AWS Storage Gateway: S3 File Gateway Setup, Configuration, and Monitoring

**SPL-226 - Version 1.0.19**

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration. The service helps you reduce and simplify your datacenter and branch or remote office storage infrastructure. Your applications connect to the service through a virtual machine or hardware gateway appliance using standard storage protocols, such as NFS, SMB, and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon FSx for Windows File Server, Amazon Elastic Block Store (EBS), and AWS Backup, providing storage for files, volumes, snapshots, and virtual tapes in AWS. The service includes a highly-optimized data transfer mechanism, with bandwidth management, automated network resilience, and efficient data transfer, along with a local cache for low-latency on-premises access to your most active data.

In this lab, you work with S3 File Gateway NFS and SMB shares, with a focus on the networking protocols and ports required for each configuration. You first deploy and configure S3 File Gateway as an EC2 instance. You then have the choice of creating and utilizing an NFS file share with a Linux instance, an SMB file share with a Windows instance, or both. In each scenario, you configure the relevant security groups to allow traffic on the required ports for the storage protocol being used, then mount the file share and copy local data to it.

TOPICS COVERED

When you finish the lab, you will be able to:

* Deploy and activate an S3 File Gateway appliance
* List the network ports required for S3 File Gateway activation, NFS, and SMB communications
* Create an NFS file share, mount it to a Linux instance, copy local data, and view the data from another Linux instance
* Create an SMB file share, mount it to a Windows instance, copy local data, and view the data from another Windows instance
* Monitor different metrics for S3 File Gateway using Amazon CloudWatch
* Analyze recent events related to S3 File Gateway resources using AWS CloudTrail

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

* **Command:** A command that you must run.
* **Expected output:** A sample output that you can use to verify the output of a command or edited file.
* **Note:** A hint, tip, or important guidance.
* **Additional information:** Where to find more information.
* **Caution:** Information of special interest or importance (not so important to cause problems with the equipment or data if you miss it, but it could result in the need to repeat certain steps).
* **Consider:** A moment to pause to consider how you might apply a concept in your own environment or to initiate a conversation about the topic at hand.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with basic navigation of the AWS Management Console, connecting to EC2 instances, storage protocols, network ports, and security groups.

DURATION

This lab requires **120** minutes to complete.

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

 You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

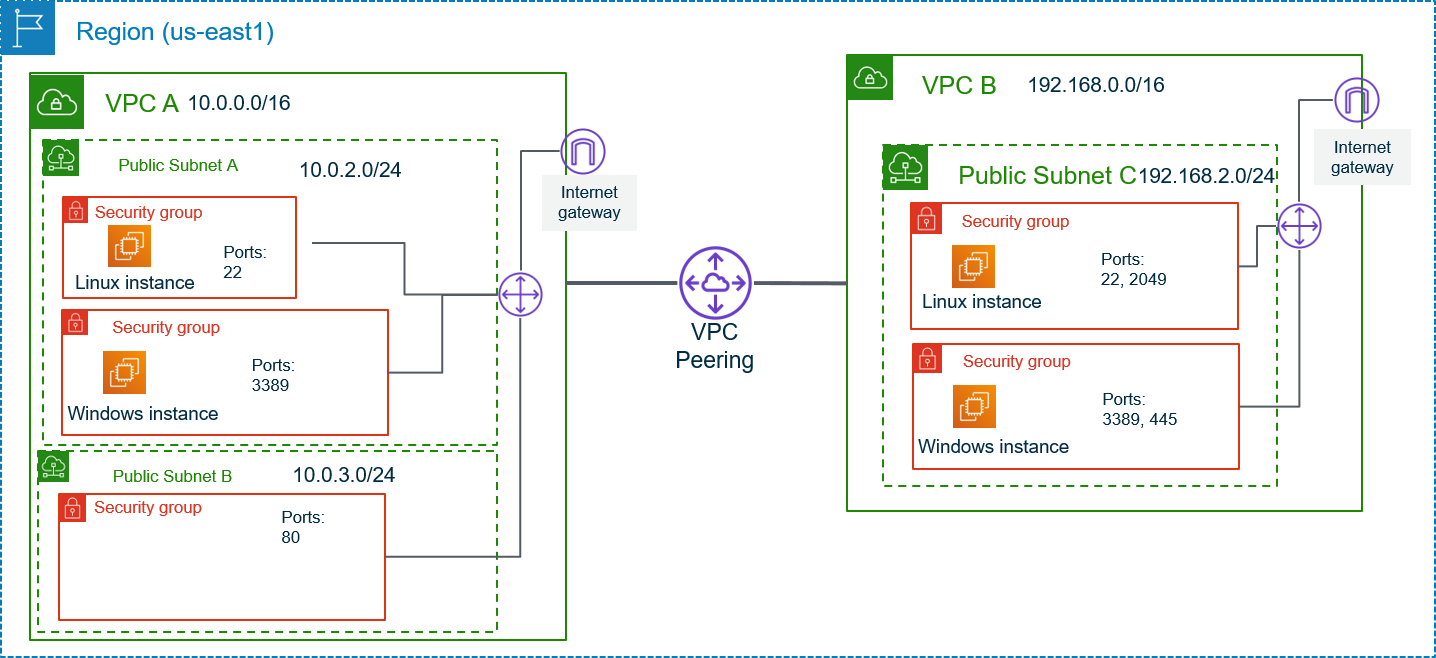
**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

