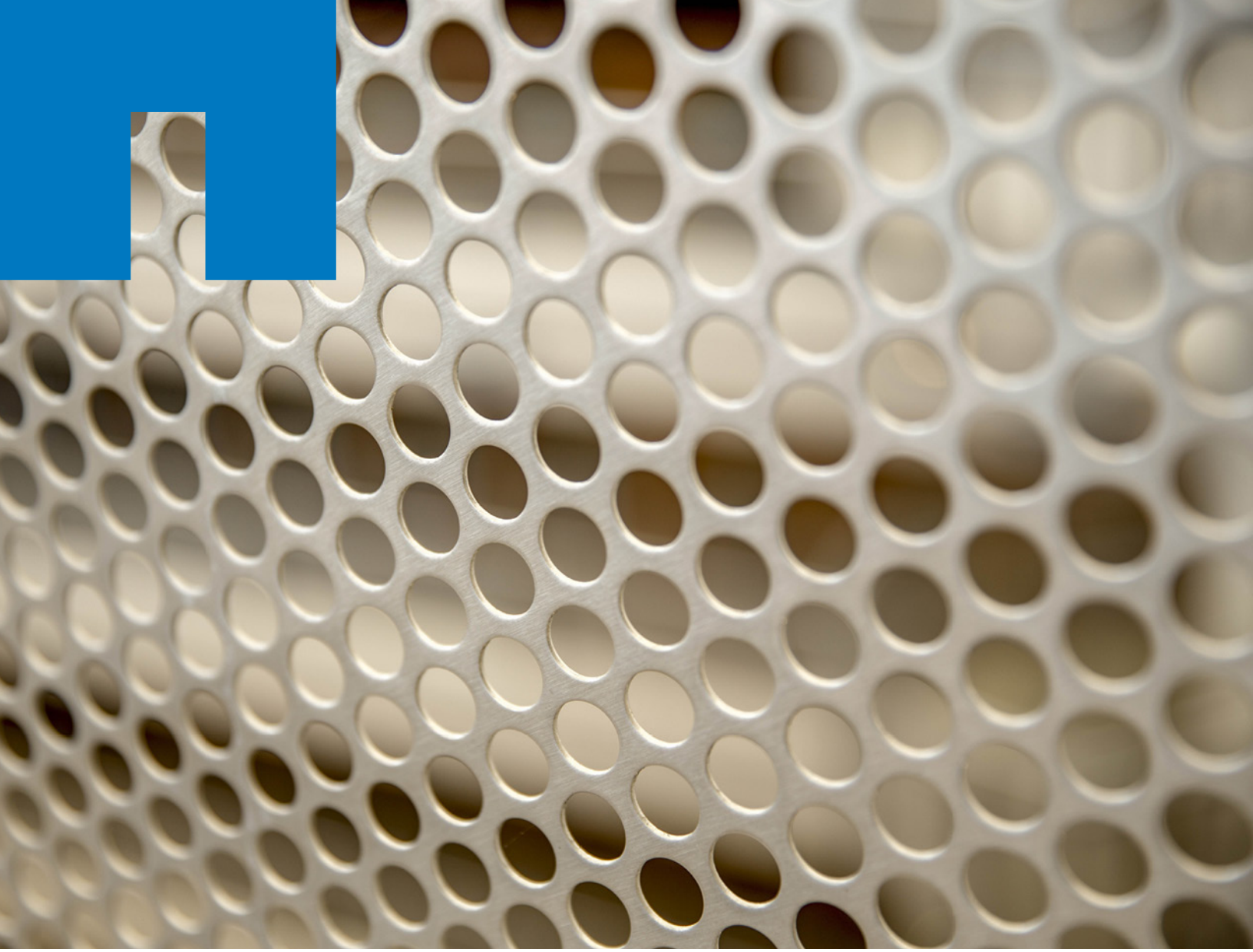


NETAPP UNIVERSITY

Integrating Hybrid Clouds with NetApp Data Fabric

Exercise Guide
Content Version 3

NetApp®

NETAPP UNIVERSITY

Integrating Hybrid Clouds with NetApp Data Fabric

Exercise Guide

Course ID: STRSW-ILT-INTHCDF
Catalog Number: STRSW-ILT-INTHCDF-EG

ATTENTION

The information contained in this course is intended only for training. This course contains information and activities that, while beneficial for the purposes of training in a closed, non-production environment, can result in downtime or other severe consequences in a production environment. This course material is not a technical reference and should not, under any circumstances, be used in production environments. To obtain reference materials, refer to the NetApp product documentation that is located at http://mysupport.netapp.com/.

COPYRIGHT

U.S. GOVERNMENT RIGHTS

Commercial Computer Software. Government users are subject to the NetApp, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

TRADEMARK INFORMATION

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TABLE OF CONTENTS

Getting Started

Study Aid Icons

In your exercises, you might see one or more of the following icons.

Warning

If you misconfigure a step marked with this icon, later steps might not work properly. Check the step carefully before you move forward.

Attention

Review this step or comment carefully to save time, learn a best practice, or avoid errors.

Information

A comment labeled with this icon provides information about the topic or procedure.

References

A comment labeled with this icon identifies reference material that provides additional information.

Exercise 0: Checking the Lab Equipment

In this exercise, you familiarize yourself with your equipment and ensure that licenses are installed. You also access your Amazon Web Services (AWS) and Azure accounts.

Objectives

This exercise focuses on enabling you to do the following:

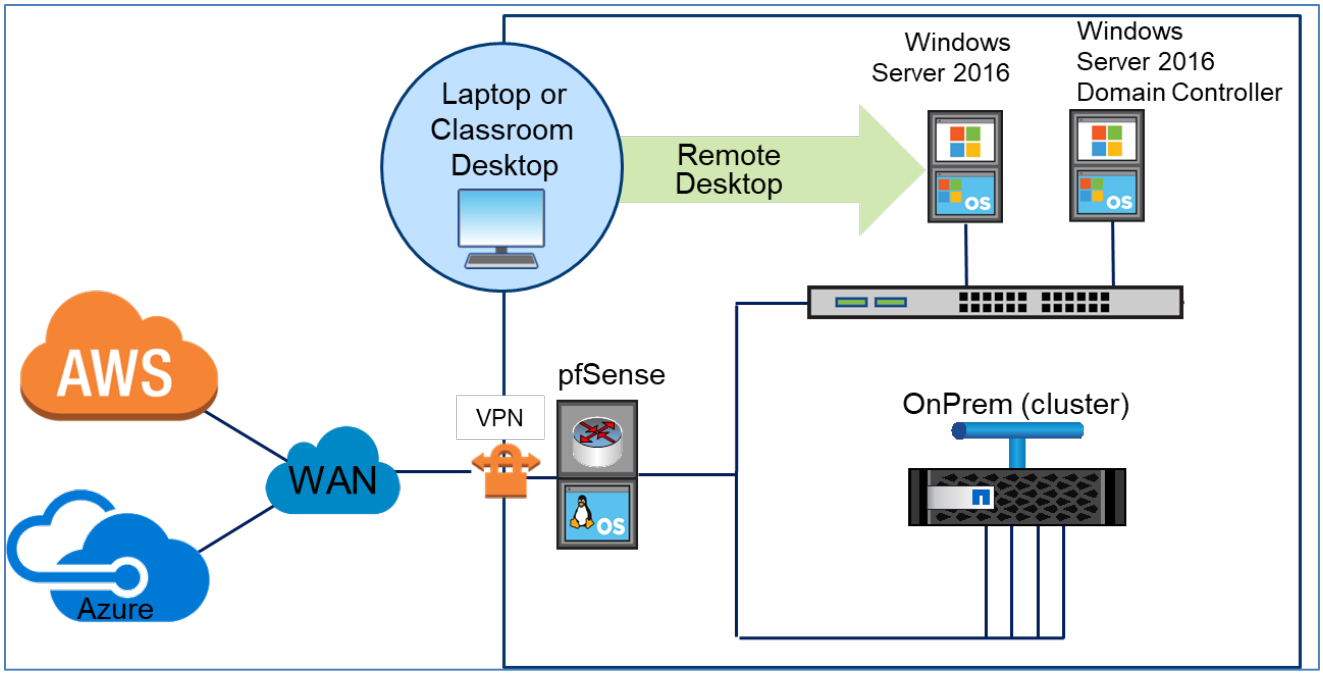
- Ensure connectivity to an ONTAP cluster
- Ensure that required licenses are installed on the ONTAP clusters
- Verify that you can log in to your assigned AWS and Azure accounts

Exercise Equipment Diagram

Your lab contains the following virtual machines:

