Lab 5: Migrating an On-Premises NFS Share Using AWS DataSync and Storage Gateway v3.0.2

Thursday, March 4, 2021 10:08 AM

***If DataSync task does create correctly double check step 42

Advanced Architecting on AWS - Lab 5: Migrating an On-Premises NFS Share Using AWS DataSync and Storage Gateway

1 hour 30 minutes Free ★★★★★

Corrections, feedback, or other questions? Contact us at *AWS Training and Certification*.

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 data in the on-premises NFS file server is not adequately backed up or protected from a disaster at the primary data center. The budget is tight. She would conduct their day-to-day business. The Chief Information Officer (CIO) is concerned that the data in the on-premises NFS file server is not adequately backed up or protected from a disaster at the primary data center. The budget is tight. She would rather spend money to improve the business instead of expensive backup or replication solutions, which will also require 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:

- Protect the data in the on-premises NFS file shares against disasters at in the company data center
- Is cost-effective
- Is easy to deploy and maintain
- Can quickly migrate the existing data
- Can replicate future data off-site with minimal interaction from support teams

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:

- Copies existing data from an on-premises NFS file server to Amazon Simple Storage Service (Amazon S3) for secure, redundant storage
- Comes with a built-in scheduling mechanism enabling you to periodically execute a data transfer task to detect and copy changes from your source storage system to the destination.
- 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.
- Is priced per gigabyte of data moved, making it cost-effective and predictable
- Can be deployed in minutes

A Storage Gateway file gateway provides the ongoing data transfer to and from Amazon S3. The file gateway acts as a file system mount on an S3 bucket. The file gateway NFS file share will replace the existing on-premises NFS file server, allowing for that server to be retired. Doing this will free up local resources and reduce maintenance time.

For more information about DataSync, Amazon S3, and Storage Gateway, refer to **Additional Resources** at the end of the lab.

Objectives

After completing this lab, you will be able to:

After completing this lab, you will be able to:

- Deploy and activate a DataSync agent as 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

Prerequisites

This lab requires:

- Access to a notebook computer with Wi-Fi and Microsoft Windows, macOS, or Linux (Ubuntu, SuSE, or Red Hat)
- An internet browser such as Chrome, Firefox, or Microsoft Edge
- A plaintext editor

Duration

This lab requires approximately **60** minutes to complete.

AWS Services Not Used in This Lab

AWS services not used in this lab are disabled in the lab environment. In addition, the capabilities of the services 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.

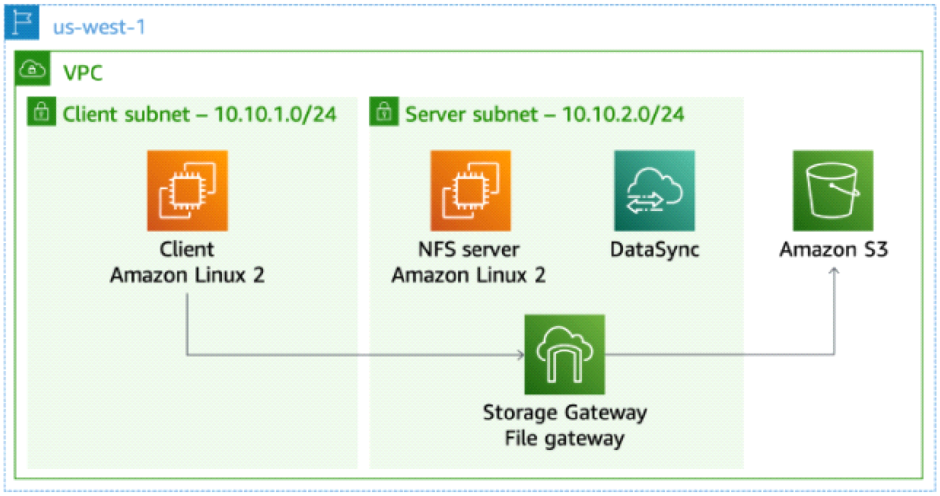
Lab Environment

The lab begins with two Linux instances in separate subnets: one instance acting as the on-premises client host and one instance acting as the on-premises Linux NFS file server. You deploy a DataSync agent instance into the same subnet as the on-premises NFS file server. Then, you configure that instance to copy sample data to an S3 bucket. Lastly, you do 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 appliance
- Reconfigure the Linux client host to connect to the new share

- Create an NFS file share on the file gateway appliance
- Reconfigure the Linux client host to connect to the new share

The following diagram shows the resources provisioned for this lab and how they are connected at the end of the lab:



Start Lab

1. At the top of your screen, launch your lab by choosing Start Lab

   This starts the process of provisioning your lab resources. An estimated amount of time to provision your lab resources is displayed. You must wait for your resources to be provisioned before continuing.

