Hybrid Storage and Data Migration with AWS Storage Gateway File Gateway

**SPL-223 - Version 1.0.24**

© 2024 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**

With AWS Storage Gateway, you can connect an on-premises software appliance with cloud-based storage to provide a seamless and secure integration between your on-premises IT environment and AWS’s storage infrastructure. For instance, you could securely upload data currently stored on-premises to the AWS cloud for cost effective backup and rapid disaster recovery.

The AWS Storage Gateway service is ideal for hybrid deployments and migration solutions looking to bridge traditional on-premises servers and storage protocols with cloud native services such as Amazon Simple Storage Service (Amazon S3) and Amazon Elastic Block Store (Amazon EBS). Customers can connect to AWS Storage Gateway in a number ways, such as file-based access, block level access, and virtual tape access.

In this lab, you use the File Gateway service to attach an NFS mount to an on-premises data store and replicate that data to an Amazon S3 bucket. Additionally, you configure advanced Amazon S3 features: S3 Lifecycle Policies and Cross-Region Replication (CRR).

This lab is spread over three regions representing the on-premises data center, the backup region where the File Gateway runs, and a third region that is used for S3 CRR allowing the data stored in the backup region to be replicated securely to a region closer to another set of customers.

TOPICS COVERED

By the end of this lab, you will know how to:

* Configure an AWS Storage Gateway file gateway with an NFS file share and attach it to a Linux instance.
* Migrate a set of data from the Linux instance to an S3 bucket.
* Create and configure a primary S3 bucket to migrate on-premises server data to.
* Create and configure a secondary S3 bucket to use for Cross-Region Replication.
* Create an S3 replication policy to automatically replicate data from an S3 bucket to another S3 bucket in a separate region.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with basic navigation of the AWS Management Console and be comfortable with basic Linux CLI commands.

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.

**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:

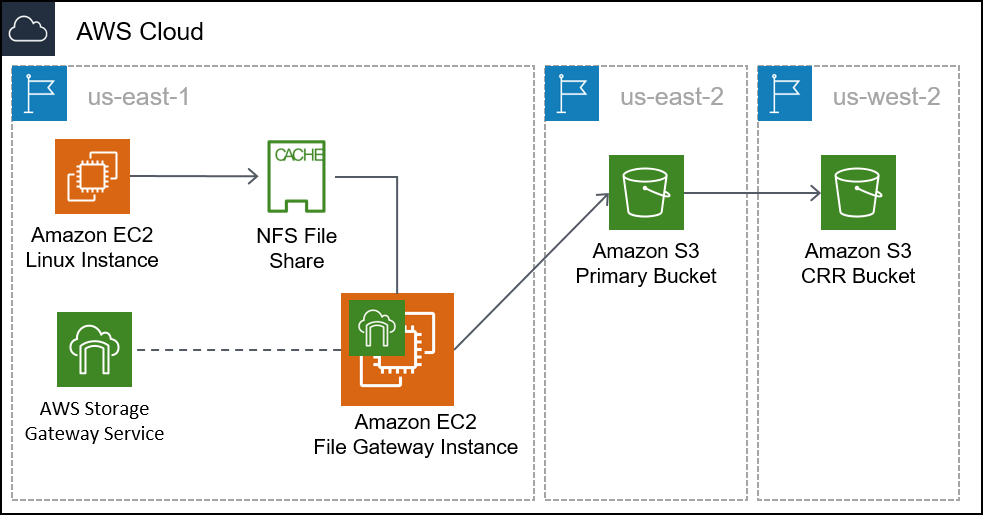
* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

**Task 1: Review the lab architecture**

This lab environment uses three AWS Regions in total. A Linux Amazon Elastic Compute Cloud (Amazon EC2) instance to emulate an on-premises server is deployed to the us-east-1 (N. Virginia) region. The Storage Gateway virtual appliance is deployed to the same region as the Linux instance. In a real-world scenario, the appliance would be deployed in a VMware vSphere or Microsoft Hyper-V environment, or as a physical Storage Gateway appliance.

You create the primary S3 bucket in the us-east-2 (Ohio) region, which is where the data from the Linux instance is copied to.

You create the secondary S3 bucket in the us-west-2 (Oregon) region, which is the target for the S3 Cross-Region Replication policy.