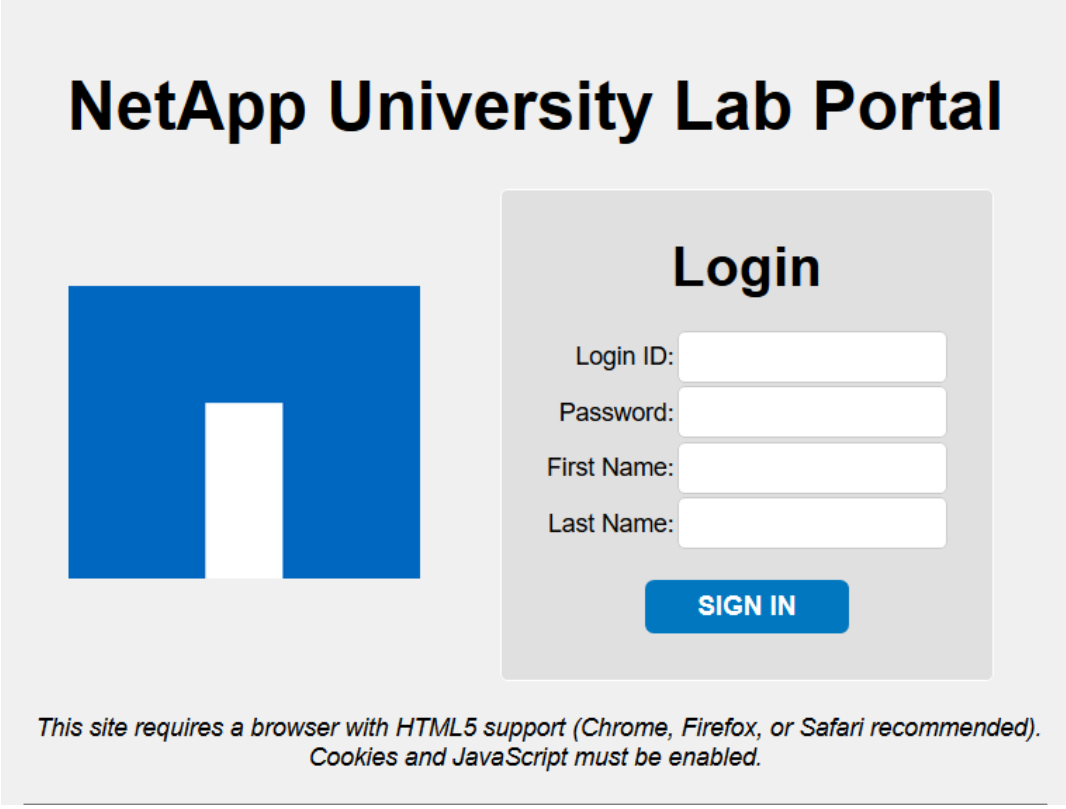
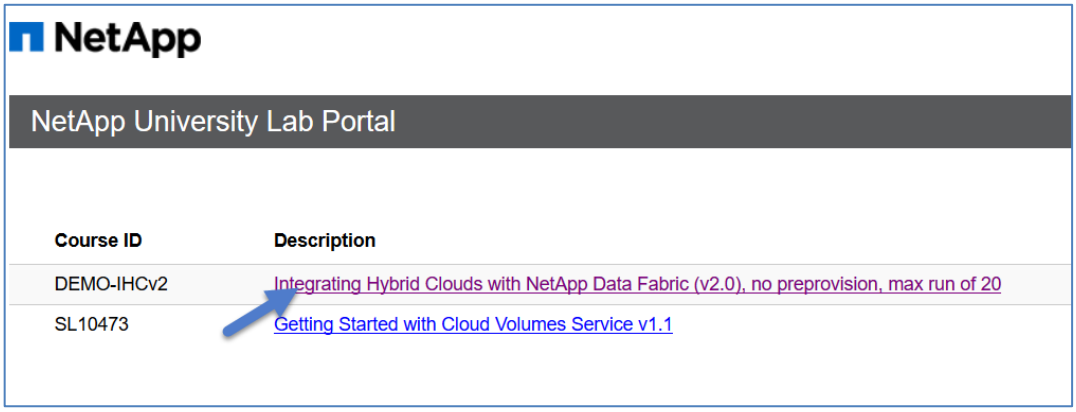
- One Windows Server 2016 system
- One ONTAP 9.5 single-node cluster (OnPrem)
- One pfSense VPN router

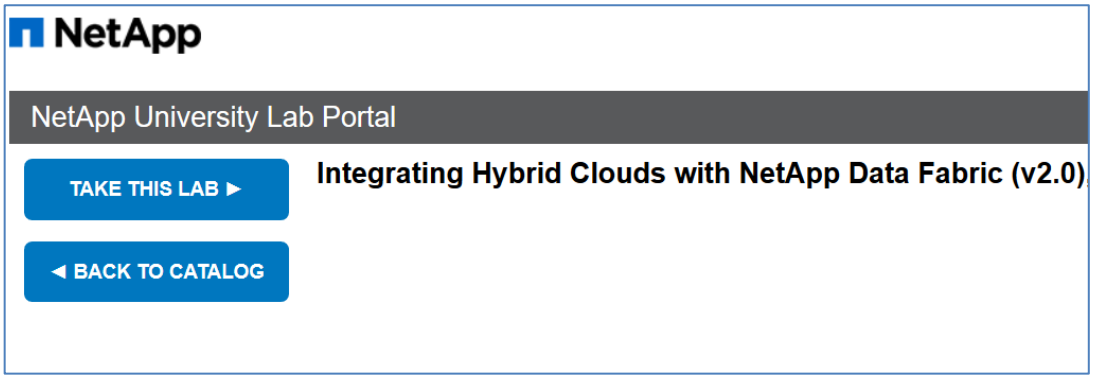
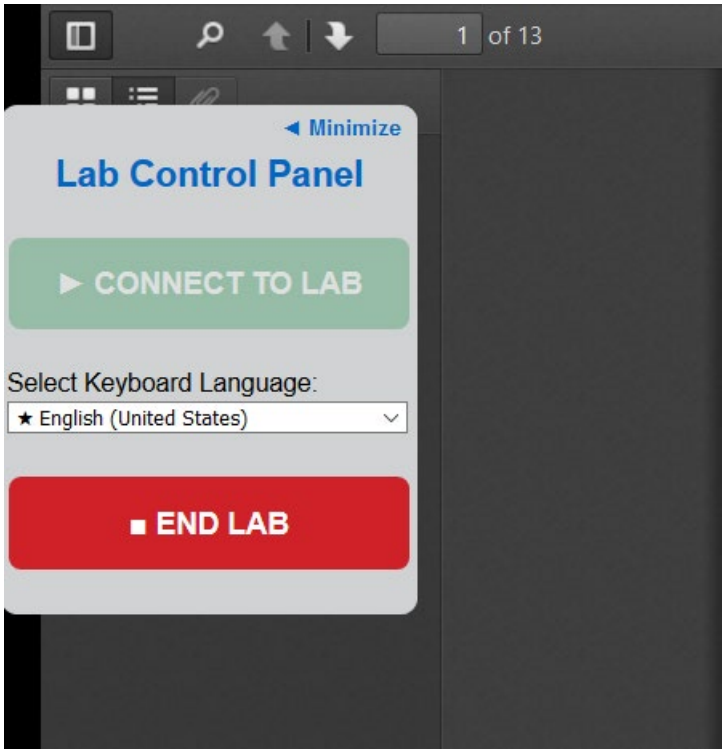
When you use the connection information that was assigned to you by your instructor, you are first connected by Remote Desktop Connection (Remote Desktop or RDC) to a Windows Server 2016. From this Windows desktop, you connect to the other servers in your exercise environment.

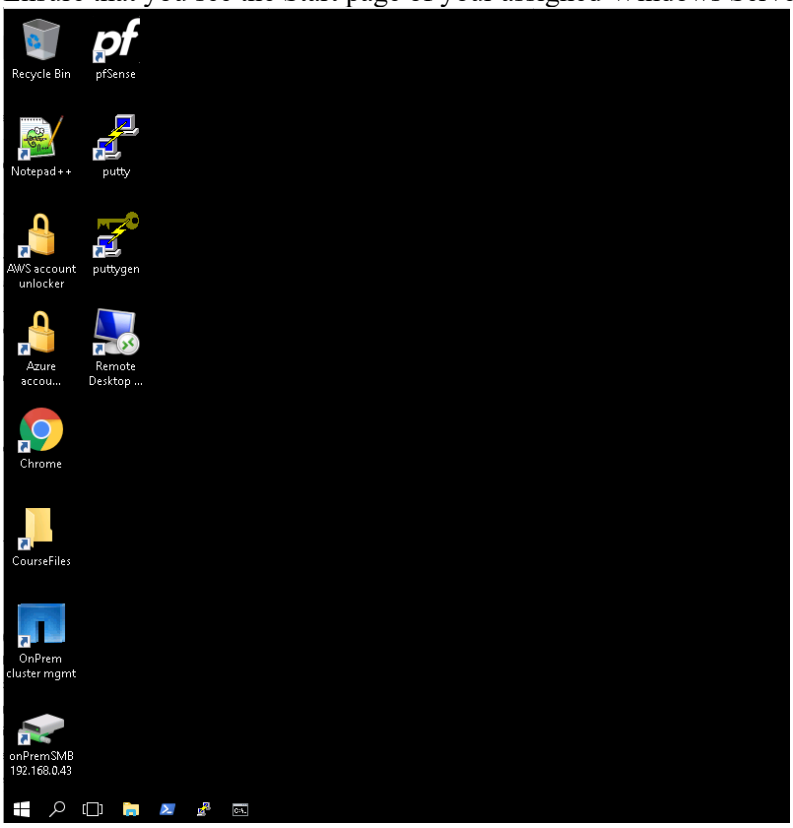


Task 0: Provision Your Lab Environment

In this task, you provision the Integrating Hybrid Cloud lab environment.

Step	Action
0-1	Open a web browser and enter https://naulabportal.netapp.com
0-2	Enter the following information and then click **SIGN IN**: • Login ID: <provided by instructor> • Password: <provided by instructor> • First Name: your first name • Last Name: your last name 
0-3	Click **Integrating Hybrid Clouds with NetApp Data Fabric**. 

