

# Guided Lab: Configuring Hybrid Storage and Migrating Data with AWS Storage Gateway S3 File Gateway

## Lab overview and objectives

In this lab, you use AWS Storage Gateway Amazon Simple Storage Service (Amazon S3) File Gateway to attach a network file system (NFS) mount to an on-premises data store. You then replicate that data to an S3 bucket on Amazon Web Services (AWS). Additionally, you configure advanced Amazon S3 features, such as Amazon S3 lifecycle policies and cross-Region replication.

After completing this lab, you should be able to do the following:

- Configure an S3 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 AWS.
- Create and configure a secondary S3 bucket to use for cross-Region replication.
- Create an S3 lifecycle policy to automatically manage data in a bucket.

## Duration

This lab requires approximately **90 minutes** to complete.

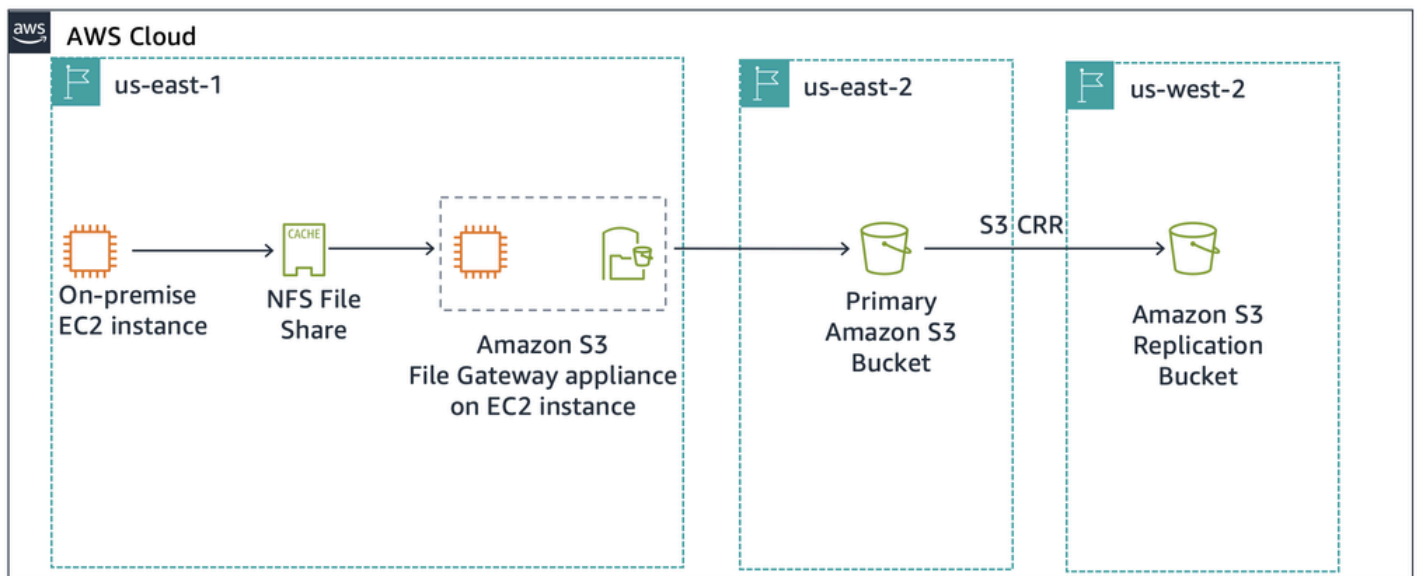
## Task 1: Reviewing the lab architecture

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

The primary S3 bucket is created in the US East (Ohio) us-east-2 Region. Data from the Linux host is copied to the primary S3 bucket. This bucket can also be called the source.

The secondary S3 bucket is created in the US West (Oregon) us-west-2 Region. This secondary bucket is the target for the cross-Region replication policy. It can also be called the destination.

The following architecture diagram shows the deployment of S3 File Gateway by using Storage Gateway services, an Amazon EC2 gateway appliance, and Amazon S3 cross-Region replication.



## Task 2: Creating the primary and secondary S3 buckets

Before you configure S3 File Gateway, you must create the primary S3 bucket (the source) where you replicate the data. You must also create the secondary S3 bucket (the destination) that is used for cross-Region replication.