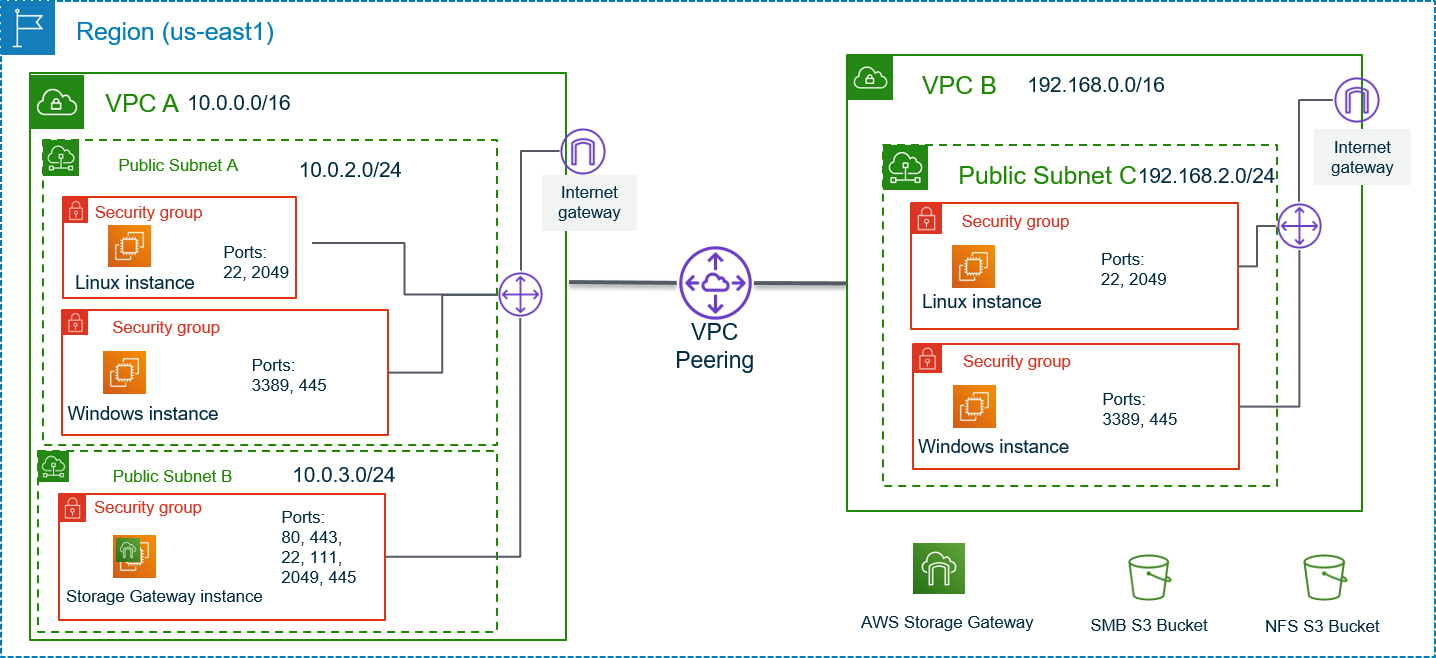
* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

**Task 1: Review the lab architecture**

Take a moment to familiarize yourself with the architecture of this lab environment. It begins with two VPCs, three subnets, two Linux EC2 instances, and two Windows EC2 instances. VPC-A is used to emulate cloud-based services, while VPC-B is used to emulate an on-premises environment.



At the end of the lab, the environment will look like this:



**Congratulations!** You successfully reviewed and visualized the architecture for this lab.

**Task 2: Create S3 buckets for file share storage**

When configuring an S3 File Gateway with an NFS or SMB file share, you are prompted for the name of an S3 bucket to serve as the storage location for that file share. In this task, you create two S3 buckets - one for use with the NFS file share and one for use with the SMB file share.

1. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. Choose **Create bucket** and then configure:

* **Bucket name:** Create a name for the NFS S3 bucket that you can easily remember. It must be globally unique.
* **AWS Region:** US East (N. Virginia) us-east-1

1. Keep default values for remaining configuration options and choose **Create bucket**.

A  **Successfully created bucket “nfs-s3-bucket-lab”** message is displayed on top of the screen.

 In this lab, you use the default settings when creating the S3 buckets. In a production environment, if you wish to enable other settings, such as object ownership, public access or versioning, you can do so using this wizard.

1. Choose **Create bucket** to create a second bucket and then configure:

* **Bucket name:** Create a name for the SMB bucket you can easily remember. It must be globally unique.
* **AWS Region:** US East (N. Virginia) us-east-1

1. Keep default values for remaining configuration options and choose **Create bucket**.

A  **Successfully created bucket “smb-s3-bucket-lab”** message is displayed on top of the screen.

 Make a note of the bucket names you just created, as they are used in future tasks.

**Congratulations!** You successfully created S3 Buckets for file share storage. You use these buckets while creating S3 File Gateway in the following tasks.

**Task 3: Deploy the S3 File Gateway appliance**

In this task, you deploy and configure the S3 File Gateway appliance as an Amazon Elastic Compute Cloud (Amazon EC2) instance. In a production environment, you also have an option to deploy the virtual appliance on VMware or Hyper-V based systems, or as a physical appliance.

1. At the top of the AWS Management Console, in the search bar, search for and choose

Storage Gateway

.

You should be prompted with an AWS Storage Gateway getting started page. This page is displayed because the Storage Gateway service has not yet been configured in this region.

1. At the top-right corner of the window, verify that the AWS Region is **N. Virginia**.
2. On the left menu select **Gateways**, and then choose **Create gateway**.
3. On the **Set up gateway** screen, under **Gateway settings** configure:

* **Gateway name:** Enter

S3 File Gateway

.

* **Gateway time zone:** Select **GMT -5:00 Eastern Time (US & Canada), Bogota, Lima** from the dropdown menu.

1. Under **Gateway options**, select  **Amazon S3 File Gateway** as the gateway type.
2. Under **Platform options**:

* For **Host platform**, select  **Amazon EC2**.
* For **Launch EC2 instance**, select  **Customize your settings**.

1. For **Set up gateway on Amazon EC2**, choose **Launch instance**.

A new tab opens to the EC2 instance launch wizard. This link automatically selects the correct Amazon Machine Image (AMI) that must be used for the file gateway appliance.

On the **Launch an instance** page, make the following selections:

1. In the **Names and tags** section, locate the **Name** textbox and enter

S3 File Gateway Appliance

.

1. Choose Add additional tags.
2. Locate the **Resource types** dropdown menu, and select **Volumes** and **Network interfaces**. Select **Instances** if not already selected.
3. In the **Application and OS Images** section, keep the pre-selected AMI for AWS Storage Gateway.
4. In the **Instance type** section, locate the **Instance type** dropdown menu and select **t2.xlarge**.

**Note:** t2.xlarge is the only instance type you can select in this lab environment. Selecting any other instance type results in an error message at the end of the wizard.

 The t2.xlarge instance type is used only as an example in this lab. When deploying a Storage Gateway appliance, always refer to the [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#requirements-hardware-storage) for correct appliance sizing.

1. In the **Key pair (login)** section, locate the **Key pair name** dropdown menu and choose an existing keypair (e.g. AWSLabsKeyPair-xxx) that was already created for this lab.
2. In the **Network settings** section, choose **Edit** and make the following selections:

* Locate the **VPC** dropdown menu and select **VPC-A**.
* Locate the **Subnet** dropdown menu and select **VPC-A-Subnet-B**.
* Locate the **Auto-assign public IP** dropdown menu and select **Enable**.
* For **Firewall**, select **Select existing security group** and then select **S3 File Gateway access** from the **Common security groups** dropdown menu.

This security group is configured to allow the following traffic:

* Ingress - port 80 (HTTP) for gateway activation
* Ingress - port 111 and 2049 for NFSv4.1 communications from VPC-B Subnet-A
* Ingress - port 445 for SMBv3 communications from VPC-B Subnet-A
* Egress - port 443 for communication with the AWS Storage Gateway service

 Refer to the [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#networks) for additional information about the ports used by AWS Storage Gateway.

