Migrating an on premises NFS share to the AWS cloud

**SPL-TF-200-ARMNFS-1 - Version 1.0.4**

© 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**

AnyCompany relies heavily on the use of Network File System (NFS) file shares to conduct their day-to-day business. The Chief Information Officer (CIO) is concerned that the on-premises NFS file server is not adequately protected from a disaster. The budget is tight. She would rather spend money to improve the business instead of expensive backup or replication solutions, which also requires many staff hours to deploy and maintain. She approaches you, as the systems engineer, to come up with a solution that meets the following criteria:

* Requires no changes to existing applications.
* Reduces physical infrastructure, cost, and complexity.
* Optimized and Secure Data Transfer.
* Low-latency access to data.

After extensive research, you have decided to build a proof of concept using AWS DataSync and an AWS Storage Gateway file gateway.

DataSync satisfies many of the requirements. The service:

* Connects to your existing storage systems using the industry-standard NFS and SMB protocols.
* Pay only for data copied by the service at a flat, per-gigabyte rate. No software licenses, contracts, maintenance fees, development cycles, or hardware are required.
* Ensures that your data arrives intact. For each transfer, the service performs integrity checks both in-transit and at-rest. These checks ensure that the data written to your destination matches the data read from your source, validating consistency.

A Storage Gateway file gateway provides the ongoing data transfer to and from Amazon S3. The service:

* Delivers end-to-end protection of customer data from the Storage Gateway in the enterprise network to the data residing in AWS.
* Maintains a cache of recently written or read data so your applications can have low-latency access to data that is stored durably in AWS.

The file gateway acts as a file system mount on an S3 bucket. The file gateway NFS file share replaces the existing on-premises NFS file server, allowing for that server to be retired. Doing this frees up local resources and reduce maintenance time.

For more information about DataSync, Amazon S3, and Storage Gateway, refer to [**Additional resources**](https://labs.skillbuilder.aws/sa/lab/arn%3Aaws%3Alearningcontent%3Aus-east-1%3A470679935125%3Ablueprintversion%2FSPL-TF-200-ARMNFS-1%3A1.0.4-85f37b78/en-US#resources) at the end of the lab.

OBJECTIVES

By the end of this lab, you should be able to do the following:

* Deploy and activate a DataSync agent on an Amazon Elastic Compute Cloud (Amazon EC2) instance.
* Create a DataSync task to copy data from a Linux-based NFS server to an S3 bucket.
* Deploy and activate a Storage Gateway file gateway appliance as an EC2 instance.
* Create an NFS file share on a file gateway.
* Configure a Linux host to connect to an NFS share on a file gateway.

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.
* **Learn more:** 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).
* **Warning:** An action that is irreversible and could potentially impact the failure of a command or process (including warnings about configurations that cannot be changed after they are made).
* **Task complete:** A conclusion or summary point in the lab.

**Start lab**

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

**Caution:** 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.

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

COMMON SIGN-IN ERRORS

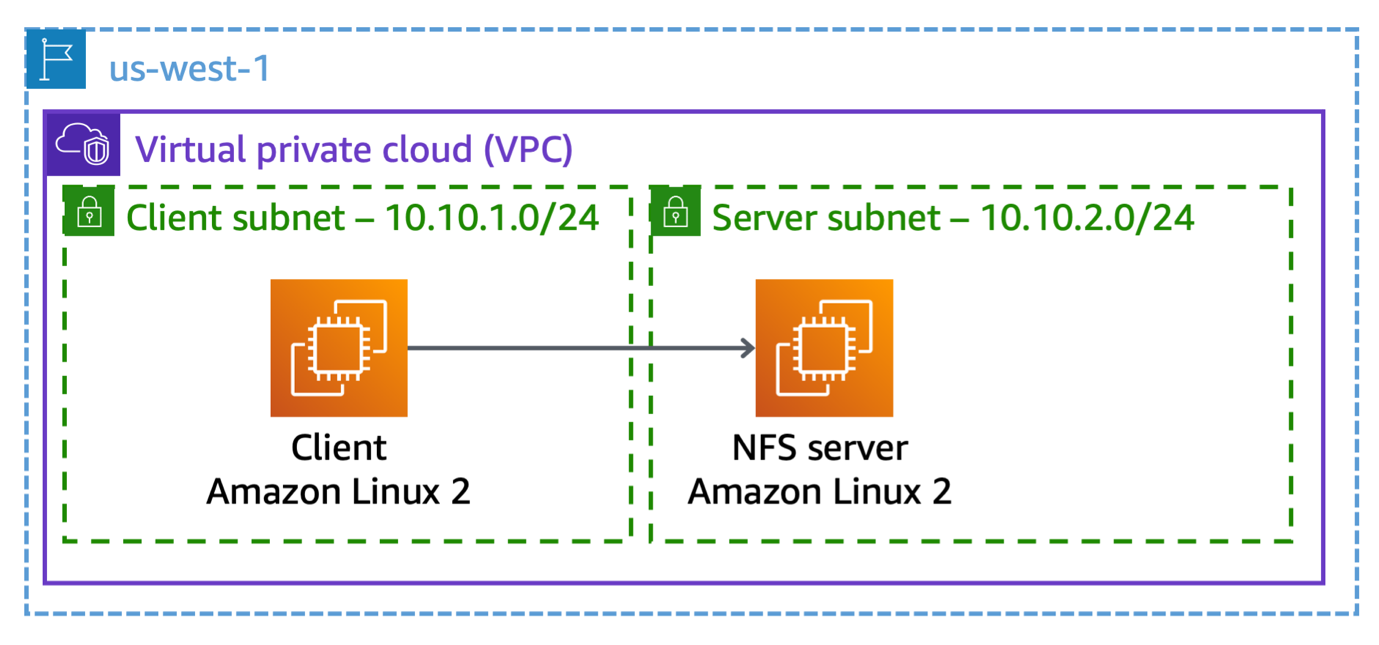
**Error: Choosing Start Lab has no effect**