1. On the AWS Management Console, in the search box, enter and choose S3 to open the Amazon S3 console.
2. Choose **Create bucket**.
3. To create the primary (or source) bucket, on the **Create bucket** page, configure the following settings:
  - **AWS Region:** Choose the **US East (Ohio) us-east-2** Region.
  - **Bucket name:** Create a name that you can remember. It must be globally unique.
  - **Bucket Versioning:** Choose **Enable**.
4. **Tip:** For cross-Region replication, you must enable versioning for both the source and destination buckets.
5. Choose **Create bucket**.
6. To create the secondary (or destination) bucket, repeat the previous steps in this task to configure the following options:
  - **AWS Region:** Choose the **US West (Oregon) us-west-2** Region.
  - **Bucket name:** Create a name that you can remember. It must be globally unique.
  - **Bucket Versioning:** Choose **Enable**.
7. Choose **Create bucket**.

## Task 3: Enabling cross-Region replication

Now that you have created your two S3 buckets and have enabled versioning on them, you create a replication policy.

1. Choose the name of the source bucket that you created in the US East (Ohio) us-east-2 Region.

2. Choose the **Management** tab, and in the **Replication rules** section, choose **Create replication rule**.
3. On the **Create replication rule** page, configure the following options:
  - In the **Replication rule configuration** section, configure the following options:
    - For **Replication rule name**, enter **crr-full-bucket**.
    - For **Status**, choose **Enabled**.
  - In the **Source bucket** section, for **Choose a rule scope**, choose **Apply to all objects in the bucket**.
  - In the **Destination** section, configure the following options:
    - Choose **Choose a bucket in this account**.
    - Choose **Browse S3**, and then choose the destination bucket that you created in the US West (Oregon) us-west-2 Region.
    - Choose **Choose path**.
  - In the **IAM role** section, in the search box, enter **S3-CRR** and choose **S3-CRR-Role**. (This role was pre-created with the required permissions for this lab.)
4. Choose **Save**.

**Note:** You might see a **Replicate existing objects?** window with a message about enabling a one-time batch operations job from this replication configuration. Leave the default option selected, and choose **Submit**.

Replicate existing objects?

×

You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. [Learn more](#) or [see pricing](#)

Existing objects

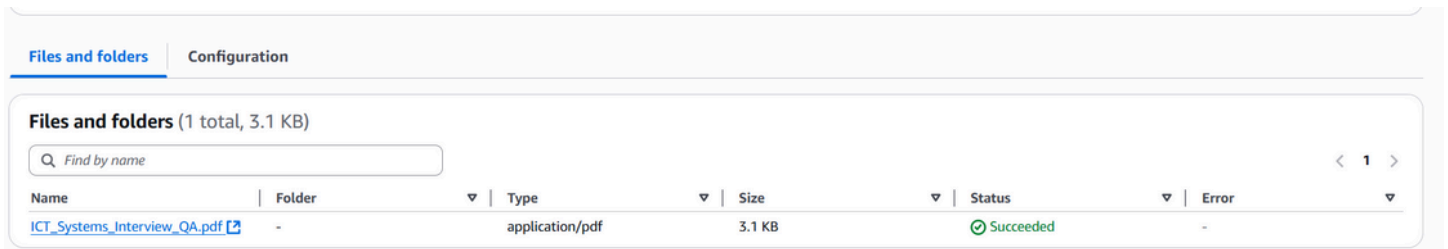
☐ No, do not replicate existing objects.

☒ Yes, replicate existing objects.

Cancel

Submit

1. Return to the source bucket that you created in the US East (Ohio) us-east-2 Region.
2. To upload a file from your local computer to the bucket, choose **Upload**.
3. For this lab, use a small file that does not contain sensitive information, such as a blank text file.
4. Choose **Add files**, navigate to the file, and choose your file.
5. Choose **Upload**.
6. Wait for the file to upload, and then return to the destination bucket that you created in the US West (Oregon) us-west-2 Region. The file that you uploaded should be copied to this bucket.
7. **Note:** For the object to appear, you might need to refresh the console.