1. In the **Configure storage** section, choose Advanced and then choose **Add new volume**.
2. For **Volume 2**, make the following selections:

* **Device name:** Select **/dev/sdb** from the dropdown menu.
* **Size (GiB):** Enter

150

.

* **Volume type:** Select **General purpose SSD (gp2)** from the dropdown menu.
* **Delete on termination:** Select **Yes** from the dropdown menu.

1. Keep default values for remaining properties and choose **Launch instance**.

A *Successfully initiated launch of instance (i-0e8ff14b9d8fad5b0)* message is displayed.

1. Choose **View all instances**.

 It might take few minutes for the **S3 File Gateway Appliance** instance to finish its status checks. You can confirm that by checking the **Status check** column where it shows Initializing and eventually moves to  2/2 checks passed. Use the refresh  option as required.

1. Select your S3 File Gateway instance from the list, and then at the bottom of the window under the **Details** tab, locate the **Public IPv4 address** and copy the IP address listed. You use it when finalizing the S3 File Gateway deployment.
2. Return to the **AWS Storage Gateway** tab in your browser. It should still be at the **Platform options** section.
3. Verify **Amazon EC2** is selected, and then in the **Confirm set up gateway** section, choose  I completed all the steps above and launched the EC2 instance.
4. Choose **Next**.

On the **Connect to AWS** screen, make the following selections:

1. In the **Gateway connection options** section, select  **IP address** as the connection option.
2. For the **IP address** field, paste the **Public IPv4 address** you copied earlier for the S3 File Gateway Appliance instance.
3. In the **Endpoint options** section, select  **Publicly accessible** as the Service endpoint.
4. Choose **Next**.
5. On the **Review and activate** screen, verify the configurations and choose **Next**.

A  **Successfully activated gateway S3 File Gateway** message is displayed on top of the screen.

1. On the **Configure gateway** screen, in the **Configure cache storage** section, wait for local disks to load.

 Here you see the following message: *Loading local disks. This can take a few minutes to load. You need to configure your local disk to move forward.*

1. After the processing is completed, under **Configure cache storage** section, verify and configure:

* **Disk ID:** /dev/sdb
* **Capacity:** 150 GiB
* **Allocated to:** Select **Cache** from the dropdown menu.

1. In the **CloudWatch log group** section, select  **Deactivate logging**.
2. In the **CloudWatch alarms** section, select  **No alarm**.
3. Choose **Configure**.

A  Successfully created gateway S3 File Gateway (sgw-XXXXXXXX). You can create file share on this gateway. message is displayed on top of the screen.

Wait for few minutes until the S3 File Gateway status changes to  Running.

1. Remain on this screen for the next task.

Now that the S3 File Gateway has been deployed and configured, you can create file shares to attach to your hosts.

 The remainder of this lab is broken up in two separate sections based on the types of file share you can create - NFS or SMB. Tasks 4 and 5 walk through the requirements and setup of an NFS file share connected to Linux hosts. Tasks 6 and 7 walk through the requirements and setup of an SMB file share connected to Windows hosts. Each section can be performed independently of the other, so you can skip to the one you care about the most, or you can choose to complete both the sections.

Continue to the next task to perform the NFS tasks.

Choose [this link](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-226%3A1.0.19-c0f82cbe/en-US#smb-tasks) to skip to the SMB tasks.

**Congratulations!** You successfully deployed and configured the S3 File Gateway appliance as an Amazon Elastic Compute Cloud (Amazon EC2) instance.

**Task 4: Create an NFS file share**

In this task, you create an NFS file share on the S3 File Gateway that is configured to use the S3 bucket that you created previously to store and retrieve files. You then configure a security group to allow NFS traffic to pass between the S3 File Gateway appliance and a Linux instance.

1. If you are not already at the Storage Gateway screen from the previous section, at the top of the AWS Management Console, in the search bar, search for and choose

Storage Gateway

.

1. **Gateways** should already be selected in the navigation menu at the left. At the top of the window, choose **Create file share**.

 You can also create a new file share from the **File shares** section, accessible from the navigation menu at the left.

1. On the **Create file share** screen, in the **Basics** section, make the following selections:

* **Gateway:** Select **S3 File Gateway (sgw-*random alphanumeric*)** from the dropdown menu.
  + **Note:** “S3 File Gateway” may be different if you used another name for your gateway in Task 3.
* **File share type:** Select  **NFS**.
* **S3 bucket:** Select the name of the S3 bucket you created in Task 2 for use with NFS.

1. At the bottom of the page, choose **Customize configuration**.
2. On the **File share settings** page, scroll down and choose **Next**.
3. On the **Amazon S3 storage settings** screen, make the following selections:

* **Storage class for new objects:** Select **S3 Standard** from the dropdown menu.
* **Object metadata:**
  + Select  Guess MIME type
  + Select  Give bucket owner full control
* **Access to your S3 bucket**: Select  Use an existing IAM role
* **IAM role:** Copy the *FgwIamPolicyARN* value from the list of parameters to the left of these instructions, and then paste it into this field.

1. Choose **Next**.

 You should see a warning message about the file share being accessible from anywhere. It is recommended to always limit access to only the required clients in your environment.

1. On the **File access settings** screen, in the **Access object** section, choose **Add client**.
2. For **Allowed clients**, add

10.0.2.0/24

 to grant access to the share from the hosts in VPC-A Subnet-A.

1. Choose **Add client** button again, and then enter

192.168.2.0/24

 to grant access to the share from the hosts in VPC-B Subnet-A.

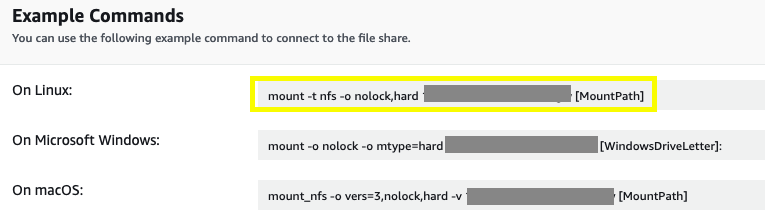
1. At the bottom-right of the window, choose **Next**.
2. On the **Review and create** screen, verify all the configurations and choose **Create**.

A  Your file share has been created and added to the gateway. message is displayed on top of the screen.

1. Monitor the **Status** field and wait for it to change from *Updating* to *Available*, which should take less than a minute.

 You may need to choose the refresh  button at the top-right of the window.

1. Select the link to the file share you just created. At the bottom of the window, make a note of the command to mount the file share on Linux. You use it in the next task.



**Congratulations!** You successfully created an NFS file share on the S3 File Gateway that is configured to use the S3 bucket that you created previously to store and retrieve files.