   ℹ If you are prompted for a token, use the one distributed to you (or credits you have purchased).

2. Open your lab by choosing Open Console

   This opens an AWS Management Console sign-in page.

3. On the sign-in page, configure:

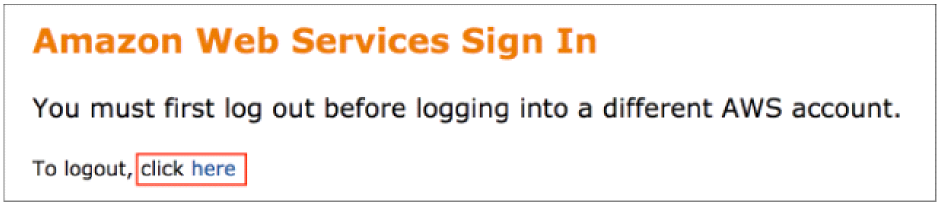
   - **IAM user name:** `awsstudent`
   - **Password:** Paste the value of **Password** from the left side of the lab page
   - Choose Sign In

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

Common Login Errors

Common Login Errors

Error: You must first log out



Amazon Web Services Sign In

You must first log out before logging into a different AWS account.

To logout, click here

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

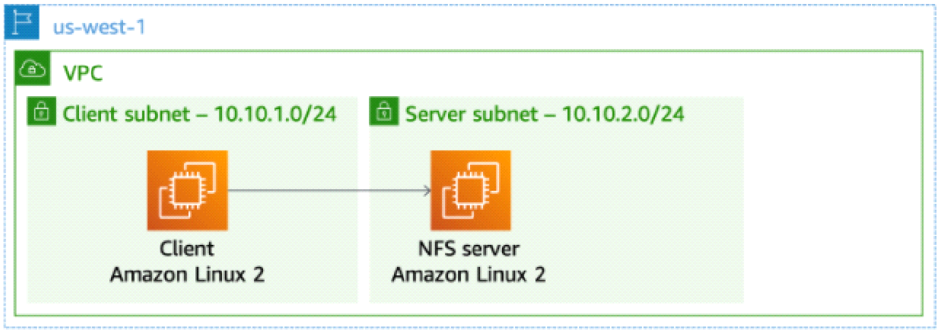
- Choose **click here**
- Close your browser tab to return to your initial lab window
- Choose Open Console again

Task 1: Connect to the On-Premises NFS Server

You want to create a test environment in which to perform the proof of concept, so you have deployed a Linux NFS file server and a Linux client host.

In this task, you use the Linux client to mount an NFS file share which is hosted from the Linux NFS server instance to finish configuring the environment. You then copy data from the client instance to the NFS file share and verify that it copied successfully.

The following diagram shows the architecture for this task:



Mount the On-Premises NFS Share

Mount the On-Premises NFS Share

4. Copy the **NfsClientInstanceSessionManagementUrl** value from the left side of the lab instructions, paste it in a new browser tab, and press ENTER.

   The NFS Client Instance terminal is displayed.

5. To mount the on-premises NFS share to the client instance, run the following command. Replace *<NfsServerPrivateIp>* with the **NfsServerPrivateIp** value from the left side of the lab instructions:

   ```
   sudo mount <NfsServerPrivateIp>:/var/nfs /mnt/nfs
   ```

6. To verify that the NFS file share was mounted successfully, run the following command:

   ```
   df -h
   ```

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

   The output should be similar to the following:

   ```
   Filesystem            Size  Used Avail Use% Mounted on
   devtmpfs              475M     0  475M   0% /dev
   tmpfs                 492M     0  492M   0% /dev/shm
   tmpfs                 492M  392K  492M   1% /run
   tmpfs                 492M     0  492M   0% /sys/fs/cgroup
   /dev/xvda1            8.0G  1.1G  7.0G  14% /
   tmpfs                  99M     0   99M   0% /run/user/1000
   10.10.2.154:/var/nfs  8.0G  1.1G  7.0G  14% /mnt/nfs
   ```

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

7. To copy the sample data from the **/data/DataSync** directory to the NFS file share, run the following command:

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

   Remain connected to this session. You need it for tasks later.