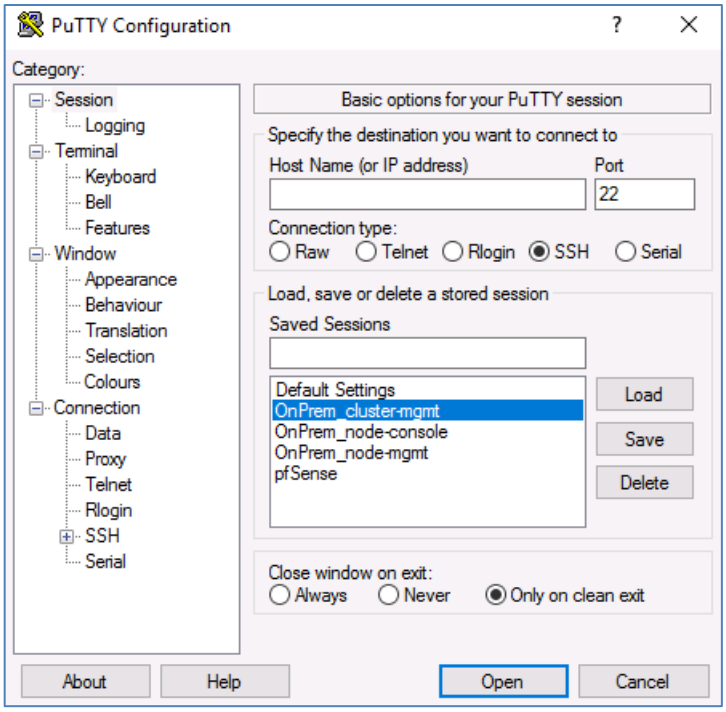
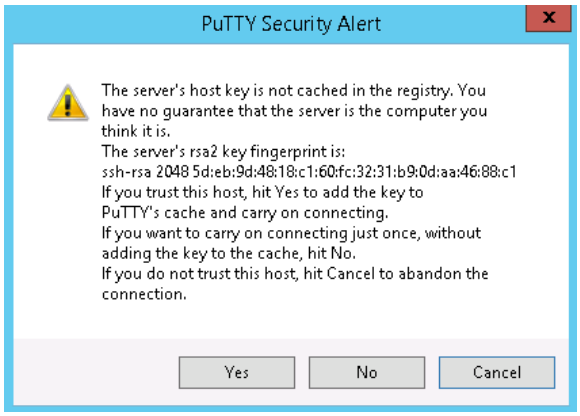
Step	Action
0-4	Click **TAKE THIS LAB**. 
0-5	Click **OK**.
0-6	Click **CONNECT TO LAB**. 

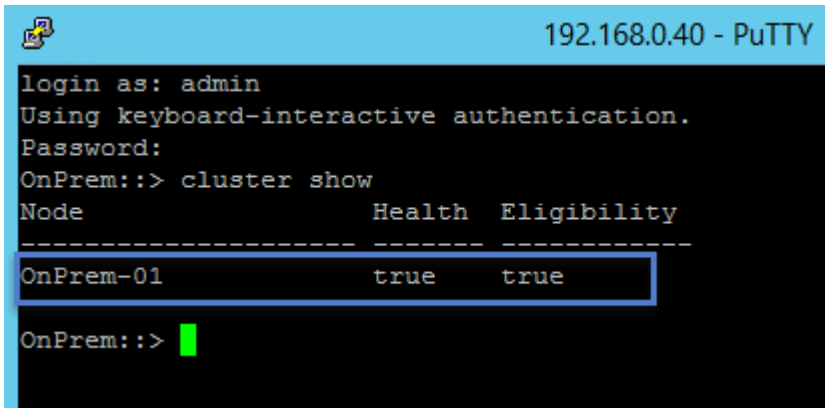
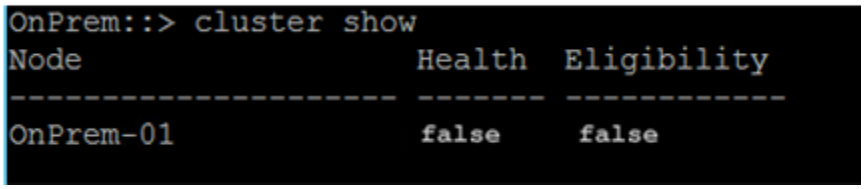
Step	Action
0-7	Ensure that you see the Start page of your assigned Windows Server 2016. 

Task 1: Ensure Connectivity to Your ONTAP Cluster

In this task, you familiarize yourself with the Windows Server 2016 desktop. You ensure connectivity to the ONTAP cluster and verify the health of the ONTAP cluster.

Step	Action
1-1	To connect to the ONTAP cluster web UI, you browse to the OnCommand System Manager URL, which is in ONTAP 9.5 software. To connect to the CLI of the ONTAP cluster, you use PuTTY. PuTTY is a UI for the Telnet and Secure Shell (SSH) protocols.
1-2	Double-click the PuTTY shortcut. 

Step	Action
1-3	In the PuTTY Configuration dialog box, verify that the OnPrem_cluster-mgmt saved session is listed, and then double-click **OnPrem_cluster-mgmt**. 
1-4	If a PuTTY Security Alert message appears, click **Yes**. 

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1-5</td><td>At the ONTAP cluster login prompt, provide the OnPrem cluster credentials:
▪ Login as: admin
▪ Password: Netapp1!
The ONTAP cluster CLI prompt and cursor appear.
 
</td></tr>
<tr><td>1-6</td><td>If you have difficulty logging in to the ONTAP cluster CLI, see the following table. You must ensure that you are using the correct user name and password in the correct case (both are case-sensitive).
<table>
<tr><th>System</th><th>Host Name</th><th>IP Address</th><th>User Name</th><th>Password</th></tr>
<tr><td>ONTAP cluster-management LIF</td><td>OnPrem</td><td>192.168.0.40</td><td>admin (case-sensitive)</td><td>Netapp1!</td></tr>
</table></td></tr>
<tr><td>1-7</td><td>Verify that the ONTAP cluster node is healthy and eligible:
cluster show
 
</td></tr>
<tr><td>1-8</td><td>If the health of the node is listed as false, alert your instructor.
 
</td></tr>
</table>

Task 2: Verify That Required License Codes Are Installed

Many of the advanced features of ONTAP software require licenses. In later exercises, you use several licensed features of ONTAP software. In this task, you ensure that the necessary licenses were preinstalled.

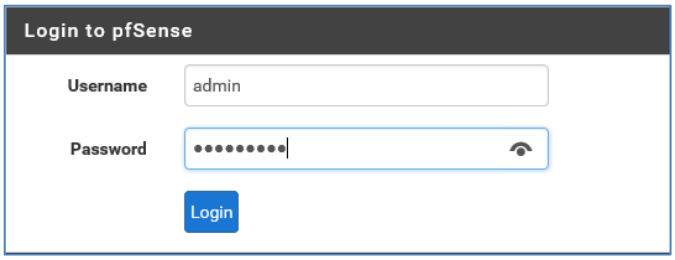
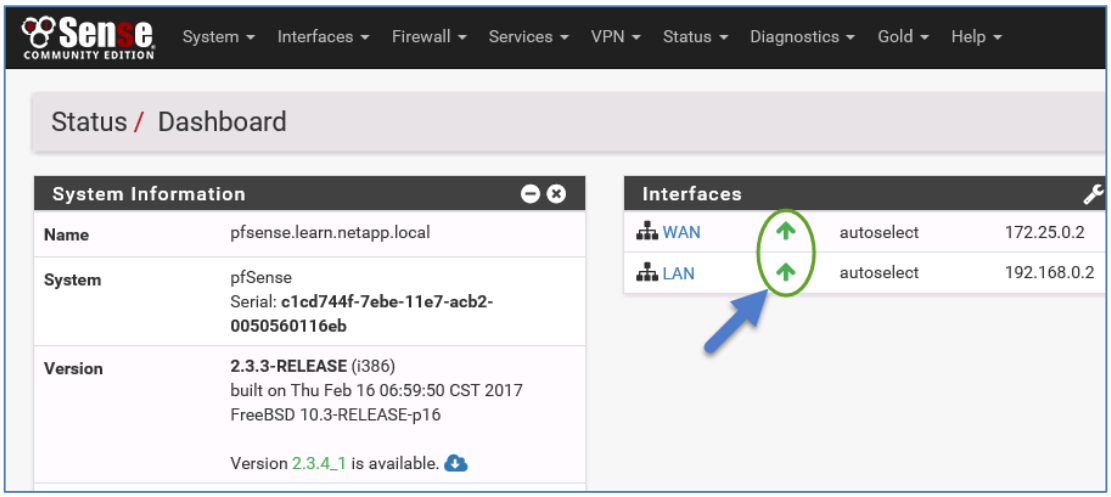
Your instructor provides you with license codes for any software that you need to install.