## Task 4: Configuring the S3 File Gateway and creating an NFS file share

In this task, you deploy the S3 File Gateway appliance as an EC2 instance. You then configure a cache disk, choose an S3 bucket to synchronize your on-premises files to, and choose an AWS Identity and Access Management (IAM) policy to use. Finally, you create an NFS file share on the S3 File Gateway.

1. On the AWS Management Console, in the search box, enter and choose Storage Gateway to open the Storage Gateway console.
2. In the upper-right of the console, verify that the current Region is **N. Virginia**.
3. Choose **Create gateway**, and then configure the following settings for **Step 1: Set up gateway**:
  - **Gateway name**: Enter File Gateway.
  - **Gateway time zone**: Choose **GMT -5:00 Eastern Time (US & Canada), Bogota, Lima**.
  - **Gateway type**: Choose **Amazon S3 File Gateway**.
  - **Host platform**: Choose **Amazon EC2**, and then for **Launch EC2 instance** choose **Customize your settings**.
4. In the **Set up gateway on Amazon EC2** section, choose **Launch instance**.
5. A new browser tab opens to the Amazon EC2 launch instance wizard on the Amazon EC2 console. This link automatically chooses the correct Amazon Machine Image (AMI) that must be used for the S3 File Gateway appliance.
6. On the **Launch an instance** page, configure the following options:
  - In the **Name and tags** section, for **Name**, enter File Gateway Appliance.
  - In the **Application and OS Images (Amazon Machine Image)** section, for **AMI from catalog**, accept the default **aws-storage-gateway** AMI.
  - In the **Instance type** section, from the **Instance type** dropdown list, choose the **t2.xlarge** instance type.
  - **Note**: t2.xlarge is the only instance type that you can choose in this lab environment. Choosing any other instance type results in an error message when you attempt to launch the instance.
  - **Tip**: The t2.xlarge instance type is used only as an example in this lab. For more information about correct appliance sizing when you deploy a Storage Gateway appliance, see the [Storage Gateway documentation](#).
  - In the **Key pair (login)** section, for **Key pair name - required**, choose the existing **vockey** key pair.

- **Note:** This SSH key pair is provided with the instructions for this lab. To see the key pair, at the top of these instructions, choose **Details**, and then choose **Show**.
  - Next, you configure the network and security group settings for the instance.
7. On the same page, in the **Network settings** section, choose **Edit**, and then configure the following options:
- For **VPC - required**, choose **On-Prem-VPC**.
  - For **Subnet**, choose **On-Prem-Subnet**.
  - For **Auto-assign public IP**, choose **Enable**.
  - For **Firewall (security groups)**, choose **Select existing security group**.
  - For **Common security groups**, configure the following options:
    - From the dropdown list, choose the security group with **FileGatewayAccess** in the name.
  - **Note:** This security group is configured to allow traffic through ports 80 (HTTP), 443 (HTTPS), 53 (DNS), 123 (NTP), and 2049 (NFS). These ports enable the activation of the S3 File Gateway appliance. They also enable connectivity from the Linux server to the NFS share that you create on the S3 File Gateway.
  - For more information about the ports used by Storage Gateway, see the [Storage Gateway documentation](#).
    - Also choose the security group with **OnPremSshAccess** in the name.
  - **Note:** This security group is configured to allow Secure Shell (SSH) connections on port 22.
    - Verify that you have chosen both security groups. Details on each security group appear in boxes in the console.
  - **Tip:** To see both security groups, you might need to choose **Show all selected**.
  - Next, you configure the storage settings for the instance.
8. On the same page, in the **Configure storage** section, notice that there is already an entry to create one 80 GiB gp3 root volume, and configure the following options:
- Choose **Add new volume**.
  - For the size of the volume, enter 150 GiB.
9. On the same page, in the **Summary** panel, keep the number of instances set to 1, and choose **Launch instance**.
10. A *Success* message displays.
11. Choose View all instances.
12. Your **File Gateway Appliance** instance will take a few minutes to initialize.
13. Monitor the status of the deployment, and wait for the **Status Check** to complete and say *2/2 checks passed*.
14. **Tip:** To check the status of the instance, choose refresh .
15. Choose your **File Gateway Appliance** instance.
16. On the **Details** tab, locate the **Public IPv4 address**, and copy it.
17. You use this IP address when you complete the S3 File Gateway deployment.
18. Return to the Storage Gateway browser tab. It should still be on the **Set up gateway on Amazon EC2** section.
19. At the bottom of the page, for **Confirm set up gateway**, select **I completed all the steps above and launched the EC2 instance**.
20. Choose Next.
21. For **Step 2: Connect to AWS**, configure the following options:

- In the **Gateway connection options** section, for **IP address**, enter the public IPv4 address that you copied in the previous steps from your **File Gateway Appliance** instance.
  - In the **Endpoint options** section, for **Service endpoint**, choose **Publicly accessible**.
22. Choose **Next**.
23. For **Step 3: Review and activate**, choose **Activate gateway**.
24. A *Successfully activated gateway File Gateway* message displays.
25. On the **Step 4: Configure gateway** page, in the **Configure cache storage** panel, you see a message indicating that the local disks are loading.
26. Wait for the local disks status to show that it finished processing (approximately 1 minute) before continuing to the next step.
27. For **Step 4: Configure gateway**, configure the following options:
- **CloudWatch log group**: Choose **Deactivate logging**.
  - **CloudWatch alarms**: Choose **No alarm**.
28. Choose **Configure**.
29. A *Successfully created gateway File Gateway* message displays.
30. Wait for the **Status** of the File Gateway to change to *Running* (approximately 1–2 minutes). Once the status is *Running*, you create a file share.
31. Select **File Gateway**, and then choose **Create file share**.
32. On the **Create file share** configuration page, choose **Customize configuration**.
33. For **Step 1: File share settings**, configure the following options:
- For **Gateway**, choose the name of the S3 File Gateway that you just created (which should be **File Gateway**).
  - For **Amazon S3 bucket name**, enter the name of the source bucket that you created in the US East (Ohio) us-east-2 Region.
  - For **AWS Region**, choose **US East (Ohio) us-east-2**.
  - For **Access objects using**, choose **Network File System (NFS)**.
34. Choose **Next**.
35. For **Step 2: Amazon S3 storage settings**, configure the following options:
- **Storage class for new objects**: Choose **S3 Standard**.
  - **Object metadata**: Select only **Guess MIME type** and **Gateway files accessible to S3 bucket owner**.
  - **Access your S3 bucket**: Choose **Use an existing IAM role**.
  - **IAM role**: To enter the value for **FgwIamPolicyARN**, follow these instructions:
    - At the top of these instructions, choose **Details**.
    - Choose **Show**.
    - Copy the **FgwIamPolicyARN** value, and paste it in the **IAM role** box on the **Step 2: Amazon S3 storage settings** page.
36. Choose **Next**.
37. **Note:** On the **Step 3: File access settings** page, you might get a warning message indicating that the file share is accessible from anywhere. For this lab, you can safely disregard this warning. In a production environment, you should always create policies that are as restrictive as possible to prevent unwanted or malicious connections to your instances.
38. On the **Step 3: File access settings** page, accept the default settings, and choose **Next**.
39. At the bottom of the **Step 4: Review and create** page, choose **Create**.

40. Monitor the status of the deployment, and wait for the **Status** to change to *Available*, which takes less than 1 minute.
41. **Note:** To check the status, choose refresh .
42. Choose the file share that you just created.
43. From **Example Commands**, copy the command for **On Linux**, which is similar to the following:
44. `mount -t nfs -o nolock,hard 10.10.1.124:/lab36ohioueast2 [MountPath]*`
45. You need this command in the next task.

## Task 5: Mounting the file share to the Linux instance and migrating the data

Before you can migrate data to the NFS share that you created, you must first mount the share. In this task, you mount the NFS share on a Linux server and then copy data to the share.