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.

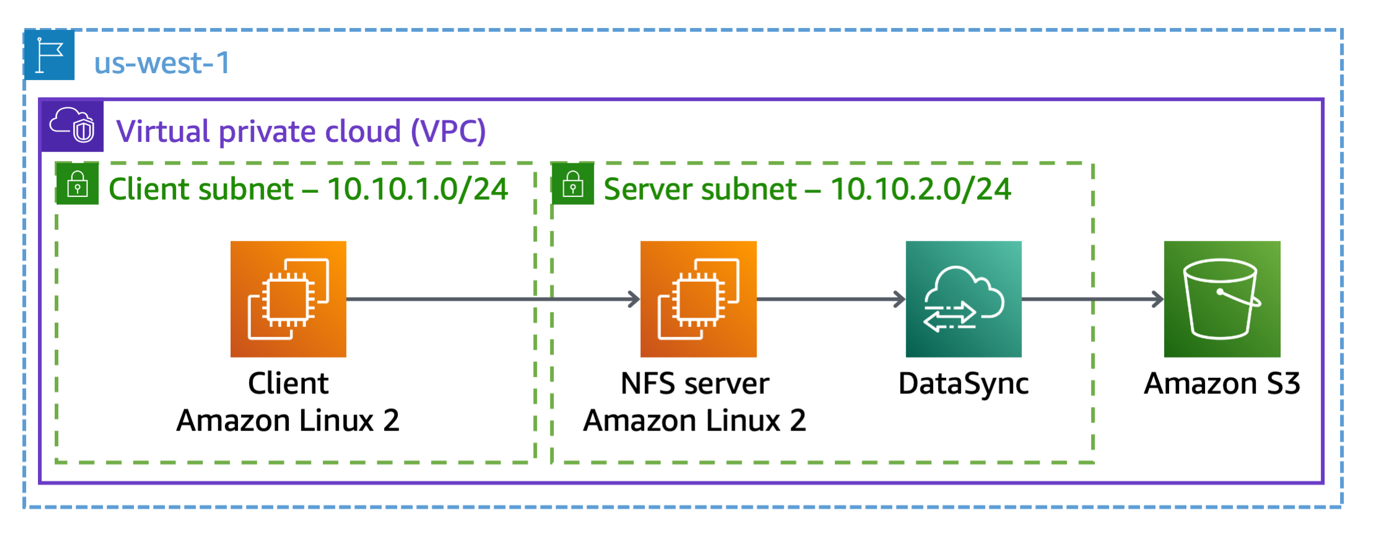
LAB ENVIRONMENT

The lab begins with two EC2 instances in separate subnets: One instance represents the on-premises client host and the other instance represents the on-premises NFS file server.