8. Copy the **NfsServerInstanceSessionManagementUrl** value from the left side of the lab page, paste it in a new browser tab, and press ENTER.

   The NFS Server Instance terminal is displayed.

9. In the terminal, verify that the data from the client instance was copied successfully

The NFS Server Instance terminal is displayed.

9. In the terminal, verify that the data from the client instance was copied successfully by running the following command:

```
ls /var/nfs
```

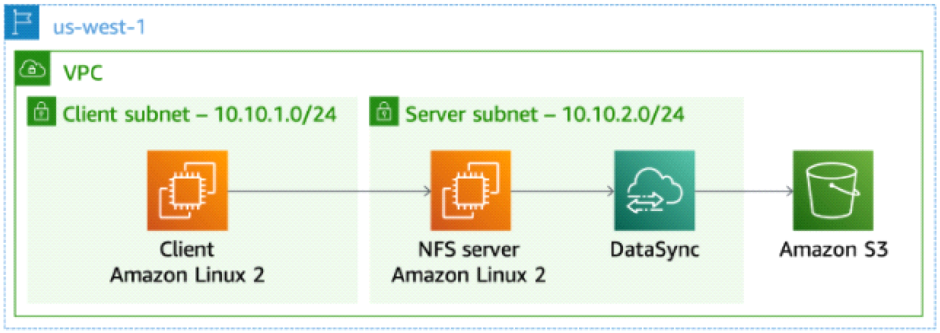
The output should return the 10 .png files that you copied from the client instance.

Remain connected to this session. You need it for tasks later.

Task 2: Deploy and Activate a DataSync Agent Instance

Now that the foundation of your proof of concept environment is complete, you are ready to deploy the DataSync agent.

In this task, you deploy a DataSync agent as an EC2 instance and then activate it, as shown in the following diagram:



In a physical environment, DataSync can also be deployed as a VMware-based virtual machine. For more information, refer to Additional Resources at the end of this lab.

10. If you have not already opened the AWS Management Console, follow the instructions in the **Start Lab** section to log in to the console.

11. On the **Services ⌄** menu, choose **EC2**.

You can also search for `EC2` in the search bar at the top of the console.

12. On the EC2 dashboard, in the **Resources** section, choose **Instances**.

13. Choose **Launch instances**.

13. Choose Launch instances.

14. In the navigation pane, choose **Community AMIs**.

15. To search for the latest DataSync agent AMI, enter `aws-datasync` in the search bar and press ENTER.

16. To the right of the line with the highest version number, choose Select.

17. On the **Choose an Instance Type** page, select **t2.xlarge**.

    📝 The t2.xlarge instance type is the only one that can deploy successfully in this lab. Selecting any other type will result in a failure message at the end of the wizard.

    ℹ The t2.xlarge instance type is used only as an example in this lab. When deploying a DataSync agent, refer to the documentation for correct host sizing.

18. Choose Next: Configure Instance Details.

19. On the **Configure Instance Details** page, configure:

    - For **Network**, choose **Lab VPC**
    - For **Subnet**, choose **Server Subnet**
    - For **Auto-assign Public IP**, choose **Use subnet setting (Enable)**
    - Accept the default values for the remaining options

20. Choose Next: Add Storage.

    ℹ The DataSync agent instance does not require additional storage beyond the 80-GiB root volume.

21. Choose Next: Add Tags.

22. On the **Add Tags** page, choose Add Tag and configure:

    - For **Key**, enter `Name`
    - For **Value**, enter `DataSync agent`
    - Select **Instances**
    - Select **Volumes**

    📝 Tags are case-sensitive.