**Congratulations!** You have reviewed the lab architecture.

**Task 2: Create the primary and backup S3 buckets**

Before configuring the file gateway, you must create the Amazon S3 bucket to replicate the data to. In this task, you create the primary S3 bucket in the us-east-2 (Ohio) region, as well as an S3 bucket in the us-west-2 (Oregon) region that is be used for Cross-Region Replication.

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

s3

.

1. Choose **Create bucket** .
2. In the **Create bucket** wizard window:

* For **Bucket name**, create a name for the primary S3 bucket that you can easily remember. It must be globally unique.
* For **Region**, select

US East (Ohio) us-east-2

 from the drop-down menu.

* For **Bucket Versioning**, select  Enable.

**Note:** *Versioning is a requirement on both the source and destination buckets for S3 Cross-Region Replication.*

1. Choose **Create bucket** .

**Expected service output:**

**Successfully created bucket “your-bucket-name-here”**

1. In the upper-left of your screen, choose **Amazon S3**.
2. Repeat the previous steps to create a second bucket with the following configuration:

* For **Bucket name**, create a name for the secondary (CRR target) bucket that you can easily remember. It must be globally unique.
* For **Region**, select

US West (Oregon) us-west-2

 from the drop-down menu.

* Enable Versioning.

**Expected service output:**

**Successfully created bucket “your-bucket-name-here”**

**Congratulations!** You have successfully created the Amazon S3 buckets to use with the file gateway and S3 Cross-Region Replication.

**Task 3: Enable Cross-Region Replication**

Now that the S3 buckets are created and versioning is enabled on both, you can create a Replication Policy. A Replication Policy defines a bucket, or objects in a bucket, you wish to replicate from, and which bucket to replicate to.

1. Choose the link with name of the **source bucket** you created in the US East (Ohio) region to view more information and settings for the bucket.
2. On the bucket overview page, choose the **Management** tab.
3. Under **Replication rules**, choose **Create replication rule** .

* For **Replication rule name**, enter

crr-full-bucket

* For **Status** make sure  **Enabled** is selected
* Under **Source bucket**, for **Choose a rule scope**, select **Apply to all objects in the bucket**.
* Under **Destination**, for **Bucket name** click **Browse S3**
* Select  **Destination bucket** and click **Choose path**
* For **IAM role**, select

S3-CRR-Role

 from the drop-down menu

**Note:** The IAM role defines the IAM permissions that the Amazon S3 service can use to replicate data between the two buckets you select. IAM roles and associated policies should always be configured with the principle of least privilege in mind. The following snippet shows the permissions included in the *S3-CRR-Role* role:

{

"Version": "2012-10-17",

"Statement": [

{

"Action": [

"s3:Get\*",

"s3:ListBucket",

"s3:ReplicateObject",

"s3:ReplicateDelete",

"s3:ReplicateTags",

"s3:GetObjectVersionTagging"

],

"Resource": "\*",

"Effect": "Allow"

}

]

}

1. Review the replication rule settings, and then choose **Save** .
2. After you save your replication rule, a pop-up window will display asking if you want to “replicate existing objects”. As there are no objects currently in your bucket, you can leave the default selection of “No, do not replicate existing objects” and choose **Submit** .

Next, upload a file to the primary S3 bucket you created to verify the replication policy is working properly.

1. Choose **S3SourceBucketName** at the top where you can observe **Amazon S3 > Buckets > S3SourceBucketName > Replication rules** to return to the overview page for the bucket you created in the US East (Ohio) region.
2. Choose **Upload** .
3. Choose **Add files** and then select a file from your local computer to upload to the bucket.

**Note:** For the purposes of this lab, use a small file that does not contain sensitive information, such as a blank text file.

1. Scroll down to the bottom of the page and choose **Upload** .

**Expected service output:**

**Upload succeeded**

1. After the file uploads, navigate to the bucket you created in the US West (Oregon) region. To do so, at the top-left corner of the page choose , and then choose **Buckets** from the left navigation menu.
2. Select the link with the name of the secondary bucket you created in the US West (Oregon) region.

You should see that the file you uploaded has been copied to this bucket as well.

**Note:** You may need to choose the refresh  button at the top of the window.

**Congratulations!** You have successfully created an S3 replication policy to replicate data from a bucket in the US East (Ohio) region to a bucket in the US West (Oregon) region, also known as S3 Cross-Region Replication.