**Task 5: Examine the security group, mount the file share to the Linux instance, and migrate data**

Before you can being migrating data to the NFS share you created, you must first mount the share. In this task, you discover that security group rules prevent you from connecting to the file share from the Linux host. You then add the appropriate rules to the security group to enable NFS communication, mount the NFS share on a Linux host, and copy data from the instance to the file share.

Next, you connect to the Linux host in VPC-A

1. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. On the EC2 Dashboard, choose **Instances** from the left navigation menu.
2. On the **Instances** screen, select  **VPC-A Linux Server** and choose **Connect**.
3. On the **Connect to instance** screen, select the **EC2 Instance Connect** tab. Leave the default **User name** as

ec2-user

 and choose **Connect**.

You should now be connected to the Linux instance.

1. From the Linux instance terminal, enter the following command to view the sample data that exists on this host. You should see 20 image files in the .png format.

ls /media/data

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.png 11.png 12.png 13.png 14.png 15.png 16.png 17.png 18.png 19.png 1.png 20.png 2.png 3.png 4.png 5.png 6.png 7.png 8.png 9.png

1. Enter the following command to create the directory that you use to synchronize data with your S3 bucket:

sudo mkdir -p /mnt/nfs/s3

1. Use the command you copied at the end of the previous task to mount the file share on the Linux instance. Replace **[MountPath]** with the path to the share you created on the host.

 You must add

sudo

 at the beginning of the command to run it with administrative rights.

sudo mount -t nfs -o nolock,hard <File-Gateway-appliance-private-IP-address>:/<S3-bucket-name> /mnt/nfs/s3

For example:

sudo mount -t nfs -o nolock,hard 10.0.3.240:/nfs-bucket-sgw /mnt/nfs/s3

 This command times out after approximately five minutes because the security group is not configured to allow NFS traffic between the Linux host and the S3 File Gateway appliance. Type Ctrl+C to interrupt the command, rather than waiting for it to time out. You add the appropriate rules next.

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

VPC

.

1. In the left navigation menu, expand the **Security** section and choose **Security groups**.
2. Select the security group named **S3 File Gateway access**.

The *S3 File Gateway access* security group is attached to the S3 File Gateway Appliance instance you created previously. It currently contains rules that allow inbound traffic to the appliance on specific ports that are required to activate the appliance, as well as to allow NFS and SMB traffic from Subnet-A on VPC-B. Refer to the network diagram at the beginning of these instructions for a visualization of the configuration.

 A security group operates much like a firewall that may be in your on-premises datacenter. When configuring your firewall rules, refer to the [AWS Storage Gateway documentation](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#networks) to verify the ports that need to be open between your endpoints and the AWS Storage Gateway service.

 If you are using AWS Direct Connect, there are additional considerations when working with Storage Gateway, such as creating a Public Virtual Interface to enable communication with the public AWS Storage Gateway endpoints. Refer to the [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/using-dx.html) for more information.

1. At the bottom of the window, choose the **Inbound rules** tab, and then choose **Edit inbound rules**.
2. To the right of the **HTTP** (port 80) entry, choose **Delete** to delete the rule.

 HTTP traffic is only required when activating the S3 File Gateway appliance, and can be removed once activation is complete.

1. Choose **Add rule**.
2. Choose the drop-down menu in the **Type** column of the new rule, and then select **NFS**.

Notice selecting NFS automatically updates the **Protocol** column to *TCP* and sets the **Port range** to *2049*.

1. In the **Source** column, select **Custom** from the drop-down menu, and then enter the IP range of VPC-A Subnet-A in CIDR notation:

10.0.2.0/24

This rule allows traffic on port 2049 to the S3 File Gateway appliance subnet (VPC-A Subnet-B) from any host on the 10.0.2.0/24 subnet.

 The version of Linux you are working with in this example uses NFS v4.1, so you open port 2049. However, in the event you need to utilize NFSv3, you want to open port 20048.

1. Choose **Add Rule**.
2. Choose the drop-down menu in the **Type** column of the new rule, and then select **Custom TCP**.
3. In the **Port Range** field, enter

111

.

1. In the **Source** column, select **Custom** from the drop-down menu, and then enter the IP range of VPC-A Subnet-A in CIDR notation:

10.0.2.0/24

This rule is also related to NFS data communications.

1. Choose **Save rules**.

A  **Inbound security group rules successfully modified on security group (sg-046d2de01cf0f04fa | S3 File Gateway access)** message is displayed on top of the screen.

1. Return to the EC2 Instance Connect session for the Linux host.
2. Re-run the command to mount the file share on the Linux instance. Replace **[MountPath]** with the path to the share you created on the host.

sudo mount -t nfs -o nolock,hard <File-Gateway-appliance-private-IP-address>:/<S3-bucket-name> [MountPath]

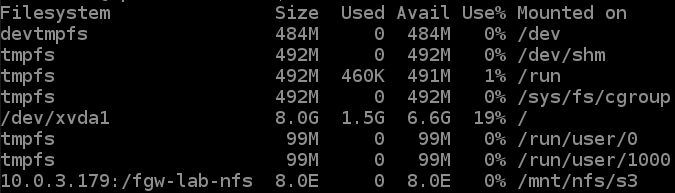
For example:

sudo mount -t nfs -o nolock,hard 10.0.3.240:/nfs-bucket-sgw /mnt/nfs/s3

1. Enter the following command to verify the share has been mounted correctly:

df -h

**Expected output:**



1. Now that the mount point has been created, use the following command to copy the data you wish to migrate to the S3 bucket into the share:

cp -v /media/data/\*.png /mnt/nfs/s3

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

‘/media/data/10.png’ -> ‘/mnt/nfs/s3/10.png’

‘/media/data/11.png’ -> ‘/mnt/nfs/s3/11.png’

‘/media/data/12.png’ -> ‘/mnt/nfs/s3/12.png’

‘/media/data/13.png’ -> ‘/mnt/nfs/s3/13.png’

‘/media/data/14.png’ -> ‘/mnt/nfs/s3/14.png’

‘/media/data/15.png’ -> ‘/mnt/nfs/s3/15.png’

‘/media/data/16.png’ -> ‘/mnt/nfs/s3/16.png’

‘/media/data/17.png’ -> ‘/mnt/nfs/s3/17.png’

‘/media/data/18.png’ -> ‘/mnt/nfs/s3/18.png’

‘/media/data/19.png’ -> ‘/mnt/nfs/s3/19.png’

‘/media/data/1.png’ -> ‘/mnt/nfs/s3/1.png’

‘/media/data/20.png’ -> ‘/mnt/nfs/s3/20.png’

‘/media/data/2.png’ -> ‘/mnt/nfs/s3/2.png’

‘/media/data/3.png’ -> ‘/mnt/nfs/s3/3.png’

‘/media/data/4.png’ -> ‘/mnt/nfs/s3/4.png’

‘/media/data/5.png’ -> ‘/mnt/nfs/s3/5.png’

‘/media/data/6.png’ -> ‘/mnt/nfs/s3/6.png’

‘/media/data/7.png’ -> ‘/mnt/nfs/s3/7.png’

‘/media/data/8.png’ -> ‘/mnt/nfs/s3/8.png’

‘/media/data/9.png’ -> ‘/mnt/nfs/s3/9.png’

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. Choose the link to the S3 bucket you created for NFS in Task 2.
2. Verify the files you copied into the mounted NFS share are displayed in the S3 bucket. You should see 20 PNG files.
3. Close the EC2 Instance Connect browser window for the **VPC-A Linux Server**.