Step	Action

2-1	In the OnPrem-mgmt CLI, enter the following command:
	`license show`
	`OnPrem::> license show`
	`  (system license show)`
	
	`Serial Number: 1-80-000054`
	`Owner: OnPrem`
	`Package  Type  Description  Expiration`
	`Base  license  Cluster Base License  -`
	
	`Serial Number: 1-81-00000000000000000000071`
	`Owner: OnPrem-01`
	`Package  Type  Description  Expiration`
	`NFS  license  NFS License  -`
	`CIFS  license  CIFS License  -`
	`iSCSI  license  iSCSI License  -`
	`SnapRestore  license  SnapRestore License  -`
	`SnapMirror  license  SnapMirror License  -`
	`FlexClone  license  FlexClone License  -`
	`SnapVault  license  SnapVault License  -`

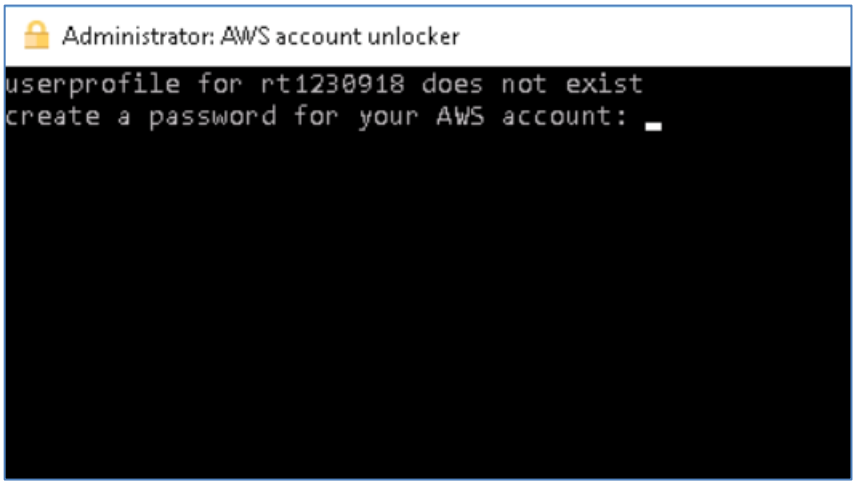
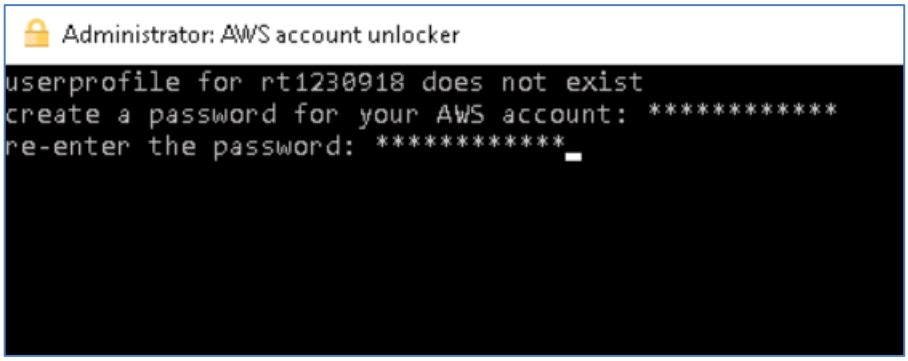
2-2	Verify that the required license codes (codes for the licenses that enable the features of ONTAP software that are required for later exercises) are installed: ▪ NFS ▪ CIFS ▪ iSCSI ▪ SnapRestore ▪ SnapMirror ▪ FlexClone ▪ SnapVault
2-3	 If any required license is not installed, contact NetApp University Support. There might be extra licenses installed that you can ignore.

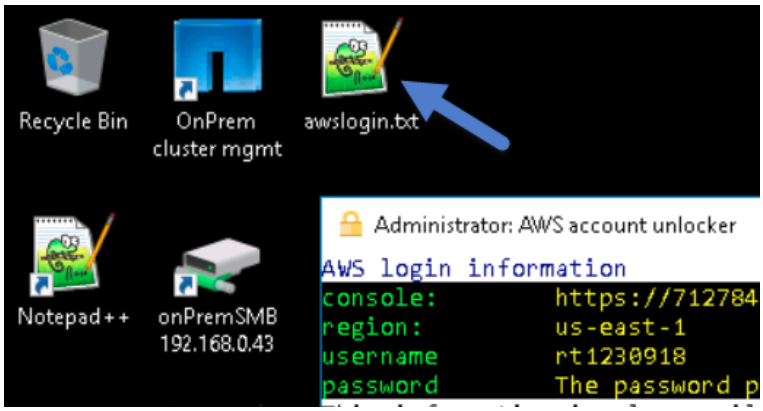
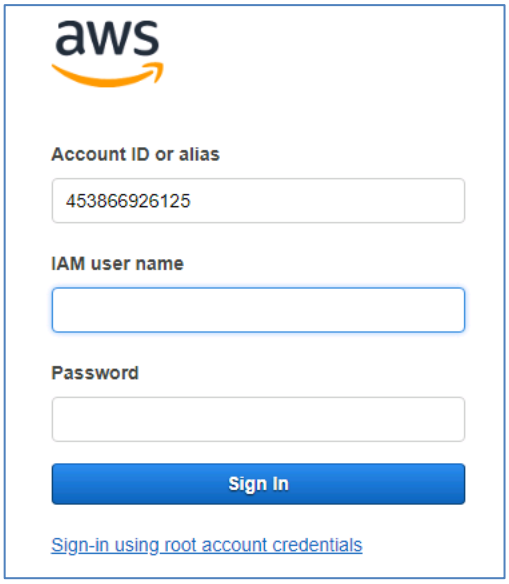
Task 3: Verify That pfSense Is Operational

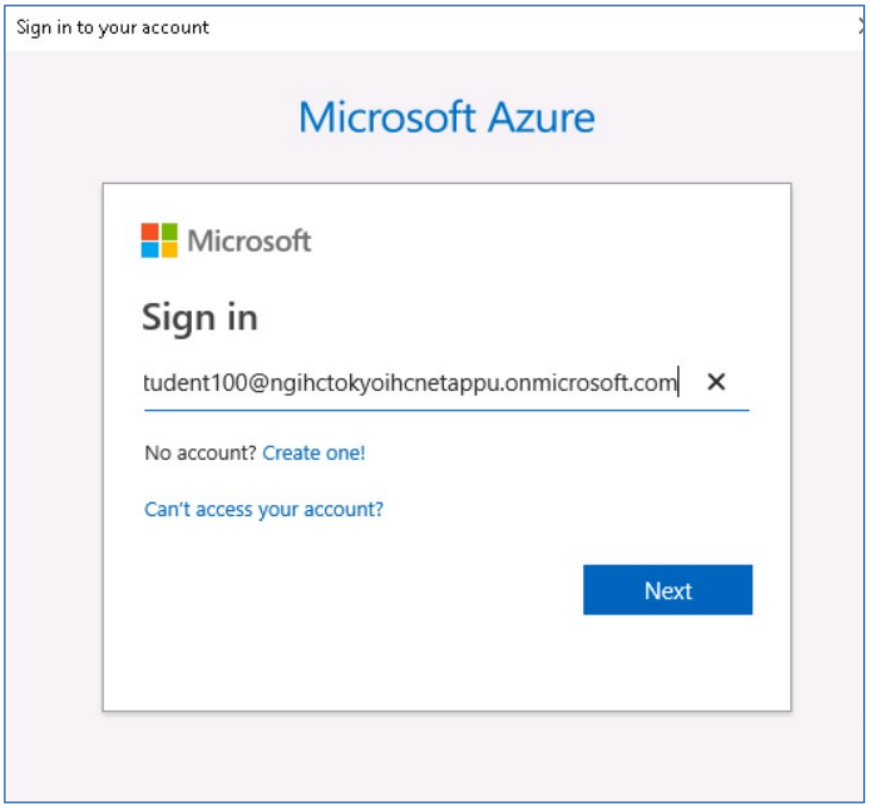
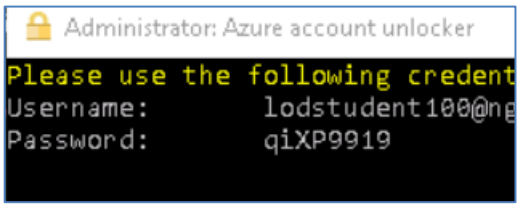
Step	Action
3-1	.
3-2	If a security warning appears, click **Click Advanced** and then click **Proceed to 192.168.0.1(unsafe)**.
3-3	Enter the following credentials: Username: **admin** Password: **Netapp1!** 
3-4	Verify that the pfSense interface appears and that the WAN and LAN interfaces are up. 