*Image description: A client EC2 instance in a client subnet is connected to a NFS server EC2 instance in a server subnet. Both subnets and instances are located in a VPC.*

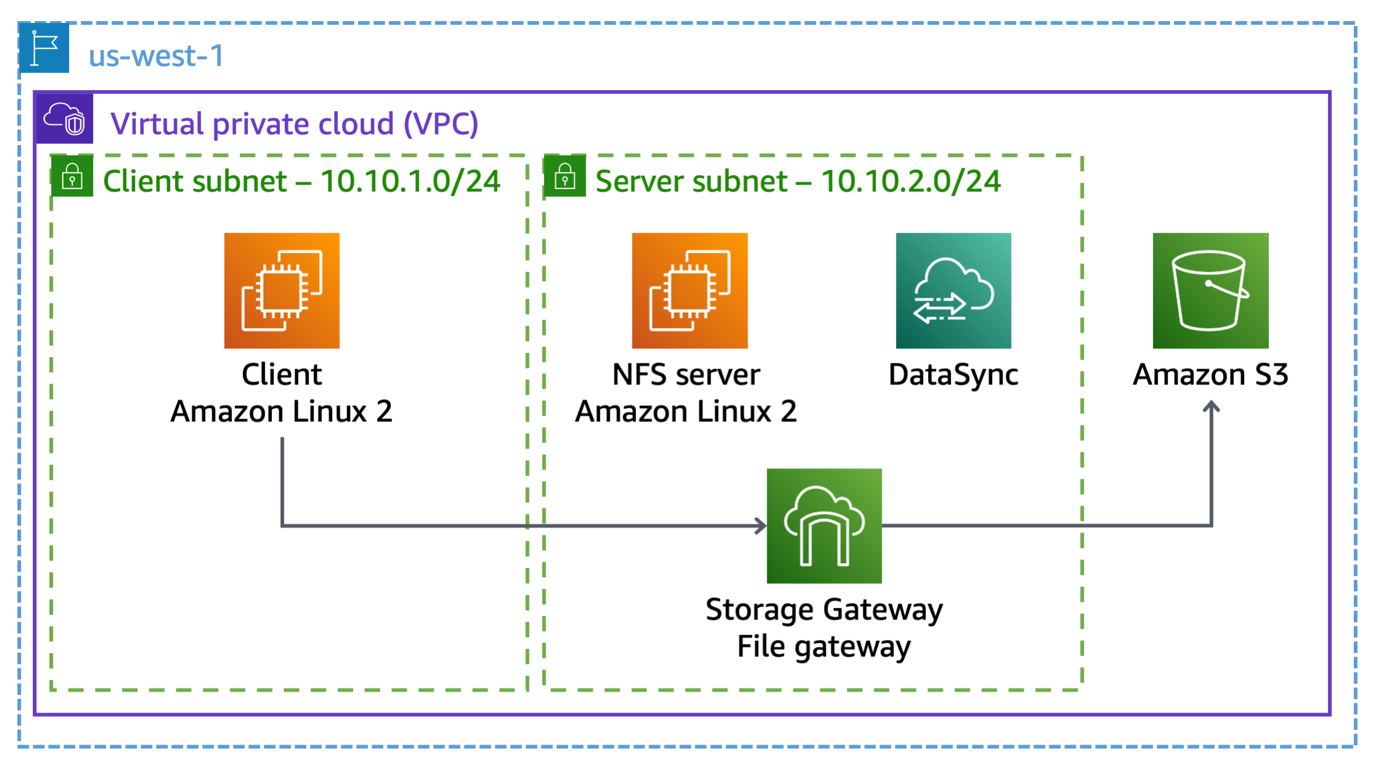
Next, you deploy a DataSync agent instance in the same subnet as the on-premises NFS file server, and configure it to copy sample data to an S3 bucket.



*Image description: A client EC2 instance in a client subnet is connected to a NFS server EC2 instance in a server subnet. Both subnets and instances are located in a VPC. The server EC2 instance uses AWS DataSync to copy sample data to Amazon S3.*

Lastly, you complete the following:

* Deploy a file gateway appliance into the same subnet as the on-premises NFS file server
* Create an NFS file share on the file gateway
* Configure the Linux client to connect to the new file share



*Image description: A client EC2 instance in a client subnet is connected to a NFS server EC2 instance in a server subnet. Both subnets and instances are located in a VPC. The server EC2 instance uses AWS DataSync to copy sample data to Amazon S3. The client EC2 instance uses AWS Storage Gateway to connect to the Amazon S3 bucket.*

AWS SERVICES NOT USED IN THIS LAB

AWS service capabilities used in this lab are limited to what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

**Task 1: Connecting to the on-premises NFS server**

Create a test environment for your Proof Of Concept (POC) build with a Linux NFS file server and a Linux client.