**Congratulations!** You successfully copied the local data from Linux host to the NFS file share and S3 bucket.

Next, you access the same NFS file share from a Linux host on another network (VPC-B) and discover that the data is on a shared resource.

1. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. On the EC2 Dashboard, choose **Instances** from the left navigation menu.
2. On the **Instances** screen, select  **VPC-B Linux Server** and choose **Connect**.
3. On the **Connect to instance** screen, select the **EC2 Instance Connect** tab. Leave the default **User name** as

ec2-user

 and choose **Connect**.

You should now be connected to the Linux instance.

1. On the Linux host, create a directory that is used to synchronize data with your S3 bucket using the following command:

sudo mkdir -p /mnt/nfs/s3

1. Use the command you copied at the end of the previous task to mount the file share on the Linux instance. Replace **[MountPath]** with the path to the share you created on the host.

 You must add

sudo

 at the beginning of the command to run it with administrative rights.

sudo mount -t nfs -o nolock,hard <File-Gateway-appliance-private-IP-address>:/<S3-bucket-name> /mnt/nfs/s3

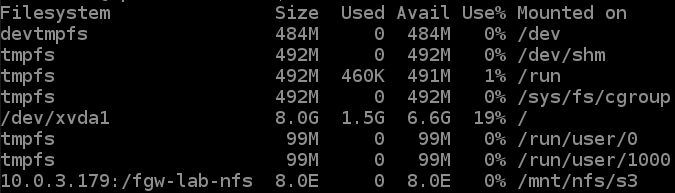
For example:

sudo mount -t nfs -o nolock,hard 10.0.3.240:/nfs-bucket-sgw /mnt/nfs/s3

1. Enter the following command to verify the share has been mounted correctly:

df -h

**Expected output:**



1. Enter the following command to verify the files show in the newly mounted share:

ls /mnt/nfs/s3

You should see the same 20 PNG files listed that you have been working with thus far.

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.png 11.png 12.png 13.png 14.png 15.png 16.png 17.png 18.png 19.png 1.png 20.png 2.png 3.png 4.png 5.png 6.png 7.png 8.png 9.png

1. To show that it is linked to the same file share as the first Linux host, enter the following commands to delete one of the files

cd /mnt/nfs/s3 && rm 1.png

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. Choose the link to the S3 bucket you created for NFS in Task 2.
2. Verify **1.png** has been deleted from the bucket.

**Congratulations!** You have successfully:

* Created an NFS file share and linked it to an S3 bucket.
* Added the appropriate NFS ports to the security group to allow NFS traffic between the S3 File Gateway appliance and the Linux hosts.
* Copied local data from a Linux host to the file share and accessed that same data from a secondary host in a separate network.

If you are not interested in performing the SMB tasks, choose [this link](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2Fspl-226%3A1.0.19-c0f82cbe/en-US#end-lab) to skip to the end of the lab. Otherwise, continue on to the next task to learn about SMB file shares on an S3 File Gateway.

**Task 6: Create an SMB file share**

In this task, you create an SMB file share on your S3 File Gateway that is configured to use the S3 bucket that you created previously to store and retrieve files. You then configure a security group to allow SMB traffic to pass between the S3 File Gateway appliance and a Windows instance.

1. At the top of the AWS Management Console, in the search bar, search for and choose

Storage Gateway

.

 For this lab, you configure an SMB guest password that is used to access the SMB file share you create. In a production environment, you are much more likely to use Active Directory as an authentication source. When using Active Directory, you must ensure the following ports are opened in addition to the ones you configure in this task:

* UDP 137 - Name service
* UDP 138 - Datagram service
* TCP 389 - Directory System Agent; client connection
* TCP 636 - LDAPS - Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL)

 Refer to the AWS Storage Gateway [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/Resource_Ports.html) for additional information.

1. In the navigation menu at the left, choose **Gateways**.
2. Select the S3 File Gateway you created in Task 3.
3. Choose **Actions**, **Edit SMB settings** and **Guest access settings**.
4. On the **Edit guest access settings** screen, for **Guest password** field enter

AWSlabs1342!@

.

 In a production environment, if you were joining your S3 File Gateway to an Active Directory domain, you would do so on this screen. **You must either join the S3 File Gateway to a domain or set a guest password before you can create an SMB file share.**

1. Choose **Save changes**.

A  Successfully updated SMB guest password. message is displayed on top of the screen.

1. In the navigation menu at the left, choose **File shares**.
2. Choose **Create file share**.

 You can also create a new file share from the *File shares* section, accessible from the navigation menu at the left.

1. On the **Create file share** screen, in the **Basics** section, make the following selections:

* **Gateway:** Select **S3 File Gateway (sgw-*random alphanumeric*)** from the dropdown menu.
  + **Note:** “S3 File Gateway” may be different if you used another name for your gateway in Task 3.
* **File share type:** Select  **SMB**.
* **S3 bucket:** Select the name of the S3 bucket you created in Task 2 for use with SMB.
* **User authentication:** Select **Guest access** from the dropdown menu.

1. At the bottom of the page, choose **Customize configuration**.
2. On the **File share settings** page, scroll down and choose **Next**.
3. On the **Amazon S3 storage settings** screen, make the following selections:

* **Storage class for new objects:** Select **S3 Standard** from the dropdown menu.
* **Object metadata:**
  + Select  Guess MIME type
  + Select  Give bucket owner full control
* **Access to your S3 bucket**: Select  Use an existing IAM role
* **IAM role:** Copy the *FgwIamPolicyARN* value from the list of parameters to the left of these instructions, and then paste it into this field.

1. Choose **Next**.
2. On the **File access settings** screen, for **Authentication method**, choose **Guest access** from the dropdown menu.

**Note:** You may see a warning message about the file share being accessible by all authenticated members. It is recommended to always limit access to only the required users and groups in your environment. The **Allowed/denied users and groups** section is only available when Active Directory is selected as the authentication method.