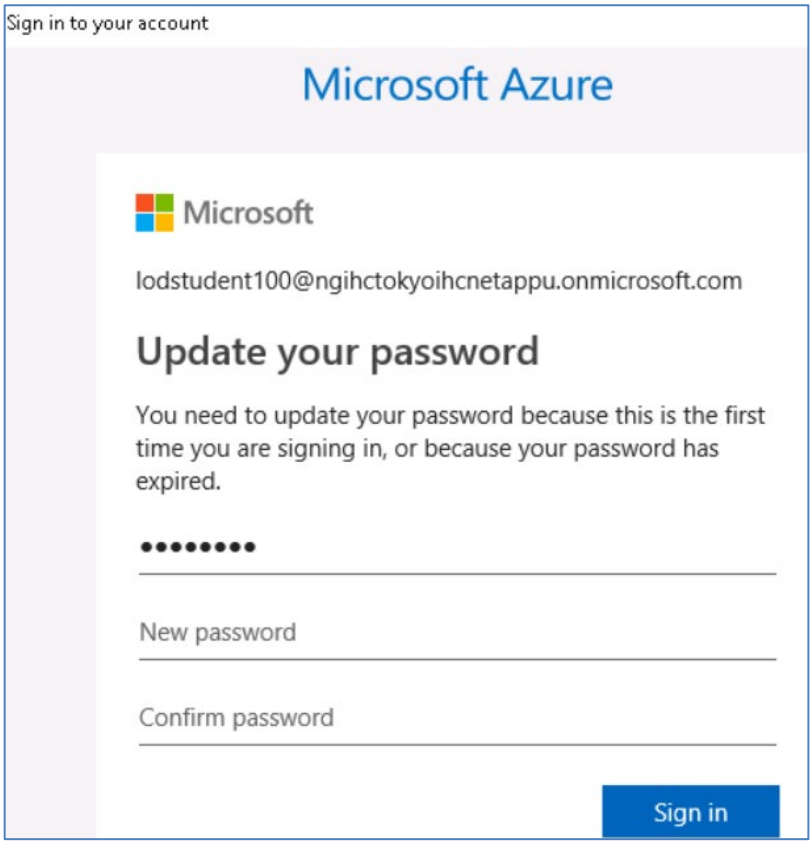
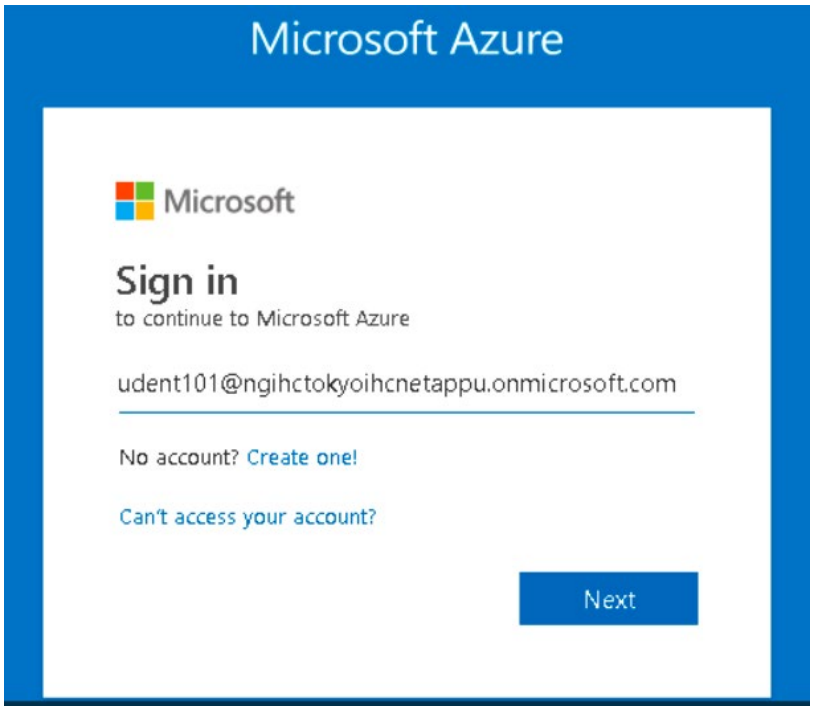
Task 4: Validate the AWS and Azure Accounts

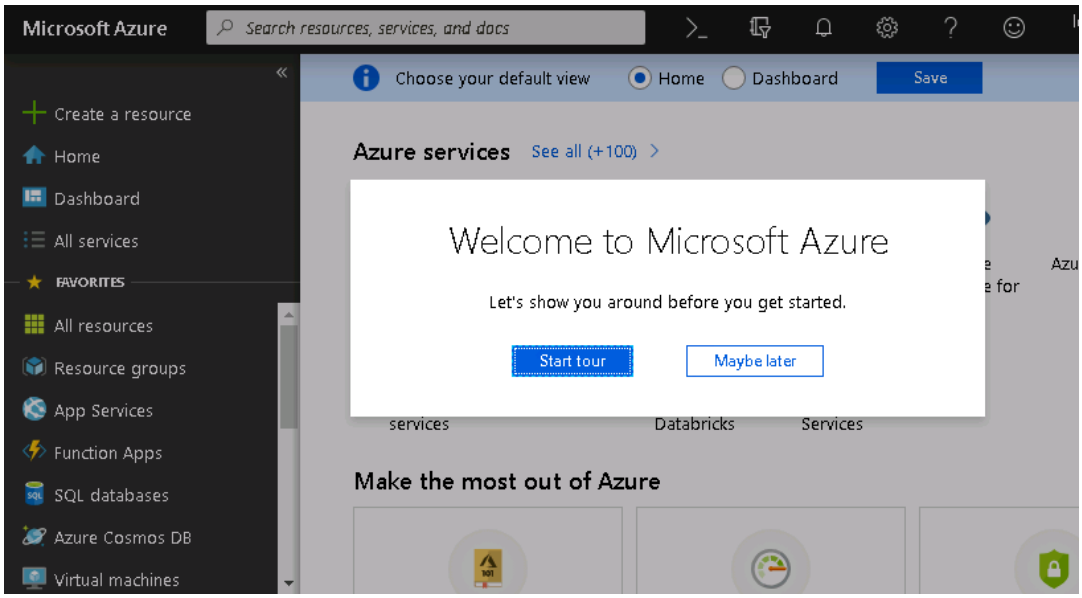
In this task, you access your assigned AWS and Azure accounts, configure a password, and verify that you can log in to the account.

Step	Action
4-1	On your Windows Server jump host, double-click the **AWS account unlocker** shortcut. 
4-2	In the Administrator AWS account unlocker window, create a password for your AWS account, (for example, Netapp1!). 
4-3	Re-enter your password and press **Enter**. 

Step	Action
4-4	Verify that an awslogin.txt file is created on the desktop. Note this text file contains your username and the AWS console login link if you need it later. 
4-5	Double click the awslogin.txt file and copy the username to your clip board.
4-6	Return to the AWS account unlocker window and press **Enter**.
4-7	In the AWS Console login page, enter this username and the password that you created and click **Sign In**. 
4-8	Verify that the login is successful.
4-9	If you forget your user name or the AWS console login address, you can view the awslogin.txt file that was created by the AWS account unlocker tool.

Step	Action
4-10	On your Windows Server jump host, double-click the **Azure account unlocker** shortcut. 
4-11	In the Azure login window that appears, enter your user name (you copy and paste it from the azurelogin.txt file on the jump host desktop). 
4-12	Click **Next**.
4-13	Enter the password that is displayed in the Azure account unlocker, and click **Sign In**. 

Step	Action
4-14	Update the password to a password of your choice, and click **Sign in**. 
4-15	When you are returned to the Azure account unlocker, press **Enter** to get to the Azure portal.
4-16	Enter your username and click **Next**. 

Step	Action
4-17	Enter your password and click **Sign In**.
4-18	When you are returned to an Azure login page, enter your user name and password and verify that you see the Azure portal. 

End of Exercise

Module 1: Data Fabric Overview

Exercise 1: Control Cloud Resources with Windows PowerShell

In this exercise, you install Amazon Web Services (AWS) Tools for Windows PowerShell and use PowerShell to control AWS resources. You also install Microsoft Azure PowerShell and issue various Azure commands.

Objectives

This exercise focuses on enabling you to do the following:

- Install AWS Tools for Windows PowerShell
- Use AWS PowerShell commands to control AWS resources
- Install the Azure PowerShell tools
- Install NetApp PowerShell Toolkit and run NetApp PowerShell commands

Task 1: Install AWS Tools for Windows PowerShell

In this task, you install AWS Tools for Windows PowerShell and configure your AWS credentials to enter commands.

Step	Action
1-1	On your Windows Server jump host, in the taskbar, click the PowerShell icon. 
1-2	Verify that the Windows PowerShell window opens.

1-3	Determine which version of PowerShell is installed:
	`PS C:\Users\Administrator> $PSVersionTable`
	Sample output:
	`PSV Name Value`
	`---- -----`
	`PSVersion 5.1.14393.206`
	`PSEdition Desktop`
	`PSCompatibleVersions {1.0, 2.0, 3.0, 4.0...}`
	`BuildVersion 10.0.14393.206`
	`CLRVersion 4.0.30319.42000`
	`WSManStackVersion 3.0`
	`PSRemotingProtocolVersion 2.3`
	`SerializationVersion 1.1.0.1`
	Note: AWS requires at least version 2.0 of PowerShell.

Step	Action
1-4	The AWS Tools for Windows PowerShell tools are installed on your jump host for use in this exercise. In a production environment, you install the tools by completing the following actions: a. Open a browser, and then enter the following URL: http://aws.amazon.com/powershell b. Click AWS Tools for Windows. c. Run the downloaded MSI installer. d. Follow the installation instructions that appear. 

1-5	Return to the PowerShell window, and then check the PowerShell execution policy:
	`PS> Get-ExecutionPolicy`
	Sample output:
	`Restricted`

1-6	If the execution policy is not set to RemoteSigned, enter the following command: `PS> Set-ExecutionPolicy RemoteSigned`
1-7	If the execution policy is not set correctly, PowerShell generates the following message: `File C:\Users\teslan\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1 cannot be loaded because the execution of scripts is disabled on this system. Please see "get-help about_signing" for more details.`
1-8	If you changed the execution policy, close the current PowerShell window, and then open a new PowerShell window.

Step	Action

1-9	Verify that the module is loaded:
	`PS> **Get-Module -ListAvailable**`
	Sample output:
	…
	`ModuleType Version Name ExportedCommands`
	`---------- ------- ---- ----------------`
	`Binary 3.3.84.0 **AWSPowerShell** {Clear-AWSHistory,`
	`Set-AWSHistoryConfiguration,`
	`Initialize...`
	…
	Note: The AWS Tools for Windows PowerShell installer automatically updates the `PSModulePath` to include the location of the directory.