23. Choose Next: Configure Security Group.

24. On the **Configure Security Group** page, select ◉ **Select an existing security group**.

25. Select the security group with **DataSyncAccess** in the name. The **Description** field is *Network traffic rules for the DataSync instance.*

    The DataSyncAccess security group is configured to allow the following traffic:

The DataSyncAccess security group is configured to allow the following traffic:

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

26. Choose **Review and Launch**

    ℹ A warning message displays, stating that port 22 is not open, so you will not be able to connect to the instance. You can safely ignore this warning, because you do not connect to this instance over SSH in this lab.

27. Choose **Continue**.

28. Choose **Launch**.

29. In the **Select an existing key pair or create a new key pair** dialog box, configure the following options:

    - Select **Choose an existing key pair**
    - For **Select a key pair**, choose **qwikLABS-xxxx-xxxx**
    - Select **I acknowledge that I have access to the selected private key file**

    This is the key pair that is provided on the left side of the lab page.

30. Choose **Launch Instances**.

31. On the **Launch Status** page, choose **View Instances**.

    The DataSync agent instance takes a few minutes to deploy. Monitor the status of the deployment and wait for the **Status check** column to display *2/2 checks passed*.

    ℹ You might need to choose the refresh ⟳ icon at the top of the page.

32. Select the **DataSync agent** instance from the list. On the **Details** tab in the lower pane, locate the **Public IPv4 address** and **Private IPv4 address** values. Copy both to a text editor to use in upcoming steps.

33. On the **Services ⌄** menu, choose **DataSync**.

34. Choose **Get started**.

    The '*Create agent*' page is displayed.

35. If the **Deploy agent** section is available, choose **Amazon EC2** from the drop-down menu.

36. In the **Service endpoint** section, keep the default **Public service endpoints** option.

37. In the **Activation key** section, for **Agent address**, enter the **Public IPv4 address** value

36. In the **Service endpoint** section, keep the default **Public service endpoints** option.

37. In the **Activation key** section, for **Agent address**, enter the **Public IPv4 address** value that you copied previously for the DataSync agent instance.

38. Choose **Get key**.

    ℹ If the activation page times out, the DataSync agent instance might still be coming online. Wait another minute or two, refresh the page, and try again.

    On the next page, there is a green check mark ✓ with the activation key listed.

39. For **Agent name**, enter `NFS DataSync agent`.

40. Scroll down to the bottom of the page and choose **Create agent**.

    The DataSync agent page displays, with a ✓ **Created agent** message at the top of the page.

Task 3: Create and Run a DataSync Task

Now it's time to use DataSync to copy the data that currently exists on the NFS file share to the S3 bucket.

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, which you use to copy data from the on-premises NFS server to an S3 bucket.

41. Return to the **NFS file server** session that you opened in Task 1.

    If you closed that session, Copy the **NfsServerInstanceSessionManagementUrl** value from the left side of the lab page, paste it in a new browser tab, and press the ENTER key.

42. Modify the **/etc/exports** file to allow connections from the DataSync agent instance, run the following command:

    Replace *<DataSyncAgentPrivateIp>* with the **Private IPv4 address** of the DataSync agent instance that you copied in the previous task.

```
sudo sh -c 'echo "/var/nfs <DataSyncAgentPrivateIp>
(rw,fsid=2,sync,no_subtree_check)" >> /etc/exports'
```

43. Activate the changes you made to the **/etc/exports** configuration, run the following command:

43. Activate the changes you made to the **/etc/exports** configuration, run the following command:

    ```
    sudo exportfs -a
    ```

44. Return to the DataSync agent page in the console.

45. In the **Tasks** section, choose **Create task**.

    ℹ You can also create tasks from the **Tasks** page, which is accessible from the left navigation pane.

    The '*Configure source location*' page is displayed.

46. Select **Create a new location** from the **Source location options** section.

47. Select **Network File System (NFS)** from the **Location type** drop-down menu, located in the **Configuration** section.

    Additional fields display.

48. Configure the following:

    - For **Agents**, select **NFS DataSync agent**
    - For **NFS Server**, paste the **NfsServerPrivateIp** value from the left side of the lab page
    - For **Mount path**, enter `/var/nfs`

49. At the bottom of the page, choose **Next**.

    The '*Configure destination location*' page is displayed.