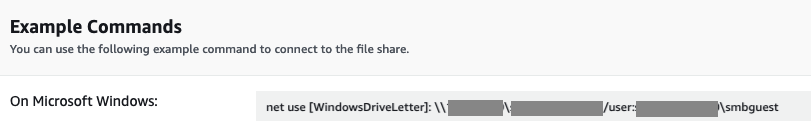
1. At the bottom of the window, choose **Next**.
2. On the **Review and create** screen, verify the configuration and choose **Create**.

A  Your file share has been created and added to the gateway. message is displayed on top of the screen.

1. Monitor the **Status** field and wait for it to change from *Updating* to *Available*, which should take less than a minute.

 You may need to choose the refresh  button at the top-right of the window.

1. Select the link to the file share you just created. At the bottom of the window, make note of the command to mount the file share on Windows. You use it for in next task.



**Congratulations!** You successfully created an SMB file share on your S3 File Gateway that is configured to use the S3 bucket that you created previously to store and retrieve files.

**Task 7: Examine the security group, mount the file share to the Windows instance, and migrate data**

Before you can being migrating data to the SMB share you created, you must first mount the share. In this task, you discover that security group rules prevent you from connecting to the file share from the Windows host. You then add the appropriate rules to the security group to enable SMB communication, mount the SMB share on a Windows host, and copy data from the instance to the file share.

1. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. On the EC2 Dashboard, choose **Instances** from the left navigation menu.
2. On the **Instances** screen, select  **VPC-A Windows Server** and choose **Connect**.
3. Choose the **RDP client** tab.

 You must have a Remote Desktop application installed on your computer to connect to the instance.

* Windows users can use the Remote Desktop application included with Windows.
* Mac users can use the Microsoft Remote Desktop app located in the App Store, or you can download the [CoRD RDP client](http://cord.sourceforge.net/).

1. Choose **Download remote desktop file** and save the file.
2. Choose **Cancel**.
3. Locate the Remote Desktop file you just downloaded, and then open it.

 The following steps to connect to the Windows host using Remote Desktop are written from a Windows system perspective. If you are using a Mac or Linux system, the prompts or buttons to choose may be slightly different than those shown here, but the general steps are the same.

1. When prompted, **The publisher of this remote connection cannot be verified. Do you want to connect anyway?** choose **Connect**.
2. When prompted for the password for the Administrator account, enter the password shown in the **WindowsAdministratorPassword** field to the left of these instructions.

 Do not use the password available in the *connect* window. The password for this instance is changed as part of the lab build process, making the default instance password invalid.

1. When prompted, **The identity of the remote computer cannot be verified. Do you want to connect anyway?** choose **Yes**.
2. On the Windows host, right-click on the Windows icon  at the bottom-left of the window, and then choose **Windows PowerShell**.
3. In the PowerShell window, enter the command you copied at the end of the previous task to mount the file share. Replace **[WindowsDriveLetter]** with

S:

 to mount the file share to drive S.

net use [WindowsDriveLetter]: \\<File-Gateway\_appliance-private-IP-address>\<S3-bucket-name> /user:<generated-user-name>\smbguest

For example:

net use S: \\10.0.3.240\smb-bucket-sgw /user:sgw-193DD270\smbguest

 This command times out after approximately five minutes because the security group is not configured to allow SMB traffic between the Windows host and the S3 File Gateway appliance. Type Ctrl+C to interrupt the command, rather than waiting for it to time out. You add the appropriate rules next.

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

System error 53 has occurred.

The network path was not found.

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

VPC

.

1. In the left navigation menu, expand the **Security** section and choose **Security groups**.
2. Select the security group named **S3 File Gateway access**.

The *S3 File Gateway access* security group is attached to the S3 File Gateway appliance instance you created previously. It currently contains rules that allow inbound traffic to the appliance on specific ports that are required to activate the appliance, as well as to allow NFS and SMB traffic from VPC-B Subnet-A. Refer to the network diagram at the beginning of these instructions for a visualization of the configuration.

 A security group operates much like a firewall that may be in your on-premises datacenter. When configuring your firewall rules, refer to the [AWS Storage Gateway documentation](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#networks) to verify the ports that you need to be open between your endpoints and the AWS Storage Gateway service.

 If you are using AWS Direct Connect, there are additional considerations when working with Storage Gateway, such as creating a Public Virtual Interface to enable communication with the public AWS Storage Gateway endpoints. Refer to the [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/using-dx.html) for more information.

1. At the bottom of the window, choose the **Inbound rules** tab, and then choose **Edit inbound rules**.
2. To the right of the **HTTP** (port 80) entry, choose **Delete** to delete the rule.

 If you performed Task 5, you have already deleted the HTTP rule.

HTTP traffic is only required when activating the S3 File Gateway appliance, and can be removed once activation is complete.

1. Choose **Add Rule**.
2. Choose the drop-down menu in the **Type** column of the new rule, and then select **SMB**.

Notice that selecting SMB automatically updates the **Protocol** column to *TCP* and sets the **Port Range** to *445*.

1. In the **Source** column, select **Custom** from the drop-down menu, then enter the IP range of Subnet-A in VPC-A in CIDR notation:

10.0.2.0/24

This rule allows traffic on port 445 to the S3 File Gateway appliance subnet from any host on the 10.0.2.0/24 subnet.

 The version of Windows you are working with in this example uses SMBv3, so you open port 445. However, in the event you need to utilize SMBv2, you want to open port 139.

1. Choose **Save rules**.

A  **Inbound security group rules successfully modified on security group (sg-046d2de01cf0f04fa | S3 File Gateway access)** message is displayed on top of the screen.

1. Return to the Remote Desktop session to the Windows host.
2. In the PowerShell window, re-run the command you copied at the end of the previous task to mount the file share. Replace **[WindowsDriveLetter]** with

S:

 to mount the file share to drive S.

net use [WindowsDriveLetter]: \\<File-Gateway\_appliance-private-IP-address>\<S3-bucket-name> /user:<generated-user-name>\smbguest

For example:

net use S: \\10.0.3.240\smb-bucket-sgw /user:sgw-193DD270\smbguest

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The command completed successfully.

1. Open File Explorer (the folder icon in the task bar at the bottom of the window), choose **This PC** in the navigation tree on the left, and verify that the **S:** drive has been mounted successfully.
2. Navigate to

C:\media\data

 and copy the 20 PNG files that are listed.

1. Paste the files into root of the **S:** drive.
2. Return to the AWS Management Console.
3. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. Choose the link to the S3 bucket you created for SMB in Task 2.
2. Verify the files you copied into the mounted SMB share are displayed in the S3 bucket. You should see 20 PNG files.