In this task, mount an NFS file share on a Linux client and copy the data from the client instance to the NFS file share to complete the POC build. Verify successful completion of the copy.

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

EC2

.

1. From the EC2 Management Console, choose **Instances**.
2. From the **Instances** screen, select **Client Linux instance** and choose **Connect**.
3. Ensure the **EC2 Instance Connect** tab is selected and choose **Connect**.
4. **Command:** To mount the on-premises NFS share to the client instance, enter the command below. Replace the **NFS\_SERVER\_PRIVATE\_IP** placeholder value with the **NfsServerPrivateIp** value that is listed to the left of these instructions:

sudo mount NFS\_SERVER\_PRIVATE\_IP:/var/nfs /mnt/nfs

**Expected output:**

*None, unless there is an error.*

1. **Command:** To verify that the NFS file share was mounted successfully, enter the following command:

df -h

**Expected output:**

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

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

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

Filesystem Size Used Avail Use% Mounted on

devtmpfs 465M 0 465M 0% /dev

tmpfs 473M 0 473M 0% /dev/shm

tmpfs 473M 464K 472M 1% /run

tmpfs 473M 0 473M 0% /sys/fs/cgroup

/dev/nvme0n1p1 8.0G 1.5G 6.5G 19% /

tmpfs 95M 0 95M 0% /run/user/1000

tmpfs 95M 0 95M 0% /run/user/0

10.10.2.175:/var/nfs 8.0G 1.5G 6.5G 19% /mnt/nfs

**Note:** The *df* command displays all currently mounted file systems and the disk space available on each one. The *-h* tag displays the size values in an easier to read format, such as “1K” instead of “1000”.

The client instance has two directories with sample data used during this lab: */data/DataSync* and */data/FileGateway*. Each directory contains ten .png files.

1. **Command:** To copy the sample data from the */data/DataSync* directory to the NFS file share, enter the following command:

sudo cp /data/DataSync/\*.\* /mnt/nfs

**Expected output:**

*None, unless there is an error.*

Remain connected to this EC2 Instance Connect session. You come back to it later.

1. Return to the AWS Management Console.
2. Use the steps you performed previously to open a new EC2 Instance Connect session to the NFS file server instance. This instance is named **Server Linux instance**.
3. **Command:** In the browser tab connected to the NFS server, verify the successful data transfer from the client instance by entering the following command:

ls /var/nfs

**Expected output:**

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

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

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

10.png 1.png 2.png 3.png 4.png 5.png 6.png 7.png 8.png 9.png

Remain connected to this EC2 Instance Connect session. You come back to it later.

**Task complete:** You have successfully copied the data from the client instance to the NFS file share.

**Task 2: Deploying and activating an AWS DataSync agent instance**

With the completion of the POC environment, deployment of the DataSync agent can begin.

In this task, you deploy and activate a DataSync agent as an EC2 instance.

In a physical environment, use a VMware-based virtual machine to deploy DataSync. For more information, see the *Additional resources* at the end of 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

EC2

.

1. From the EC2 Management Console, choose **Launch instance**.
2. In the **Names and tags** section, locate the **Name** text box and enter

DataSync agent

 for the value.

1. In the **Names and tags** section, choose **Add additional tags**, locate the **Resource types** drop-down menu, and select **Volumes** and **Network interfaces**. Select **Instances** if it is not already selected.
2. In the **Application and OS Images** section, locate the search bar, input

aws-datasync

 and press **Enter**.

The **Choose an Amazon Machine Image (AMI)** page displays the AMI search results.

1. Choose the **Community AMIs** tab.
2. Locate the highest version of the AWS DataSync AMI. To the right of the AMI, choose **Select**.
3. In the **Instance type** section, select the drop-down menu and choose **t3.xlarge**.

**Note:** The t3.xlarge instance type is the only one that deploys successfully in this lab. Selecting any other type results in a failure message at the end of the launch wizard.

**Learn more:** The t3.xlarge instance type selection provides an example specific to this lab environment. Refer to *Requirements for AWS DataSync* in the **Additional resources** section for more information about deploying a DataSync agent in the real world.

1. In the **Key pair (login)** section, choose **Proceed without a key pair (Not recommended)**.
2. In the **Network settings** section, choose **Edit**, locate the **VPC - required** drop-down menu, and choose the VPC named **Lab VPC**.
3. Locate the **Subnet** drop-down menu, and choose the subnet named **Server Subnet**.
4. Locate the **Auto-assign public IP** drop-down menu, and choose **Enable**.
5. Locate the **Firewall (security groups)** parameter, and choose **Select existing security group**.
6. Locate the **Common security groups** drop-down menu, and choose the security group named **DataSyncAccess**.