**Task 4: Configure the file gateway and create an NFS file share**

You are now ready to deploy and configure the Storage Gateway file gateway appliance.

In this task, you deploy a Storage Gateway file gateway appliance as an Amazon EC2 instance. You then configure a cache disk, select an S3 bucket to synchronize your on-premises files to, and select an IAM policy to use. Finally, you create an NFS file share on the file gateway.

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

Storage Gateway

.

**Note:** You can also search for

Storage Gateway

 at the top of the Services menu.

In case you are prompted with an AWS Storage Gateway getting started page, this page is displayed because the Storage Gateway service has not been configured in this region.

1. At the top-right of the page, verify the current region is **N. Virginia** .
2. Choose **Create gateway**.
3. On the **Set up gateway** page under **Gateway settings** section make the following selections:

* For **Gateway name**, enter

File Gateway

* For **Gateway time zone**, select

GMT -5:00 Eastern Time (US & Canada), Bogota, Lima

 from the drop-down menu

1. Under **Gateway options** section:

* For **Gateway type**, select

Amazon S3 File Gateway

.

1. Under **Platform options** section:

* For **Host Platform**, select

Amazon EC2

.

* For **Launch EC2 instance**, choose **Customize your settings .**

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

**Note:** The browser opens a new tab 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.

1. Under **Name and tags** section, enter

File Gateway Appliance

 for the **Name** field.

1. In order to propagate the **Name** tag to other resource types, choose the Add additional tags link , and under **Resource types** choose

Instances

,

Volumes

 and

Network interfaces

 from the drop-down menu.

1. Under **Application and OS Images (Amazon Machine Image)**, it should already have the correct AMI selected with a name that starts with **aws-storage-gateway**.
2. Under **Instance type** section, select the **t2.xlarge** instance type from the drop-down menu.

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

1. Under **Key pair (login)** section, for **Key pair name**, select an existing keypair from the drop-down menu (E.g. AWSLabsKeyPair-xxxxx).

**Note:** This is the key pair that is provided to the left of these instructions under **EC2 Key Pair Private Key**.

1. Under **Network Settings** section, choose **Edit** and configure the following selections:

* For **VPC**, select

On-Prem-VPC

 from the drop-down menu

* For **Subnet**, select

On-Prem-Subnet

 from the drop-down menu

* For **Auto-assign Public IP**, select

Enable

 from the drop-down menu

* For **Firewall (security groups)**, choose **Select existing security group** and choose the Security Group with

FileGatewayAccess

 in the name from the drop-down menu

* + This security group is configured to allow ingress (incoming) traffic through ports 80 (HTTP), 443 (HTTPS), and 2049 (NFS). These ports allow for activation of the File Gateway appliance and for connectivity from the Linux server to the NFS share you will create on the File Gateway. It also allows egress (outgoing) traffic on port 443 (HTTPS) to allow for communication with the AWS Storage Gateway service endpoints.

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

1. Under **Configure storage** section, choose Advanced, then choose **Add new volume** and configure the following:

* For **Storage type**, make sure

EBS

 is selected

* For **Device name**, keep the default selection of

/dev/sdb

* For **Size (GiB)**, enter

150

* For **Volume type**, select

General purpose SSD (gp3)

 from the drop-down menu

* For **Delete on termination**, select

Yes

 from the drop-down menu

1. Under **Summary** section, ensure that **Number of instances** is set to

1

.

1. Choose **Launch instance**
2. At the bottom-right of the page, choose **View all instances**
3. The

File Gateway Appliance

 instance takes a few minutes to deploy. Monitor the status of the deployment and wait for **Status check** to show  2/2 checks passed.

**Note:** You may need to choose the refresh  button at the top-right of the page to see the checks status update.

1. Select the File Gateway Appliance instance from the list. At the bottom of the page, locate the **Public IPv4 address** and copy the IP address listed. You will use it when finalizing the File Gateway deployment.
2. Return to the **AWS Storage Gateway** tab in your browser. It should still be at the **Set up gateway** page.
3. In **Platform options** section, verify **Amazon EC2** is selected, and then select  **I completed all the steps above and launched the EC2 instance** checkbox to confirm the gateway setup.
4. Choose **Next** .
5. On the **Connect to AWS** page configure the following options:

* For **Endpoint options** section, choose **Publicly accessible**.
* For **Gateway connection options** section, choose **IP address** and enter the **Public IPv4 address** that you copied from your file gateway appliance instance.