50. Select **Create a new location** from the **Destination location options** section.

51. Choose **Amazon S3** from the **Location type** drop-down menu, located in the **Configuration** section.

    Additional fields display.

52. Configure the following:

    - For **S3 bucket**, select the bucket name that starts with **nfs-bucket**
    - For **IAM role**, select the role with **NfsS3BucketAccessRole** in the name. You can type in this field to assist in searching.

53. Choose **Next**.

    The '*Configure settings*' page is displayed.

54. Locate the **Task logging** section.

The '*Configure settings*' page is displayed.

54. Locate the **Task logging** section.

55. Choose **Do not send logs to CloudWatch** from **Log level** drop-down menu.

56. Keep the default options for all other fields, and then choose **Next**.

    The '*Review*' page is displayed.

57. Review your selected settings and then choose **Create task**.

    A new page loads with the task ID and a ✓ **Created task** banner is displayed at the top of the page.

58. Wait for the **Task status** to change to ✓ **Available**, which takes approximately 1–2 minutes.

59. At the top right of the page, choose **Start**, **Start with defaults**. This runs the DataSync task.

    ⚠ **Note** choose **Start** if **Start with defaults** is not an available choice.

    A ✓ **Started execution** banner is displayed at the top of the page.

60. On the right side of the ✓ **Started execution** banner, choose **See execution details**.

61. On the **Execution details** page, wait for **Execution status** to change to ✓ **Success**, which takes approximately 3–4 minutes.

62. On the **Services ⌄** menu, choose **S3**.

63. Choose the bucket name that starts with **nfs-bucket** to review its contents.

    The 10 .png files that you copied to the NFS file share in Task 1, in addition to an **aws-datasync-metadata** file are listed.

    ℹ 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 a file gateway, providing on-premises file-based access to data that DataSync stores in Amazon S3.

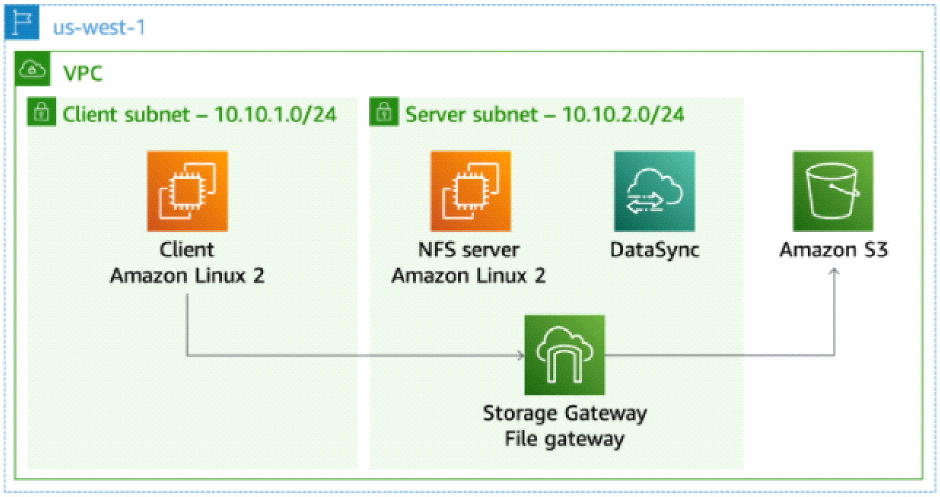
    When DataSync copies from an NFS server, the POSIX permissions from the files and folders on the source are stored in the Amazon S3 user metadata. When copying from an SMB file share, default POSIX permissions are stored in the Amazon S3 user metadata.

    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, 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 4: Deploy and Activate a Storage Gateway File Gateway

Now that you have migrated the existing data from the NFS file share to Amazon S3, you can deploy the file gateway that will host the new NFS file share.

In this task, you deploy a file gateway appliance as an EC2 instance and then activate it, as shown in the following image:



64. On the **Services ⌄** menu, choose **Storage Gateway**.

    You are prompted with a getting started page. This page is displayed because the Storage Gateway service has not yet been configured in this Region.

65. Choose **Get started**.

66. At the top-right corner of the page, verify that the AWS Region matches the **Region** value from the left side of the lab page.

    The '*Select gateway type*' page is displayed.