The DataSyncAccess security group is configured to allow traffic as follows:

* Inbound - Port 80 (HTTP) for agent activation
* Outbound - Port 443 for communication with the AWS DataSync service
* Outbound - Port 2049 for NFS v4.1 communications to the server subnet

1. Leave the remaining parameters set to their default values and choose **Launch instance**.
2. Navigate to the bottom of the page and choose **View all instances**.

The DataSync agent instance deployment takes a few minutes. Monitor the deployment by reviewing the status in the **Status check** column for the DataSync agent instance. Wait for the status to return **2/2 checks passed**. This may take approximately *5* minutes.

**Note:** You might need to choose the refresh  button at the top of the page.

1. Select **DataSync agent** instance from the list and navigate to the **Details** tab.
2. Locate the **Public IPv4 address** and **Private IPv4 addresses** values. Copy both values and paste them into a text editor for use in upcoming steps.
3. At the top of the AWS Management Console, in the search bar, search for and choose

DataSync

.

1. From the AWS DataSync console, expand the three lines menu on the left side of the screen, and choose **Agents**.
2. Choose **Create agent**.
3. On the **Create agent** page, configure the following selections:

* In the **Deploy agent** section, locate the **Hypervisor** drop-down menu and choose **Amazon EC2**.
* In the **Activation key** section, select **Automatically get the activation key from your agent**.
* In the **Agent address** text box, enter the **Public IPv4 address** of the DataSync agent instance. Use the value of **Public IPv4 address** copied previously.

1. Choose **Get key**.

**Expected output:**

**Successfully retrieved activation key from agent**

**Note:** If you receive an activation time out error, wait for few minutes and refresh the page. In this case, the DataSync agent instance needs more time to launch successfully.

The **Create agent** page returns a successful activation key message.

1. Locate the **Agent name** section, select the **Agent name** text box, and enter

NFS DataSync agent

.

1. Navigate to the bottom of the **Create agent** page, and choose **Create agent**.

**Expected service output:**

**Created agent**

**Task complete:** You have successfully deployed and activated a DataSync agent.

**Task 3: Creating and running a DataSync task**

In this task, you modify the on-premises NFS server configuration to allow connections from the DataSync agent instance. You then create a new DataSync task that you use to copy data from the on-premises NFS server to an S3 bucket.

1. Return to the EC2 Instance Connect session for **Server Linux instance** that you opened during Step 11.
2. **Command:** To modify the */etc/exports* file to allow connections from the DataSync agent instance, in the SSH session, enter the following command:

sudo vi /etc/exports

1. **Command:** To insert text, press the **o** key.
2. **Command:** On a new line at the end of the file, enter the following text:

Replace the **DATA\_SYNC\_AGENT\_IP** placeholder value with the *Private IP* of the DataSync agent instance that you copied in the previous task.

/var/nfs DATA\_SYNC\_AGENT\_IP(rw,fsid=2,sync,no\_subtree\_check)

1. **Command:** To turn off insert mode, press **Esc**.
2. **Command:** To save the changes and exit the text editor, enter

:x

, and then press **Enter**.

1. **Command:** To activate the changes you made to the */etc/exports* configuration, enter the following command:

sudo exportfs -a

**Expected output:**

*None, unless there is an error.*

1. Return to the **AWS DataSync** Console window.
2. On the **NFS DataSync agent** page, choose **Tasks** from the left menu of the DataSync console.
3. Choose **Create task**.
4. On the **Configure source location** page, make the following selections:

* In the **Source location options** section, choose **Create a new location**.
* In the **Configuration** section, select the **Location type** drop-down menu and choose **Network File System (NFS)**.

Additional fields appear upon selection of the NFS location type.

1. Continue to make the following selections:

* Locate the **Agents** drop-down menu and choose **NFS DataSync agent**.
* Locate the **NFS Server** text box and paste the value of *NfsServerPrivateIp* listed to the left of these instructions.
* Locate the **Mount path** text box and enter

/var/nfs

.

1. Navigate to the bottom of the page, choose **Next**.
2. On the **Configure destination location** page, configure the following:

* In the **Destination location options** section, choose **Create a new location**.
* In the **Configuration** section, select the **Location type** drop-down menu and choose **Amazon S3**.