1. Select **Next** .

**Note:** If the next page fails to load, wait a couple of minutes and then refresh the page. The file gateway appliance instance may still be initializing.

1. On the **Review and activate gateway** page, review the settings and then select **Activate** .

**Expected service output:**

**Successfully activated gateway File Gateway**

1. On the **Configure gateway** page make the following selections:

* For **Configure cache storage** section, wait for *local disks* to finish processing (approximately 1 minute), and then for **Allocated to**, select **Cache** .
* For **CloudWatch log group** section, select  **Deactivate Logging**.

1. Choose **Configure** .

**Expected service output:**

**Successfully created gateway File Gateway**

**Note:** Wait for the File Gateway status to change to  Running (approximately 1-2 minutes).

You can now create an NFS file share on the file gateway.

1. On the **Gateway overview** screen, choose **Create file share** .
2. On the **Create file share** page:

* For **Gateway**, select the name of the gateway you just created **File Gateway** (if you are following this guide).
* For **File share protocol**, select  **NFS**.
* For **S3 bucket**, Choose S3 bucket you created in the US East (Ohio) region in Task 1.

1. Choose **Customise configuration**
2. On the **File share settings configuration** page:

* For **Gateway**, select the name of the gateway you just created **File Gateway** (if you are following this guide).
* For **Amazon S3 location**, choose  **S3 bucket name** and enter the name of the bucket you created in the US East (Ohio) region in Task 1.
* For **AWS region** select **US East (Ohio) us-east-2** as the region you created for your source S3 bucket.
* For **Access objects using**, select  **Network File System (NFS)**.

1. Leave all remaining options with their default values.
2. Choose **Next** .
3. On the **Amazon S3 storage settings** page:

* For **Storage class for new objects**, select **S3 Standard** .
* For **Object metadata** configure the following options:
  + Select  **Guess MIME type**.
  + Select  **Gateway files acccessible to S3 bucket owner**.
  + Deselect  **Enable requester pays**.
* For **Access to your S3 bucket**, select  **Use an existing IAM role**.
* For **IAM role**, copy the *FgwIamPolicyARN* value at the left of these instructions, and then paste it into this field.

**Note:** The IAM role defines the IAM permissions that the file gateway can use to access the S3 bucket you define in the wizard. IAM roles and associated policies should always be configured with the principle of least privilege in mind. The following snippet shows the permissions included in the role used in this lab:

{

"Version": "2012-10-17",

"Statement": [

{

"Action": [

"s3:AbortMultipartUpload",

"s3:DeleteObject",

"s3:DeleteObjectVersion",

"s3:GetAccelerateConfiguration",

"s3:GetBucketLocation",

"s3:GetBucketVersioning",

"s3:GetObject",

"s3:GetObjectAcl",

"s3:GetObjectVersion",

"s3:ListBucket",

"s3:ListBucketVersions",

"s3:ListBucketMultipartUploads",

"s3:ListMultipartUploadParts",

"s3:PutObject",

"s3:PutObjectAcl"

],

"Resource": "\*",

"Effect": "Allow"

}

]

}

1. For **Encryption** choose  **S3-Managed Keys (SSE-S3)**
2. Choose **Next** .

**Note:** A warning message about the file share being accessible from anywhere is displayed. In a production environment you should always create policies that are as restrictive as possible to prevent unwanted or malicious connections to your instances.

Let’s secure this file share.

1. In **Access object** section, choose **Add client** .
2. Copy the value of **OnPremLinuxInstanceIP** shown to the left of these instructions.

This is the private IP address of the on-premises Linux instance that you connect to the file share in the next task.

1. Paste the **OnPremLinuxInstanceIP** which you copied in the previous step, in the **Allowed client’s** box.
2. At the bottom-right of the page, choose **Next** .
3. Choose **Create** .

**Expected service output:**

**Successfully created file share share-7A1ECC10.**

1. Monitor the status of the deployment and wait for **Status** to change to *Available*, which takes less than a minute.

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

1. Select the file share ID link you just created. At the bottom of the page, make note of the command to mount the file share **On Linux**. You will need it for the next task.

**Congratulations!** You have successfully deployed and configured a file gateway appliance and created an NFS file share on the appliance.