 You may need to choose the refresh  button at the top-right of the window.

 Congratulations! You have successfully copied the local data from the the Windows host to the SMB file share and S3 bucket.

Next, you access the same SMB share from a Windows host on another network (VPC-B) and discover that the data is on a shared resource.

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. On the EC2 Dashboard, choose **Instances** from the left navigation menu.
2. On the **Instances** screen, select  **VPC-B Windows Server** and choose **Connect**.
3. On the **Connect to instance** screen, select the **RDP client** tab.
4. Choose **Download remote desktop file** and save the file.
5. Choose **Cancel**.
6. Locate the Remote Desktop file you just downloaded, and then open it.
7. When prompted, **The publisher of this remote connection cannot be verified. Do you want to connect anyway?** choose **Connect**.
8. When prompted for the password for the Administrator account, enter the password shown in the **WindowsAdministratorPassword** field to the left of these instructions.

 Do not use the password available in the *connect* window. The password for this instance is changed as part of the lab build process, making the default instance password invalid.

1. When prompted, **The identity of the remote computer cannot be verified. Do you want to connect anyway?** choose **Yes**.
2. On the Windows host, right-click on the Windows icon  at the bottom-left of the window, and then choose **Windows PowerShell**.
3. In the PowerShell window, enter the command you copied at the end of the previous task to mount the file share. Replace **[WindowsDriveLetter]** with

S:

 to mount the file share to drive S.

net use [WindowsDriveLetter]: \\<File-Gateway\_appliance-private-IP-address>\<S3-bucket-name> /user:<generated-user-name>\smbguest

For example:

net use S: \\10.0.3.240\smb-bucket-sgw /user:sgw-193DD270\smbguest

**Expected output:**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* This is OUTPUT ONLY. \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The command completed successfully.

1. Open File Explorer and verify that the **S:** drive has been mounted successfully.
2. Navigate to the **S:** drive and verify the 20 PNG files you copied from the other host are listed.
3. **Delete** *1.png*.
4. Return to the AWS Management Console.
5. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. Choose the link to the S3 bucket you created for SMB in Task 2.
2. Verify **1.png** has been deleted from the bucket.

**Congratulations!** You have successfully:

* Created an SMB file share and linked it to an S3 bucket.
* Added the appropriate SMB ports to the security group to allow SMB traffic between the S3 File Gateway appliance and the Windows hosts.
* Copied local data from a Windows host to the file share and accessed that same data from a secondary host in a separate network.

**Task 8.a: Monitoring S3 File Gateway with Amazon CloudWatch**

AWS Storage Gateway is integrated with Amazon CloudWatch which monitors your AWS resources in real time, and you use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

Some of the important metrics to watch for monitoring throughput between the S3 File Gateway and AWS are **ReadBytes** and **WriteBytes**. Similarly, for monitoring cache performance, you can use metrics like **CacheHitPercent**, **CachePercentDirty** and **CachePercentUsed**. Further, you can use **CloudBytesUploaded** and **CloudBytesDownloaded** to detect possible connection failures between the S3 File Gateway and AWS.

In this task, you use Amazon CloudWatch for monitoring your S3 File Gateway resources and the metrics that were discussed above.

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

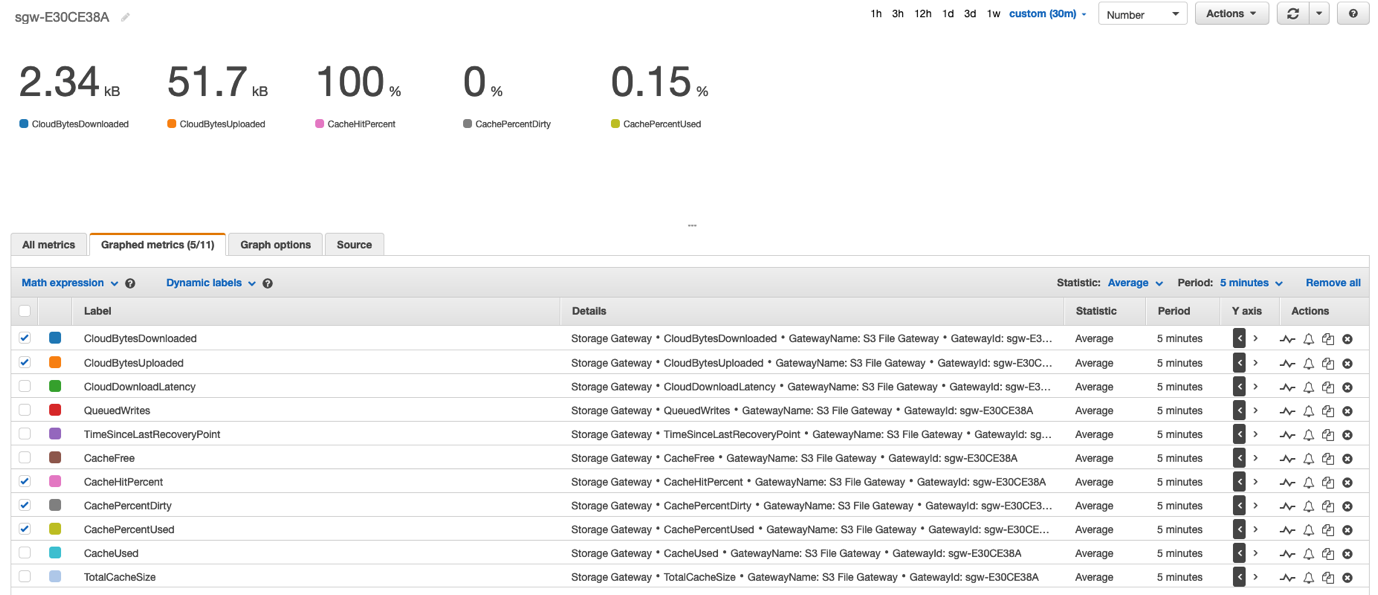
Storage Gateway

.

1. On the left menu select **Gateways**, and then choose **S3 File Gateway** that was created for this lab.
2. Scroll down to the **Details** tab, and choose CloudWatch metrics  in the **Metrics** section.

A new tab opens to the Amazon CloudWatch console. This link automatically selects the default graphed metrics for the S3 File Gateway resource.

1. Select the **Number** filter from the top-right corner of the screen (instead of Line graph), and adjust the time interval to **30 minutes** to get better results on the metrics.



From the above Number graph, review the following important metrics:

* CloudBytesDownloaded: 2.34kB
* CloudBytesUploaded: 51.7 kB

CloudBytesUploaded

 is the total number of bytes that the gateway uploaded to AWS during the reporting period.

CloudBytesDownloaded

 is the total number of bytes that the gateway downloaded from AWS during the reporting period.