Additional fields appear upon selection of the Amazon S3 location type.

1. Continue to make the following selections:

* Locate the **S3 bucket** drop-down menu and choose the bucket whose name matches the *S3BucketName* value, located to the left of these instructions.
* Locate the **IAM role** drop-down menu and choose

S3BucketAccessRole

.

1. Navigate to the bottom of the page, choose **Next**.
2. On the **Configure settings** page, navigate to the **Logging** section, locate the **Log level** drop-down menu and select **Do not send logs to CloudWatch**.

**Note:** You can ignore the warning message about **DataSync logs for this task won’t be published to CloudWatch.**.

1. Navigate to the bottom of the page, choose **Next**.
2. On the **Review** page, navigate to the bottom of the page and choose **Create task**.

**Expected service output:**

**Created task**

The DataSync task creation takes a few minutes. Monitor the status by reviewing the **Task status** field for the DataSync task. Wait for few minutes until the status changes to **Available**.

1. To run the DataSync task, select the **Start** drop-down menu and choose **Start with defaults**.

**Expected service output:**

**Started execution**

1. To the right of the **Started execution** message, choose **See execution details**.
2. In the **Overview** section, wait for **Execution status** to change from **Launching** to **Success**, which can take approximately 3–4 minutes.

Next, you review and verify the migrated data from NFS file share to Amazon S3 bucket.

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

S3

.

1. Choose the link for the bucket that has **nfsbucket** in its name.

The 10 .png files and an *aws-datasync-metadata* file copied to the NFS file share are listed here.

**Note:** When files or folders are copied to Amazon S3, there is a one-to-one relationship between a file or folder and an object. File and folder metadata timestamps and POSIX permissions, including user ID, group ID, and permissions, are stored in Amazon S3 user metadata. File metadata stored in Amazon S3 user metadata is interoperable with file gateway, providing on-premises file-based access to data stored in Amazon S3 by DataSync.

When DataSync copies from an NFS server, the POSIX permissions from the files and folders on the source are stored in the Amazon S3 user metadata. When copying from an SMB file share, default POSIX permissions are stored in the Amazon S3 user metadata.

When DataSync copies objects that contain this user metadata back to an NFS server, the file metadata is restored. When copying back to an SMB file share, ownership is set based on the user configured in DataSync to access that file share, and default permissions are assigned.

**Task complete:** You have successfully migrated data from NFS file share to Amazon S3.

**Task 4: Deploying and activating an AWS Storage Gateway file gateway**

With the completion of existing data migration from NFS file share to Amazon S3, deployment of the file gateway appliance that hosts the new NFS file share can begin.

In this task, you deploy and activate a file gateway appliance as an EC2 instance.

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

Storage Gateway

.

1. From the AWS Storage Gateway console, choose **Create gateway**.
2. On the **Set up gateway** page, make the following selections:

* In the **Gateway settings** section, for **Gateway name**, enter

File Gateway

.

* Locate the **Gateway time zone** drop-down menu and choose **GMT -8:00 Pacific Time (US & Canada)**.
* In the **Gateway options** section, locate the **Gateway type** parameter and choose **Amazon S3 File Gateway**.
* In the **Platform options** section, locate the **Host platform** parameter and choose **Amazon EC2**.
* For **Launch EC2 instance**, choose **Customize your settings**.
* On the **Set up gateway on Amazon EC2** card, choose **Launch instance**.

A new browser tab opens to the EC2 **Launch an instance** wizard. This link automatically selects the correct Amazon Machine Image (AMI) that you must use for the file gateway appliance.

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

File Gateway appliance

 for the value.

1. In the **Names and tags** section, choose **Add additional tags**, locate the **Resource types** drop-down menu, and select **Volumes** and **Network interfaces**. Select **Instances** if not already selected.
2. In the **Application and OS Images** section, keep the pre-selected AMI for file gateway.
3. In the **Instance type** section, select the drop-down menu and choose **t3.xlarge**.

**Note:** The t3.xlarge instance type is the only one that deploys successfully in this lab. Selecting any other type results in a failure message at the end of the launch wizard.

1. In the **Key pair (login)** section, choose **Proceed without a key pair (Not recommended)**.
2. In the **Network settings** section, choose **Edit**, locate the **VPC - required** drop-down menu, and choose the VPC named **Lab VPC**.
3. Locate the **Subnet** drop-down menu, and choose the subnet named **Server Subnet**.
4. Locate the **Auto-assign public IP** drop-down menu, and choose **Enable**.
5. Locate the **Firewall (security groups)** parameter, and choose **Select existing security group**.
6. Locate the **Common security groups** drop-down menu, and choose the security group with **FileGatewayAccess** in the name.