**Task 5: Mount the file share to the Linux instance and migrate the data**

You must first mount the NFS file share before you can begin migrating data to it. In this task, you mount the NFS share on a Linux server, and then copy data to the share.

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

EC2

.

1. On the Amazon EC2 dashboard, choose **Instances**.
2. Select **On-Prem Linux Server** and then choose **Connect** .
3. In the **Connect to instance** window, choose the **EC2 Instance Connect** tab. Leave the default **User name** as

ec2-user

 and choose **Connect** .

A new window opens with an SSH session to the instance.

The URL uses EC2 Instance Connect to create an SSH connection to the EC2 instance. Refer to the *Additional resources* section at the end of the lab for more information.

1. **Command:** On the Linux instance, enter the following command to view the data that exists on this server. 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. **Command:** Enter the following command to create a new directory that you use to synchronize data with your S3 bucket.

sudo mkdir -p /mnt/nfs/s3

**Expected output:**

*None, unless there is an error.*

1. **Command:** Enter the following command to mount the NFS file share on the Linux instance. This is the command that you copied at the end of the last task, with *sudo* added at the beginning and the path to the directory you created at the end.

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

OR

sudo [Replace with "On Linux" mount command copied during previous task] /mnt/nfs/s3

For example the command should be similar to below after replacing variables:

sudo mount -t nfs -o nolock,hard 10.10.1.33:/lab-nfs-bucket /mnt/nfs/s3

**Expected output:**

*None, unless there is an error.*

1. **Command:** Enter the following command to verify the share was mounted.

df -h

The *df* command outputs a summary of disk space statistics for all disks attached to the host. The *-h* tag displays the output in an easier to read format.

**Expected output:**

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

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

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

Filesystem Size Used Avail Use% Mounted on

devtmpfs 471M 0 471M 0% /dev

tmpfs 479M 0 479M 0% /dev/shm

tmpfs 479M 464K 478M 1% /run

tmpfs 479M 0 479M 0% /sys/fs/cgroup

/dev/nvme0n1p1 8.0G 1.3G 6.8G 16% /

tmpfs 96M 0 96M 0% /run/user/0

tmpfs 96M 0 96M 0% /run/user/1000

10.10.1.60:/spl-sgw-prim 8.0E 0 8.0E 0% /mnt/nfs/s3

1. **Command:** Now that the mount point has been created, enter the following command to copy the sample data from the host 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’

Next, verify the data you copied into the NFS file share was migrated to the S3 bucket.

1. Return to your browser tab with 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 with the name of the bucket you created in the US East (Ohio) region and verify the 20 image files are listed.

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

1. Return to the main S3 dashboard with the list of buckets.
2. Choose the link with the name of the bucket you created in the US West (Oregon) region.

Verify the files you copied to the primary bucket replicated here per the policy you created previously.

**Congratulations!** You have successfully mounted the NFS file share on a Linux instance, copied sample data into it, and verified that the data is replicated to both S3 buckets.

**Conclusion**

**Congratulations!** You have successfully:

* Configured an AWS Storage Gateway file gateway with an NFS file share and attached it to a Linux instance.
* Migrated a set of data from the Linux instance to an S3 bucket.
* Created and configured a primary S3 bucket to migrate on-premises server data to.
* Created and configured a secondary S3 bucket to use for Cross-Region Replication.
* Created an S3 replication policy to automatically replicate data from an S3 bucket to another S3 bucket in a separate region.

After your data is stored in S3, you can act on it just like native S3 data. In this lab, you created a replication policy to copy the data to a secondary region. You could perform other operations as well, such as configuring a lifecycle policy to automatically migrate infrequently used data from S3 Standard to S3 Glacier for long term storage, reducing costs.

For more information, please visit the relevant product pages linked in the *Additional resources* section at the end of the lab.

**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**

* [Amazon S3](https://aws.amazon.com/s3/?nc2=h_m1)
* [Amazon S3 Glacier](https://aws.amazon.com/glacier/?nc2=h_m1)
* [Amazon S3 security](https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html)
* [AWS Storage Gateway](https://aws.amazon.com/storagegateway/?nc2=h_m1)
* [AWS Storage Gateway Hardware and Storage Requirements](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#requirements-hardware-storage)
* [AWS Storage Gateway Network and Firewall Requirements](https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html#networks)
* [EC2 Instance Connect](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html)

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).