* CacheHitPercent: 100%
* CachePercentUsed: 0.15%

CacheHitPercent

 is the percent of application read operations from the file shares that are served from cache. Ideally,

CacheHitPercent

 should be close to 100% and that means that your application is reading data from the cache.

CachePercentUsed

 is the file share’s contribution to the overall percent use of the gateway’s cache storage. A high

CachePercentUsed

 is good, but when this metric reaches 100%, the

CacheHitPercent

 is impacted. 100%

CachePercentUsed

 could indicate that the cache is too small for the working set.

In this case,

CachePercentUsed

 is at 0.15% which indicates that the gateway has enough cache and you need not increase the size of your gateway cache.

* CachePercentDirty: 0%

Finally, the

CachePercentDirty

 is the file share’s contribution to the overall percentage of the gateway’s cache that has not been persisted to AWS. A low

CachePercentDirty

 indicates that your Storage Gateway resource is working as expected.

 Refer to the [documentation](https://docs.aws.amazon.com/filegateway/latest/files3/monitoring-file-gateway.html#monitoring-file-gateway-resources) for more information on all the file share metrics with S3 File Gateway.

**Congratulations!** You have successfully used Amazon CloudWatch for monitoring your S3 File Gateway resource.

**Task 8.b: Analyzing S3 File Gateway information in AWS CloudTrail**

AWS 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 AWS 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.

In this task, you use AWS CloudTrail for analyzing recent events for S3 File Gateway resource that was created for this lab.

1. Return to the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

CloudTrail

.

1. In the navigation menu at the left, choose **Event history**.
2. On the Event history screen, choose the **Event source** filter from the drop-down list and filter by **storagegateway.amazonaws.com**.

Here, you see a list of all recent events associated with your S3 File Gateway resource. Below example shows an entry from the CloudTrail event that shows the **CreateNFSFileShare** action.

{

"eventVersion": "1.08",

"userIdentity": {

"type": "AssumedRole",

"principalId": "XXXXXX",

"arn": "arn:aws:sts::XXXXXXXX:assumed-role/AWSLabsUser-XXXXX/XXX",

"accountId": "XXXXXXXX",

"accessKeyId": "XXXXXXXX",

"sessionContext": {

"sessionIssuer": {

"type": "Role",

"principalId": "XXXXXXXX",

"arn": "arn:aws:iam::XXXXXXXX:role/AWSLabsUser-XXXXXXXX",

"accountId": "XXXXXXXX",

"userName": "AWSLabsUser-XXXXXXXX"

},

"webIdFederationData": {},

"attributes": {

"creationDate": "2022-01-25T16:23:15Z",

"mfaAuthenticated": "false"

}

}

},

"eventTime": "2022-01-25T18:16:36Z",

"eventSource": "storagegateway.amazonaws.com",

"eventName": "CreateNFSFileShare",

"awsRegion": "us-east-1",

"sourceIPAddress": "XX.XX.XXX.XX",

"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0",

"requestParameters": {

"readOnly": false,

"clientToken": "XXXX.XXXX",

"defaultStorageClass": "S3\_STANDARD",

"clientList": [

"192.168.2.0/24",

"10.0.2.0/24"

],

"squash": "RootSquash",

"guessMIMETypeEnabled": true,

"kMSEncrypted": false,

"requesterPays": false,

"role": "arn:aws:iam::XXXXXXXX:role/FileGatewayRole",

"objectACL": "bucket-owner-full-control",

"gatewayARN": "arn:aws:storagegateway:us-east-1:XXXXXXXX:gateway/sgw-XXXXXXXX",

"nFSFileShareDefaults": {

"ownerId": 65534,

"groupId": 65534,

"fileMode": "0666",

"directoryMode": "0777"

},

"locationARN": "arn:aws:s3:::nfs-sgw-lab",

"tags": [],

"bucketRegion": "us-east-1"

},

"responseElements": {

"fileShareARN": "arn:aws:storagegateway:us-east-1:XXXXXXXX:share/share-59E52532"

},

"requestID": "026b715d-dba4-4d1d-8238-cb000e442ee2",

"eventID": "7e541c7f-1483-4200-9ade-8aaaee088e54",

"readOnly": false,

"resources": [

{

"accountId": "XXXXXXXX",

"ARN": "arn:aws:storagegateway:us-east-1:XXXXXXXX:gateway/sgw-4132DD28"

},

{

"accountId": "XXXXXXXX",

"ARN": "arn:aws:iam::XXXXXXXX:role/FileGatewayRole"

}

],

"eventType": "AwsApiCall",

"apiVersion": "20130630",

"managementEvent": true,

"recipientAccountId": "XXXXXXXX",

"eventCategory": "Management",

"tlsDetails": {

"tlsVersion": "TLSv1.2",

"clientProvidedHostHeader": "storagegateway.us-east-1.amazonaws.com"

},

"sessionCredentialFromConsole": "true"

}

As you can see, information is provided about the user who performed the action, such as type of user, account ID, and user name. Also, information about the event such as timestamp, event name, AWS Region, the IP address of the user, along with a list of API parameters showing the configuration of the file share, such as read-only, Amazon S3 Storage class, requester pays and so forth are also provided.

 Refer the [documentation](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html) for more information on AWS CloudTrail.

**Congratulations!** You have successfully used AWS CloudTrail for analyzing recent events for S3 File Gateway resources.

**Conclusion**

**Congratulations!** You now have successfully:

* Deployed and activated an S3 File gateway appliance.
* Created an NFS file share on the S3 File Gateway and linked it to an S3 bucket.
* Configured the ports required to pass NFS traffic between the S3 File Gateway and Linux hosts in two subnets.
* Copied local data from a Linux host to the NFS file share, viewed it in the linked S3 bucket, and manipulated the data from a second Linux host.
* Created an SMB file share on the S3 File Gateway and linked it to an S3 bucket.
* Configured the ports required to pass SMB traffic between the file gateway and Linux hosts in two subnets.
* Copied local data from a Windows host to the SMB file share, viewed it in the linked S3 bucket, and manipulated the data from a second Windows host.
* Monitored different metrics for S3 File Gateway using Amazon CloudWatch.
* Analyzed recent events related to S3 File Gateway resources using AWS CloudTrail.

 The same concepts you learned in this lab also apply to the other Storage Gateway types. Refer to the AWS Storage Gateway [documentation](https://docs.aws.amazon.com/storagegateway/?id=docs_gateway) for additional information.

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

**Additional resources**

For more information about AWS Training and Certification, see [*https://aws.amazon.com/training/*](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*  
If you would like to share any feedback, suggestions, or corrections, please provide the details in our [*AWS Training and Certification Contact Form*](https://support.aws.amazon.com/#/contacts/aws-training).