The **FileGatewayAccess** security group is configured to allow traffic as follows:

* Inbound - Port 80 (HTTP) for gateway activation
* Inbound - port 2049 for NFS v4.1 communications from the client subnet
* Outbound - Port 443 for communication with the AWS Storage Gateway service
* Outbound - Port 2049 for NFS v4.1 communications to the Client Subnet

**Learn more:** Refer to *Port Requirements* in the **Additional resources** section for more information about the ports used by Storage Gateway.

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

* Locate the **Device name** drop-down menu and choose **/dev/sdb**.
* Locate the **Size (GiB)** text box and enter

150

.

* Locate the **Volume type** drop-down menu and choose **General purpose SSD (gp2)**.
* Locate the **Delete on termination** drop-down menu and choose **Yes**.

1. Leave the remaining parameters set to their default values and choose **Launch instance**.
2. Navigate to the bottom of the page and choose **View all instances**.

The file gateway appliance instance deployment takes a few minutes. Monitor the deployment by reviewing the status in the **Status check** column for the DataSync agent instance. Wait for the status to return **2/2 checks passed**.

**Note:** You might need to choose the refresh  button at the top of the page.

1. Select **File Gateway appliance** instance from the list and navigate to the instance details tab.
2. Locate the **Public IPv4 address** value. Copy the value and paste it into a text editor for use in upcoming steps.
3. Return to the **AWS Storage Gateway** tab in your browser. It should still be at the **Platform options** section.
4. Ensure that the **Amazon EC2** is selected for the host platform parameter.
5. Navigate to the bottom of the page and confirm the gateway set up by selecting **I completed all the steps above and launched the EC2 instance.**
6. Choose **Next**.
7. On the **Connect to AWS** page, make the following selections:

* In the **Gateway connection options** section, locate the **Connection options** parameter and choose **IP address**.
* Locate the **IP address** text box and paste the **Public IPv4 address** address of the file gateway appliance instance that was copied earlier.
* In the **Endpoint options** section, locate the **Service endpoint** parameter and choose **Publicly accessible**.

1. Choose **Next**.
2. On the **Activate gateway** page, navigate to the bottom of the page and choose **Activate gateway**.

**Expected service output:**

**Successfully activated gateway File Gateway**

**Note:** If the activation page times out, the file gateway instance may still be coming online. Wait another minute or two and then refresh the page.

1. In the **Configure cache storage** section, you see the following message: **Loading**

**Note:** Wait for the above message to finish processing (approximately 1–2 minutes).

1. In the **Configure cache storage** section, locate the **Allocated to** drop-down menu and choose **Cache**.
2. In the **CloudWatch log group** section, locate the **Choose how to set up log group** parameter and choose **Deactivate logging**.
3. In the **CloudWatch alarms** section, locate the **Choose how to set up alarm** parameter and choose **No alarm**.
4. Navigate to the bottom of the page and choose **Configure**.

**Expected service output:**

**Successfully created gateway File Gateway (sgw-xxxxx). You can create file share on this gateway.**

1. Wait for the file gateway status to change to **Running** (approximately 1 minute).

**Task complete:** You have successfully deployed and activated a file gateway appliance.

**Task 5: Creating an NFS share on the file gateway and reconfiguring the Linux client**

Your POC is nearly complete! Now that you have deployed the file gateway, you can create an NFS file share to attach to the Linux client.

In this task, you do the following:

* Create an NFS file share on the file gateway
* Reconfigure the Linux client to mount the new NFS file share
* Copy a second set of sample data to the new NFS file share

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. In the left navigation pane, make sure **Gateways** is selected and choose **Create file share**.
2. On the **Create file share** page, make the following selections:

* For **Gateway**, choose **File Gateway**.
* For **File share type**, choose **NFS**.
* Locate the **S3 bucket** drop-down menu and choose the value of *S3BucketName* parameter, located to the left of these instructions.

1. Choose **Customize configuration**.
2. Choose **Next**.
3. On the **Connect S3** page, make the following selections:

* Locate the **Storage class for new objects** drop-down menu and choose **Standard**.
* Locate the **IAM role** dropdown menu and choose **S3BucketAccessRole**.
* Locate the **Guess MIME types - *optional*** parameter and make the following selections:
  + **Guess media MIME type**

1. Choose **Next**.

On the **Control access** page, configure the following:

1. For **Client access**, choose **Specific NFS clients**, and then choose **Add client**.
2. Locate the **Allowed clients** text box and enter

10.10.1.0/24

.