Step	Action

1-10	Determine which version of AWS Tools for Windows PowerShell is installed and which services are available:
	`PS> **Get-AWSPowerShellVersion -ListServices**`
	Sample output:
	`AWS Tools for Windows PowerShell`
	`Copyright 2012-2017 Amazon.com, Inc. or its affiliates. All Rights Reserved.`
	
	`Amazon Web Services SDK for .NET`
	`Core Runtime Version 3.3.13.3`
	`Copyright 2009-2015 Amazon.com, Inc. or its affiliates. All Rights Reserved.`
	
	`Release notes: https://aws.amazon.com/releasenotes/PowerShell`
	
	`This software includes third party software subject to the following copyrights:`
	`- Logging from log4net, Apache License [http://logging.apache.org/log4net/license.html]`
	
	`Service Noun Prefix API Version`
	`------- ----------- -----------`
	`AWS AppStream APS 2016-12-01`
	`AWS Batch BAT 2016-08-10`
	`AWS Budgets BGT 2016-10-20`
	`AWS Certificate Manager ACM 2015-12-08`
	`AWS Cloud Directory CDIR 2016-05-10`
	`AWS Cloud HSM HSM 2014-05-30`
	`AWS CloudFormation CFN 2010-05-15`
	`AWS CloudTrail CT 2013-11-01`
	`AWS CodeBuild CB 2016-10-06`
	`AWS CodeCommit CC 2015-04-13`
	`AWS CodeDeploy CD 2014-10-06`
	`AWS CodePipeline CP 2015-07-09`
	`AWS CodeStar CST 2017-04-19`
	`...`

1-11	 Each AWS Tools for Windows PowerShell command must include a set of AWS credentials, which is used to cryptographically sign the corresponding web service request.

1-12	Use the AWS software development kit (SDK) store to encrypt your credentials and to set your credentials as the default (enter the following command all on one line):
	`PS> **Set-AWSCredentials`
	`**-AccessKey** <*the access key in the awslogin.txt file*>`
	`**-SecretKey** <*the secret key in the awslogin.txt file*>`
	`**-StoreAs default**`

Step	Action
1-13	If you ever need to generate new AWS Access Keys, you perform these steps: (For information only) a. In the AWS console, select Services > IAM > Users. a. Click the user for which you want to generate the keys. b. Click the Security credentials tab. c. Click Create access key. d. Click Download .csv file.
1-14	Set the default region: `PS> Set-DefaultAWSRegion -Region us-east-1`
1-15	The default region setting persists only for the current session. To apply the setting to all PowerShell sessions, you use the **`Initialize-AWSDefaults`** command. For more information, you can see Using AWS Credentials: http://docs.aws.amazon.com/powershell/latest/userguide/specifying-your-aws-credentials.html

1-16	Run the following command to get a list of availability zones in the region:
	`PS> Get-EC2AvailabilityZone`
	Sample output:
	`Messages RegionName State ZoneName`
	`-------- ---------- ----- --------`
	`{} us-east-1 available us-east-1a`
	`{} us-east-1 available us-east-1b`
	`{} us-east-1 available us-east-1c`
	`{} us-east-1 available us-east-1d`
	`{} us-east-1 available us-east-1e`
	`{} us-east-1 available us-east-1f`

1-17	Run the following command to list the IAM Users in your AWS account:
	`PS> Get-IAMUsers`
	Sample output:
	`Arn : arn:aws:iam::827153241274:user/rt1233780`
	`CreateDate : 1/22/2019 9:04:40 PM`
	`PasswordLastUsed : 1/23/2019 3:38:10 PM`
	`Path : /`
	`UserId : AIDAJSQJMNTYGOODOU2NE`
	`UserName : rt1233780`

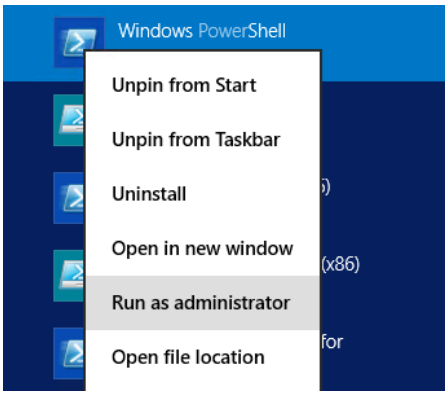
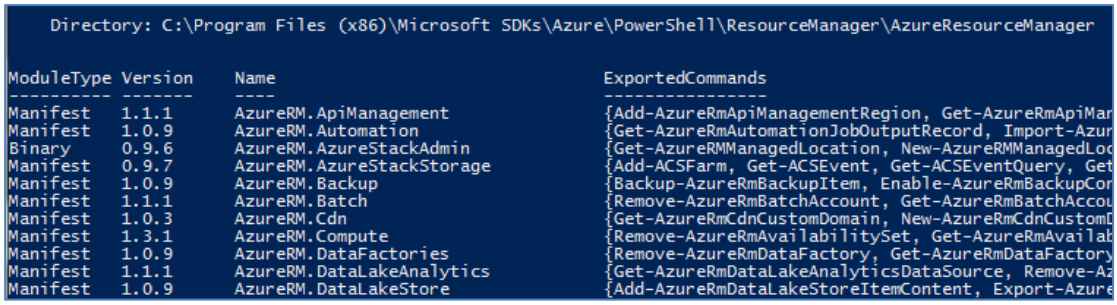
Step	Action
1-18	Run the following command to list of EC2 images that you can use: `PS> Get-EC2ImageByName` Sample output: 

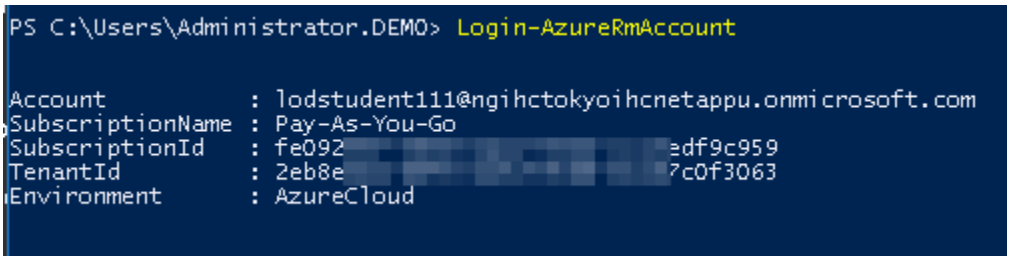
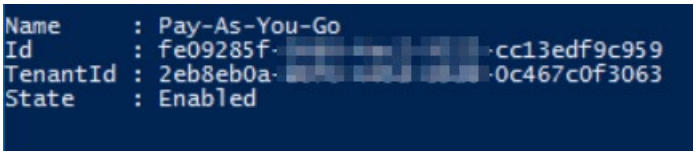
Step	Action

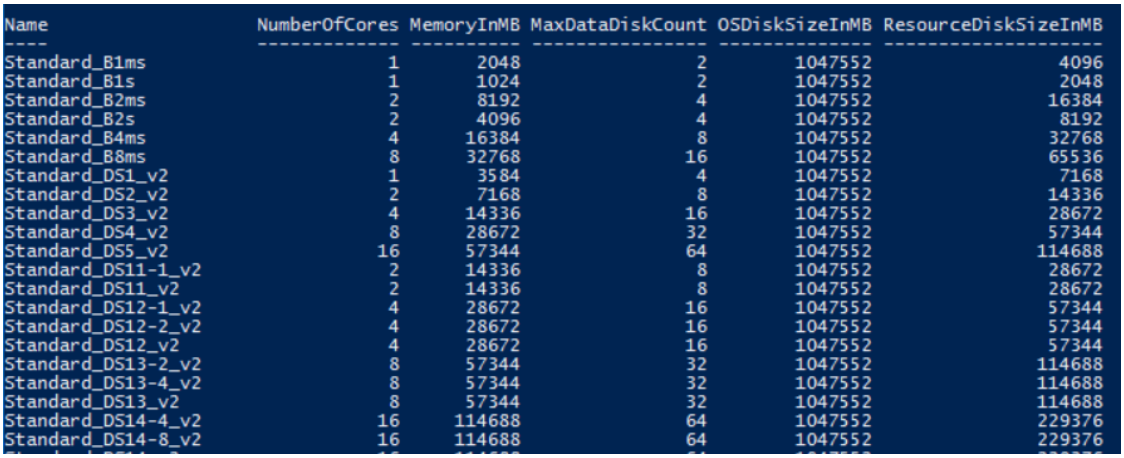
1-19	Run the following command to list of EC2 images that you can use:
	`PS> Get-EC2ImageByName -Name WINDOWS_2016_BASE`
	Sample output:
	`Architecture : x86_64`
	`BlockDeviceMappings : {/dev/sda1, xvdca, xvdcb, xvdcc...}`
	`CreationDate : 2019-01-10T01:51:19.000Z`
	`Description : Microsoft Windows Server 2016 with Desktop Experience Locale`
	`EnaSupport : True`
	`Hypervisor : xen`
	`ImageId : ami-0f4c7e570f044b46f`
	`ImageLocation : amazon/Windows_Server-2016-English-Full-Base-2019.01.10`
	`ImageOwnerAlias : amazon`
	`ImageType : machine`
	`KernelId :`
	`Name : Windows_Server-2016-English-Full-Base-2019.01.10`
	`OwnerId : 801119661308`
	`Platform : Windows`
	`ProductCodes : {}`
	`Public : True`
	`RamdiskId :`
	`RootDeviceName : /dev/sda1`
	`RootDeviceType : ebs`
	`SriovNetSupport : simple`
	`State : available`
	`StateReason :`
	`Tags : {}`
	`VirtualizationType : hvm`