67. Select **File gateway**, and then choose **Next**.

    The '*Select host platform*' page is displayed.

The '*Select host platform*' page is displayed.

68. Select **Amazon EC2**, and then choose Launch instance.

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

69. On the **Choose an Instance Type** page, select **t2.xlarge**.

    🗒 The t2.xlarge instance type is the only one that will deploy successfully in this lab. Selecting any other type will result in a failure message at the end of the wizard.

    ℹ 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 for correct appliance sizing.

70. Choose Next: Configure Instance Details.

71. On the **Configure instance details** page, configure:

    - For **Network**, choose **Lab VPC**
    - For **Subnet**, choose **Server Subnet**
    - For **Auto-assign Public IP**, choose **Use subnet setting (Enable)**
    - Accept the default values for the remaining options

72. Choose Next: Add Storage.

73. Choose Add New Volume and configure:

    - For **Volume Type**, choose **EBS**
    - For **Device**, choose **/dev/sdb**
    - For **Size (GiB)**, enter `150`
    - For **Volume Type**, choose **General Purpose SSD (gp2)**
    - Select **Delete on Termination**

74. Choose Next: Add Tags.

75. On the **Add Tags** page, choose Add Tag and configure:

    - For **Key**, enter `Name`
    - For **Value**, enter `File Gateway appliance`
    - Select **Instances**
    - Select **Volumes**

    🗒 Tags are case-sensitive.

76. Choose Next: Configure Security Group.

77. On the **Configure Security Group** page, choose the option ◉ **Select an existing**

76. Choose Next: Configure Security Group.

77. On the **Configure Security Group** page, choose the option ● **Select an existing security group**.

78. Select the security group with **FileGatewayAccess** in the name. The Description field is *Network traffic rules for the file gateway instance*.

    The FileGatewayAccess security group is configured to allow the following traffic:

    - Inbound: Port 80 (HTTP) for gateway activation
    - Inbound: Port 2049 for NFS v4.1 communication from the client subnet
    - Outbound: Port 443 for communication with Storage Gateway
    - Outbound: Port 2049 for NFS v4.1 communication to the client subnet

    For more information about the ports that Storage Gateway uses, refer to Network and Firewall Requirements.

79. Choose **Review and Launch**.

    ℹ A warning message states that port 22 is not open, so you will not be able to connect to the instance. You can safely ignore this warning, because you do not connect to this instance over SSH in this lab.

80. Choose **Continue**.

81. Choose **Launch**.

82. On the **Select an existing key pair or create a new key pair** page, configure:

    - Select the option **Choose an existing key pair**
    - For **Select a key pair**, choose **qwikLABS-xxxx-xxxx**
    - Select **I acknowledge that I have access to the selected private key file**

    📝 This is the key pair that is provided on the left side of the lab page.

83. Choose **Launch Instances**.

84. On the **Launch Status** page, choose **View Instances**.

    The file gateway appliance instance takes a few minutes to deploy. Monitor the status of the deployment and wait for the **Status check** column to display *2/2 checks passed*.

    ℹ You might need to choose the refresh ⟳ icon at the top of the page.

85. Select your file gateway instance from the list. On the **Details** tab in the lower pane, locate the **Public IPv4 address**. Copy the IP address listed. You will use this value when completing the file gateway deployment.

86. Return to the **AWS Storage Gateway** tab in your browser. It should still be at the **Select host platform** page.

86. Return to the **AWS Storage Gateway** tab in your browser. It should still be at the **Select host platform** page.

87. Verify that **Amazon EC2** is selected, and then choose **Next**.

    The '*Service endpoint*' page is displayed.

88. For **Endpoint type**, select **Public**, and then choose **Next**.

    The '*Connect to gateway*' page is displayed.

89. For **IP address**, paste the **Public IPv4 address** that you previously copied for the file gateway appliance instance, and then choose **Connect to gateway**.

    ℹ If the activation page times out, the file gateway instance may still be coming online. Wait another minute or two, refresh the page, and try again.

    The '*Activate gateway*' page is displayed.

90. On the **Activate gateway** page, configure the following:

    - For **Gateway name**, enter `File Gateway`

91. Choose **Activate gateway**.

    The '*Configure local disks*' page is displayed.