1. Navigate to the bottom of the page and choose **Next**.
2. On the **Review and launch** page, scroll to the bottom and choose **Create**.

**Expected service output:**

**Your file share has been created and added to the gateway.**

The file share takes a few minutes for its creation. Monitor the creation by reviewing the **Status** column and wait for it to change from *Updating* to *Available*.

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

1. Navigate to the bottom of the page and locate the **Example Commands** section.
2. Locate the **On Linux** command to mount the file share and copy it into a text editor. Replace **[MountPath]** with

/mnt/nfs

.

1. Return to the **Client Linux instance** EC2 Instance Connect session you opened previously in Task 1.

If you closed that session, use the steps you performed previously to open a new EC2 Instance Connect session to the **Client Linux instance**.

1. **Command:** In the EC2 Instance Connect session, enter the following command to unmount the exiting connection to the on-premises NFS file server:

sudo umount -f /mnt/nfs

**Expected output:**

*None, unless there is an error.*

1. Command: Paste the **On Linux** command (copied earlier) to mount the file gateway NFS file share.

**Example command:** This shows an example mount command. Do not use the following command.

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

**\*\*\*\*** This is an EXAMPLE ONLY. **\*\*\*\***

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

sudo mount -t nfs -o nolock,hard 10.10.2.33:/nfs-bucket-ql-23453634245 /mnt/nfs

1. **Command:** To verify that the NFS file share was mounted successfully, enter the following command:

df -h

**Expected output:**

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

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

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

Filesystem Size Used Avail Use% Mounted on

devtmpfs 465M 0 465M 0% /dev

tmpfs 473M 0 473M 0% /dev/shm

tmpfs 473M 408K 472M 1% /run

tmpfs 473M 0 473M 0% /sys/fs/cgroup

/dev/nvme0n1p1 8.0G 1.5G 6.5G 19% /

tmpfs 95M 0 95M 0% /run/user/1000

10.10.2.169:/labstac-12345678910-vdu8xhqg3qbaut2k76rlve-nfsbucket-g1gcwhqxr8fo 8.0E 0 8.0E 0% /mnt/nfs

1. **Command:** Enter the following command to verify that the 10 .png files you previously copied to the NFS file share are present:

ls /mnt/nfs

**Expected output:**

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

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

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

10.png 1.png 2.png 3.png 4.png 5.png 6.png 7.png 8.png 9.png

1. **Command:** To copy the second set of data to the file gateway NFS file share, enter the following command:

sudo cp /data/FileGateway/\*.\* /mnt/nfs

**Expected output:**

*None, unless there is an error.*

Next, you review and verify the second set of migrated data from NFS file share to Amazon S3 bucket.

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 bucket name that contains **nfsbucket**.

The twenty .png files and an *aws-datasync-metadata* file copied to the NFS file share are listed here.

**Task complete:** You have successfully created an NFS file share on the file gateway and migrated the data to Amazon S3 bucket.

**Conclusion**

After a successful POC, you present your findings to the CIO, along with a recommendation to move forward with AWS DataSync and AWS Storage Gateway. They are impressed and agree with your assessment. They approve the project and budget!

You have successfully done the following:

* Deployed and activated a DataSync agent on an EC2 instance.
* Created a DataSync task to copy data from a Linux-based NFS server to an S3 bucket.
* Deployed and activated a Storage Gateway file gateway appliance as an EC2 instance.
* Created an NFS file share on a file gateway.
* Configured a Linux host to connect to an NFS share on a file gateway.

**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**

* [Getting started with AWS DataSync](https://docs.aws.amazon.com/datasync/latest/userguide/requirements.html#hosts-requirements)
* [AWS DataSync FAQs](https://aws.amazon.com/datasync/faqs/)
* [AWS DataSync Pricing](https://aws.amazon.com/datasync/pricing/)
* [Storage class considerations with Amazon S3 transfers](https://docs.aws.amazon.com/datasync/latest/userguide/create-s3-location.html#using-storage-classes)
* [Amazon S3 pricing](https://aws.amazon.com/s3/pricing/)
* [AWS Storage Gateway FAQs](https://aws.amazon.com/storagegateway/faqs/?nc=sn&loc=6)
* [AWS Storage Gateway pricing](https://aws.amazon.com/storagegateway/pricing/?nc=sn&loc=3)

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).