Task 2: Install Azure PowerShell

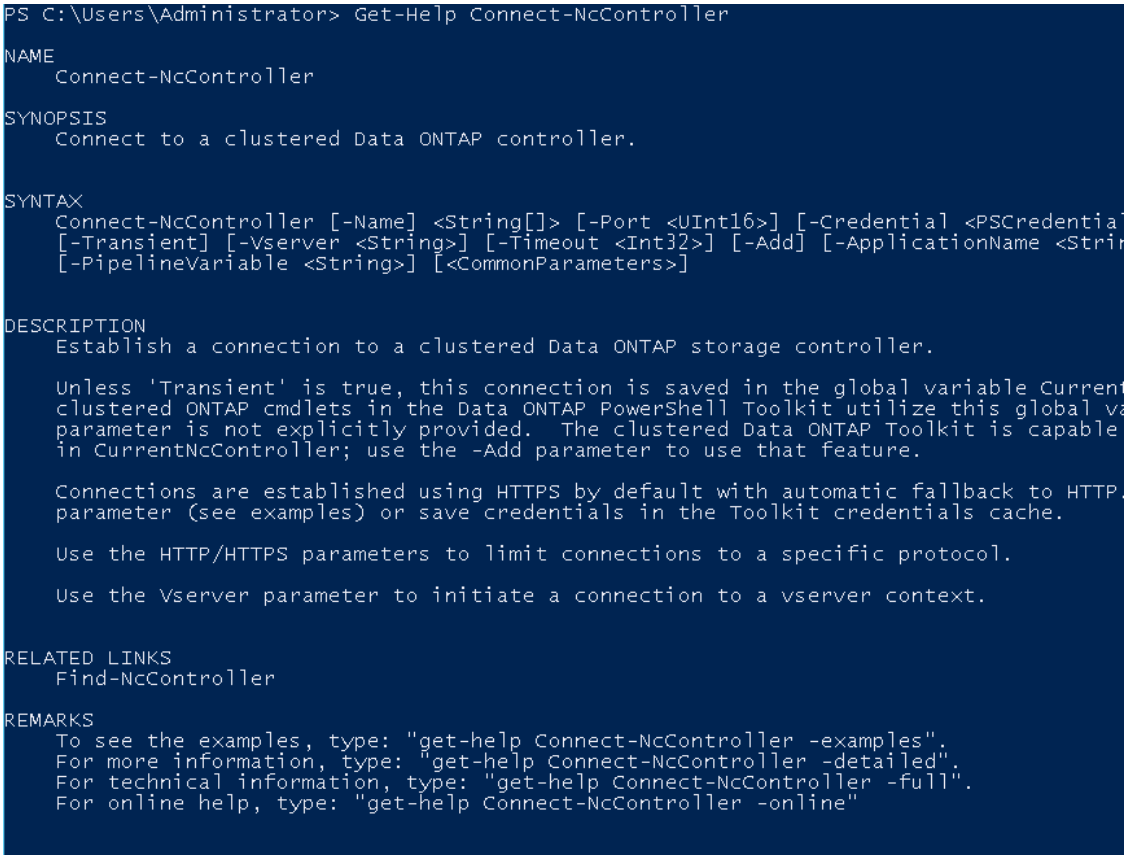
Step	Action
2-1	The Azure PowerShell tools are installed on your jump host. In a production environment, you install the tools by completing the following actions: a. Open a browser, and then enter the following URL: https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-1.0.0 b. Click Install Azure PowerShell with PowerShellGet. c. In PowerShell, enter `Install-Module -Name AzureRM` d. Follow the installation instructions that appear.

Step	Action
2-2	Open your PowerShell window: a. Select the Windows PowerShell application. b. Select **Run as administrator**. 
2-3	Enter the following command: `PS C:\Users\Administrator.DEMO>` **`Get-Module -ListAvailable`** Sample concatenated output 
2-4	If you do not have the azurelogin.txt file open, double click it to open it, to have your account information available.
2-5	Enter the following command: `PS>` **`Login-AzureRmAccount`**
2-6	In the Sign in to your account window, enter the following information: • Email or phone: *<Found in azurelogin.txt file on your desktop>* • Password: *<Password that you set up for your Azure account>* **Note:** If a dialog box asks whether the account is a Work or Personal account, select **Personal**.

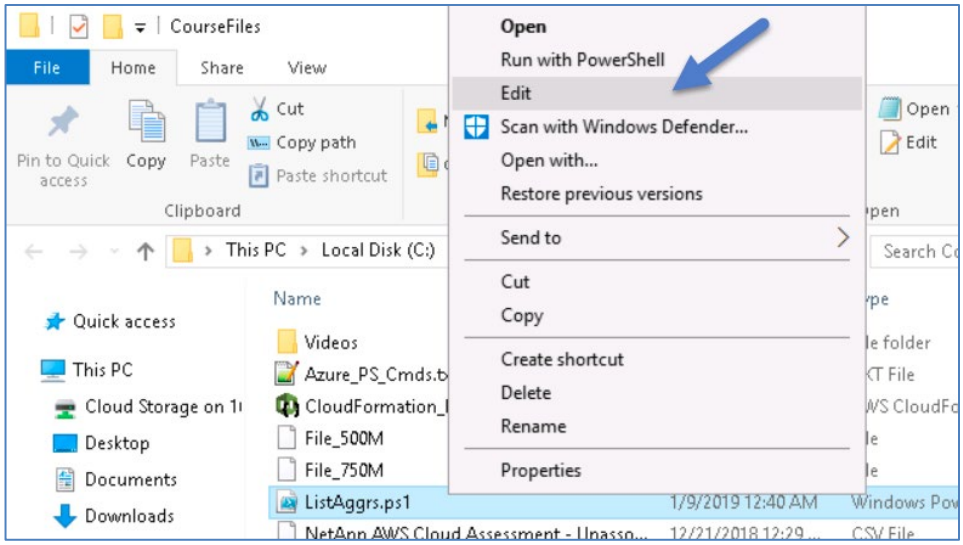
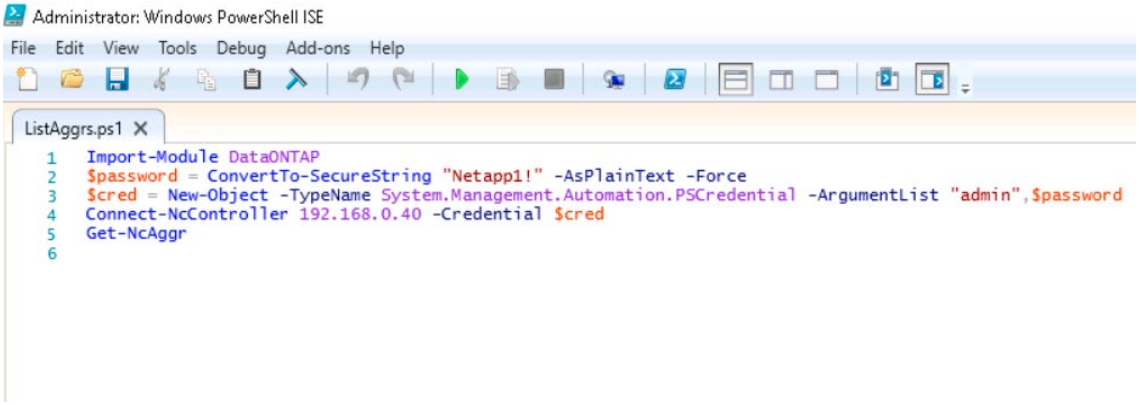
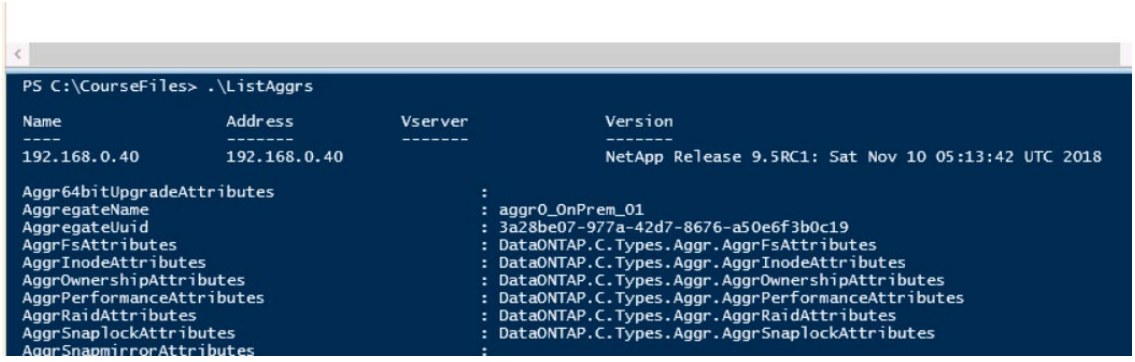
Step	Action
2-7	In the PowerShell window, confirm your account information. 
2-8	View all subscriptions for your account: `PS> Get-AzureRmSubscription` Sample output: 

2-9	View the VM sizes available in us-east.
	`PS> Get-AzureRmVMSize -Location "East US"`
	`Sample concatenated output:`
	 