1. To connect to the **On-Prem Linux Server** instance, at the top of these instructions, choose **Details** and then choose **Show**.
2. Copy the value for **InstanceSessionURL**, and paste it into a new browser tab to connect to the EC2 instance by using Session Manager, a capability of AWS Systems Manager.
3. You should now be connected to the instance.
4. On the Linux instance, to view the data that exists on this server, run the following command:
5. `sudo su -l ec2-user`
6. `ls /media/data`
7. You should see 20 image files in the .png format.
8. To create the directory that will be used to synchronize data with your S3 bucket, run the following command:
9. `sudo mkdir -p /mnt/nfs/s3`
10. To mount the file share on the Linux instance, enter the command that you copied at the end of the previous task. In the command, replace the value for *[MountPath]* with the following:
11. `/mnt/nfs/s3*`
12. Use sudo to run your adjusted command. Your adjusted command should look similar to the following:
13. `sudo mount -t nfs -o nolock,hard 10.10.1.33:/lab-nfs-bucket /mnt/nfs/s3`
14. To verify that the share was mounted correctly, run the following command:
15. `df -h`
16. You have now created the mount point.
17. To copy the data that you want to migrate to Amazon S3 into the share, run the following command:
18. `cp -v /media/data/*.png /mnt/nfs/s3`



The screenshot shows a terminal window within the AWS Management Console. The terminal displays the following commands and output:

```
ec2-user@ip-10-10-1-48 ~]$ ls /media/data
1.png 10.png 11.png 12.png 13.png 14.png 15.png 16.png 17.png 18.png 19.png 2.png 20.png 3.png 4.png 5.png 6.png 7.png 8.png 9.png
ec2-user@ip-10-10-1-48 ~]$ sudo mkdir -p /mnt/nfs/s3
ec2-user@ip-10-10-1-48 ~]$ sudo mount -t nfs -o nolock,hard 10.10.1.89:/primarybucket0011 /mnt/nfs/s3*
ec2-user@ip-10-10-1-48 ~]$ df -h
filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0   4.0M   0% /dev
tmpfs           475M   0   475M   0% /dev/shm
tmpfs           190M  436K   190M   1% /run
/dev/xvda1       8.0G  1.6G   6.5G  20% /
tmpfs           475M   0   475M   0% /tmp
/dev/xvda128     10M   1.3M   8.7M  13% /boot/efi
tmpfs           95M   0    95M   0% /run/user/0
10.10.1.89:/primarybucket0011 8.0E   0   8.0E   0% /mnt/nfs/s3
ec2-user@ip-10-10-1-48 ~]$ cp -v /media/data/*.png /mnt/nfs/s3
'/media/data/1.png' -> '/mnt/nfs/s3/1.png'
'/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/2.png' -> '/mnt/nfs/s3/2.png'
'/media/data/20.png' -> '/mnt/nfs/s3/20.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'
ec2-user@ip-10-10-1-48 ~]$
```

## Task 6: Verifying that the data is migrated

You have finished configuring the gateway and copying data into the NFS share. Now, you verify that the configuration works as intended.


1. On the AWS Management Console, in the search box, enter and choose S3 to go to the Amazon S3 console.
2. Choose the source bucket that you created in the US East (Ohio) us-east-2 Region, and verify that the 20 image files are listed.
3. **Note:** In the console, you might need to choose refresh .
4. Return to the S3 buckets page, and choose the destination bucket that you created in the US East (N. Virginia) us-east-1 Region. Verify that the images files replicated to this bucket based on the policy that you created earlier.
5. **Note:** Amazon S3 object replication can take up to 15 minutes to complete. Continue to refresh the page until you see the replicated objects.



## Objects (21)



Copy S3 URI

 Copy URL

Download

Open 

Delete

Actions ▼

Create folder








Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

🔍 Find objects by prefix

☐ Show versions

< 1 > 

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	 <a href="#">4.png</a>	png	August 4, 2025, 12:40:05 (UTC+03:00)	3.6 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">5.png</a>	png	August 4, 2025, 12:40:05 (UTC+03:00)	4.1 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">6.png</a>	png	August 4, 2025, 12:40:05 (UTC+03:00)	5.0 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">7.png</a>	png	August 4, 2025, 12:40:06 (UTC+03:00)	3.4 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">8.png</a>	png	August 4, 2025, 12:40:06 (UTC+03:00)	5.5 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">9.png</a>	png	August 4, 2025, 12:40:06 (UTC+03:00)	5.1 KB	Standard-IA
<input type="checkbox"/>	 <a href="#">ICT_Systems_Interview_QA.pdf</a>	pdf	August 4, 2025, 12:13:22 (UTC+03:00)	3.1 KB	Standard