92. On the **Configure local disks** screen, wait for *Preparing local disks* to finish processing (approximately 1–2 minutes).

93. Choose **Cache** from the **Allocated to** drop-down menu.

94. Choose **Configure logging**.

    The '*Gateway health log group*' page is displayed.

95. Choose **Disable logging** and then choose **Save and continue**.

    Wait for the file gateway status to change to *Running* (approximately 1 minute). Remain on this screen for the next task.

Task 5: Create an NFS Share on the File Gateway and Reconfigure the Linux Client

Gateway and Reconfigure the Linux Client

Your proof of concept 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 will 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

96. If you are not already in the **Gateways** section of the Storage Gateway console from the previous task, on the **Services ⌄** menu, choose **Storage Gateway**.

97. In the navigation pane, make sure that **Gateways** is selected. Choose **Create file share**.

    ℹ You can also create a new file share from the **File shares** section of the Storage Gateway console.

    The '*Configure file share settings*' page is displayed.

98. On the **Configure file share settings** page, configure the following:

    - For **Amazon S3 bucket name**, paste the **S3BucketName** value from the left side of the lab page
    - For **Access objects using**, choose **Network File System (NFS)**
    - For **Gateway**, choose **File Gateway (sgw-xxxx)**

99. Choose **Next**.

    The '*Configure how files are stored in Amazon S3*' page is displayed.

100. Configure the following:

    - For **Storage class for new objects**, choose **S3 Standard**
    - For **Object metadata**, select:

        - ☑ **Guess MIME type**
        - ☑ **Give bucket owner full control**

    - For **Access to your S3 bucket**, select **Use an existing IAM role**

    - For **IAM role**, paste the **NfsS3AccessPolicyARN** value from the left side of the lab page

101. Choose **Next**.

    The '*Review*' page is displayed.

    🟨 There is a warning message about the file share being accessible from anywhere

The '*Review*' page is displayed.

There is a warning message about the file share being accessible from anywhere. AWS recommends that you always limit access to only the required clients in your environment.

102. To the right of **Allowed clients**, choose **Edit**.

103. To grant access to the share from the hosts in the client subnet, change the 0.0.0.0/0 entry to `10.10.1.0/24`

104. To the right of **Allowed clients**, choose **Close** and then verify that the **Allowed clients** list was updated with the value you added.

105. Choose **Create file share**.

     The AWS Storage Gateway console is displayed.

106. Wait for the **Status** column to display *Available*, which should take less than a minute.

     ℹ You might need to periodically choose the refresh 🔄 icon at the top of the page.

107. Select the newly created file share.

108. In the lower pane, find and copy the command to mount the file share on Linux into a text editor.

109. In your text editor, replace **[MountPath]** in the command with `/mnt/nfs`

110. Return to the NFS Client Instance session that you opened in Task 1.

     If you closed that session or the session timed out, then Copy the **NfsClientInstanceSessionManagementUrl** value from the left side of the lab page, paste it in a new browser tab, and press ENTER.

111. In the terminal, to unmount the existing connection to the on-premises NFS file server, run the following command:

```
sudo umount -f /mnt/nfs
```

112. Enter `sudo` and then paste the command from your text editor to mount the file gateway NFS file share. The command should be similar to the following:

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

113. Run the command.

114. To verify that the NFS file share was mounted successfully, run the following

113. Run the command.

114. To verify that the NFS file share was mounted successfully, run the following command:

```
df -h
```

The output should be similar to the following:

```
Filesystem                                           Size  Used Avail
Use% Mounted on
devtmpfs                                             475M     0  475M
0% /dev
tmpfs                                                492M     0  492M
0% /dev/shm
tmpfs                                                492M  448K  492M
1% /run
tmpfs                                                492M     0  492M
0% /sys/fs/cgroup
/dev/xvda1                                           8.0G  1.1G  7.0G
14% /
tmpfs                                                 99M     0   99M
0% /run/user/0
tmpfs                                                 99M     0   99M
0% /run/user/1000
10.10.2.227:/nfs-bucket-qls-145848-11ff4e94b8d86cd6  8.0E     0  8.0E
0% /mnt/nfs
```

115. To verify that the 10 .png files you previously copied to the NFS file share are present, run the following command:

```
ls /mnt/nfs
```

The output lists the 10 .png files.

