host header to specify the 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 Storage Gateway, see 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 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. 166).

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. 168) 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. 168) 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. 168), 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

This section provides reference information about 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. 183).

Exceptions

The following table lists Storage Gateway API exceptions. When an 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. 171) 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. 171).	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. 171).	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 occurs more than 15 minutes in the future.	400 Bad Request
`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

Exception	Message	HTTP Status Code
`SubscriptionRequiredException`	The AWS Access Key Id needs a subscription for the service.	400 Bad Request
`ThrottlingException`	Rate exceeded.	400 Bad Request
`UnknownOperationException`	An unknown operation was specified. Valid operations are listed in Operations in Storage Gateway (p. 185).	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 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. 170).

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 AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	The specified disk does not exist.	AddCache AddUploadBuffer

Operation Error Code	Message	Operations That Return this Error Code
		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. 170).

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 *Storage Gateway API Reference*.

Document history for the Amazon FSx File Gateway User Guide

- **API version**: 2013-06-30
- **Latest documentation update**: July 07, 2021

The following table describes the documentation releases for Amazon FSx File Gateway. For notification about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
Multiple file system support (p. 186)	Amazon FSx File Gateway now supports up to five attached Amazon FSx file systems. For more information, see Attach an Amazon FSx for Windows File Server file system.	July 7, 2021
Amazon FSx soft storage quota support (p. 186)	Amazon FSx File Gateway now supports soft storage quotas (which warn you when users surpass their data limits) when writing to attached Amazon FSx file systems where storage quotas are configured. Hard quotas (which enforce data limits by denying write access) are not supported. Soft quotas work for all users except the Amazon FSx admin user. For more information about setting up storage quotas, see Storage quotas in the *FSx for Windows File Server User Guide*.	July 7, 2021
New guide (p. 186)	In addition to the original file gateway (now known as Amazon S3 File Gateway), Storage Gateway provides Amazon FSx File Gateway (FSx File). FSx File provides low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility. For more information, see What is Amazon FSx File Gateway?	April 27, 2021