116. To copy the second set of data to the file gateway NFS file share, run the following command:

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

117. Return to the AWS Management Console. On the **Services ⌄** menu, choose **S3**.

118. Choose the bucket name that starts with **nfs-bucket** and review its contents.

There is a returned list of a total of 20 .png files: the 10 files that you copied to the NFS file share in Task 1 (1-10) and the 10 files that you just copied (11-20).

Conclusion

👍 Congratulations! You now have successfully:

- Deployed and activated a DataSync agent as 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, end your lab, and evaluate the experience.

119. Return to the AWS Management Console.

120. On the navigation bar, choose **awsstudent@<AccountNumber>**, and then choose **Sign Out**.

121. Choose **End Lab**

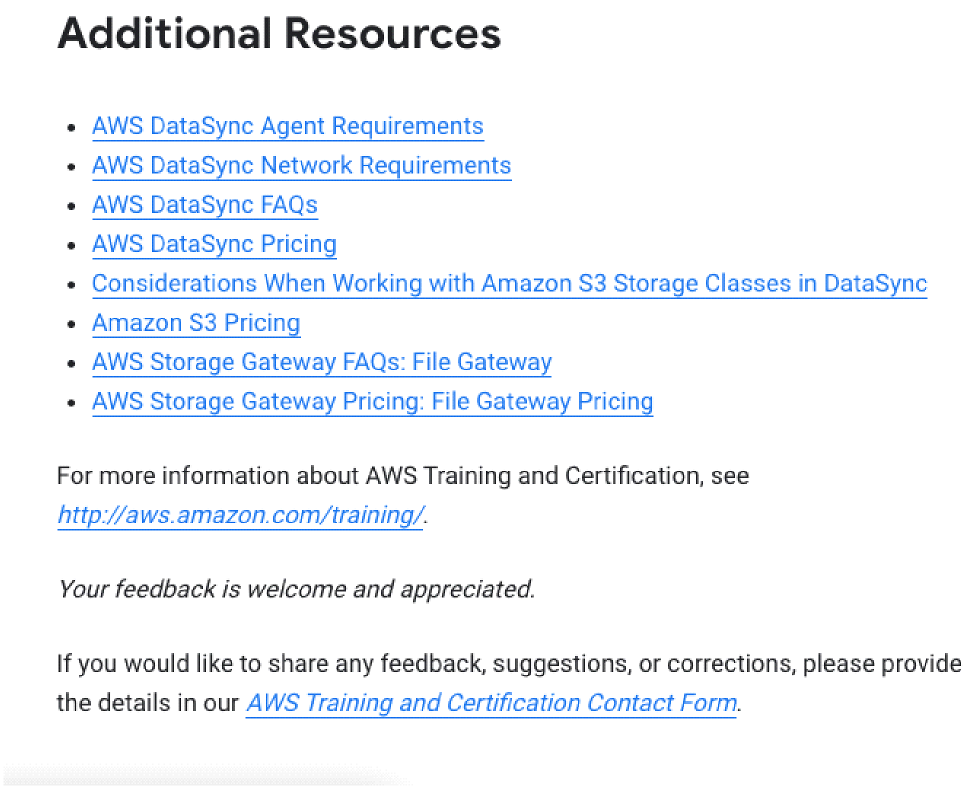
122. Choose **OK**

123. (Optional):

    - Select the applicable number of stars ☆
    - Type a comment
    - Choose **Submit**

        - 1 star = Very dissatisfied
        - 2 stars = Dissatisfied
        - 3 stars = Neutral
        - 4 stars = Satisfied
        - 5 stars = Very satisfied

You may close the window if you don't want to provide feedback.



Additional Resources

- AWS DataSync Agent Requirements
- AWS DataSync Network Requirements
- AWS DataSync FAQs
- AWS DataSync Pricing
- Considerations When Working with Amazon S3 Storage Classes in DataSync
- Amazon S3 Pricing
- AWS Storage Gateway FAQs: File Gateway
- AWS Storage Gateway Pricing: File Gateway Pricing

For more information about AWS Training and Certification, see *http://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*.