Task 3: Install the NetApp PowerShell Toolkit

Step	Action
3-1	The toolkit is installed on your jump host for use in this exercise. In a production environment, you install the tools by completing the following actions: a. Open a browser, and then enter the following URL: http://mysupport.netapp.com/tools/info/ECMLP2310788I.html?productID=61926/ b. Select I have read and agree to the License Terms & Conditions. c. Click Continue. d. Click NetApp_PowerShell_Toolkit_4.7.0.msi. e. Run the downloaded installer. f. Follow the installation instructions that appear.
3-2	Import the ONTAP module: `PS C:\Users\Administrator> Import-Module DataONTAP`
3-3	Review the basic commands for ONTAP software: `PS> Show-NcHelp`
3-4	Confirm the details of a connect command: `PS> Get-Help Connect-NcController` Sample output: 

```
PS C:\Users\Administrator> Get-Help Connect-NcController

NAME
    Connect-NcController

SYNOPSIS
    Connect to a clustered Data ONTAP controller.


SYNTAX
    Connect-NcController [-Name] <String[]> [-Port <UInt16>] [-Credential <PSCredentia
    [-Transient] [-Vserver <String>] [-Timeout <Int32>] [-Add] [-ApplicationName <Strin
    [-PipelineVariable <String>] [<CommonParameters>]


DESCRIPTION
    Establish a connection to a clustered Data ONTAP storage controller.

    Unless 'Transient' is true, this connection is saved in the global variable Current
    clustered ONTAP cmdlets in the Data ONTAP PowerShell Toolkit utilize this global va
    parameter is not explicitly provided.  The clustered Data ONTAP Toolkit is capable
    in CurrentNcController; use the -Add parameter to use that feature.

    Connections are established using HTTPS by default with automatic fallback to HTTP.
    parameter (see examples) or save credentials in the Toolkit credentials cache.

    Use the HTTP/HTTPS parameters to limit connections to a specific protocol.

    Use the Vserver parameter to initiate a connection to a vserver context.


RELATED LINKS
    Find-NcController

REMARKS
    To see the examples, type: "get-help Connect-NcController -examples".
    For more information, type: "get-help Connect-NcController -detailed".
    For technical information, type: "get-help Connect-NcController -full".
    For online help, type: "get-help Connect-NcController -online"
```

Step	Action
3-5	Using Windows Explorer, go to the CourseFiles folder, right-click the file **ListAggrs.ps1** and then select **Edit**. 
3-6	Review the commands: 
3-7	At the bottom of the screen run the script: `PS C:\CourseFiles> .\ListAggrs.ps1` Sample concatenated output: 

End of Exercise

Module 1: Data Fabric Overview

Exercise 2: Assess Azure and Amazon Web Services Environments

In this exercise, you run the Amazon Web Services (AWS) and Azure Assessment tool in NetApp Cloud Central to determine orphaned resources and unprotected items.

Objectives

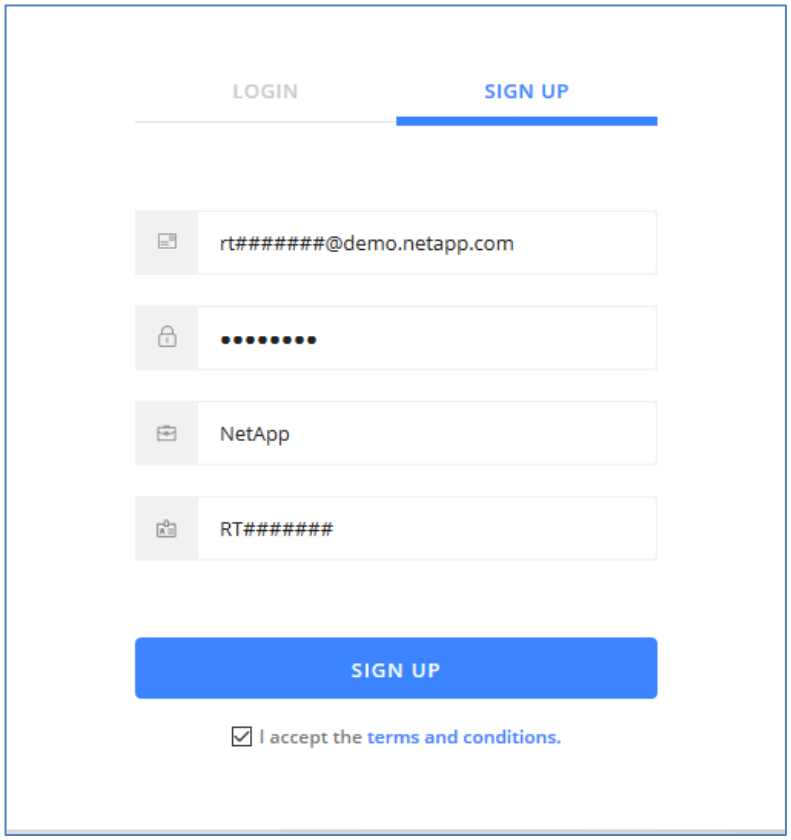
This exercise focuses on enabling you to do the following:

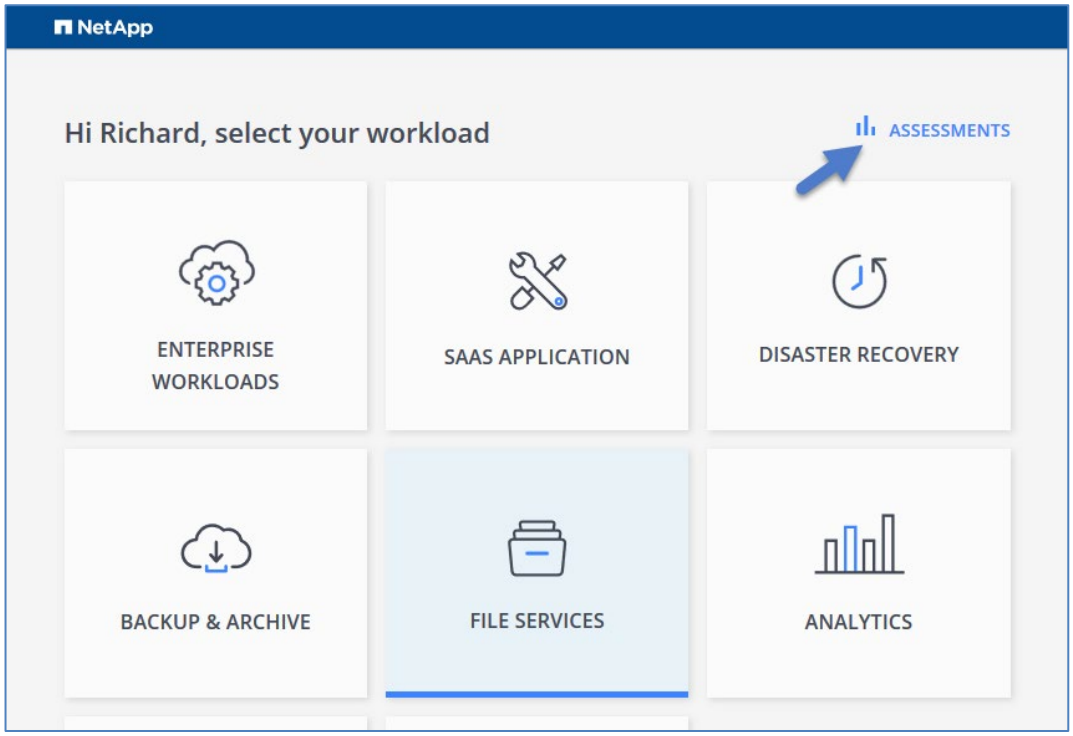
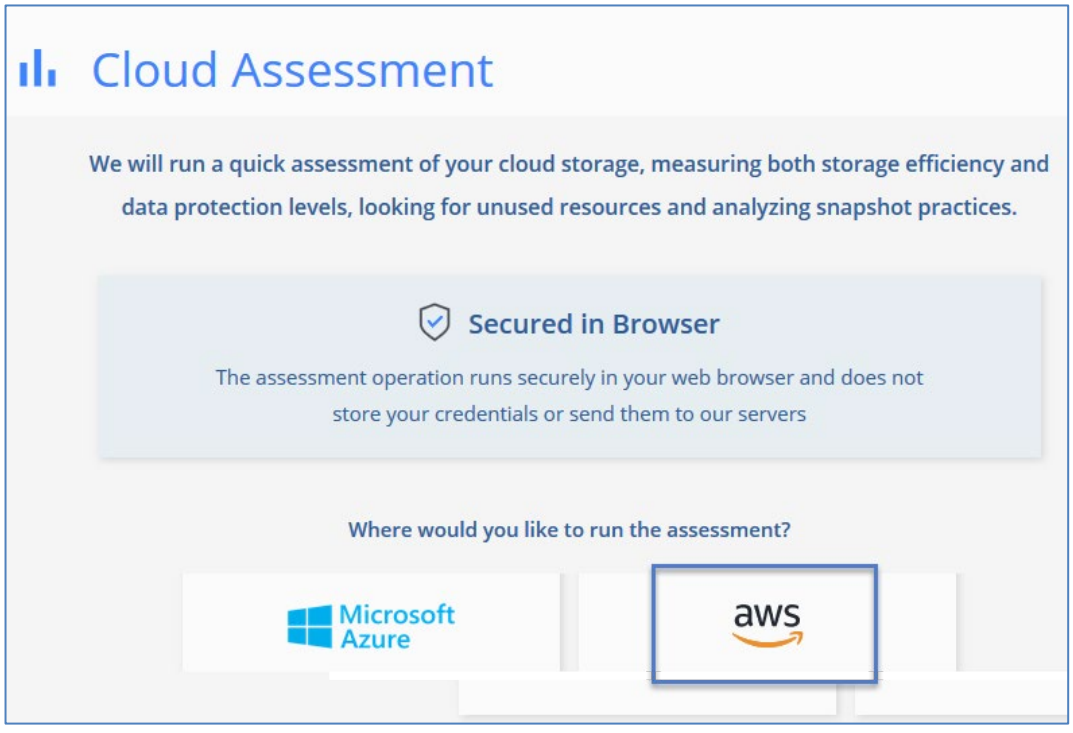
- Find unattached Amazon Elastic Block Store (Amazon EBS) volumes (AWS) and unattached disks (Azure)
- Find unassociated snapshots

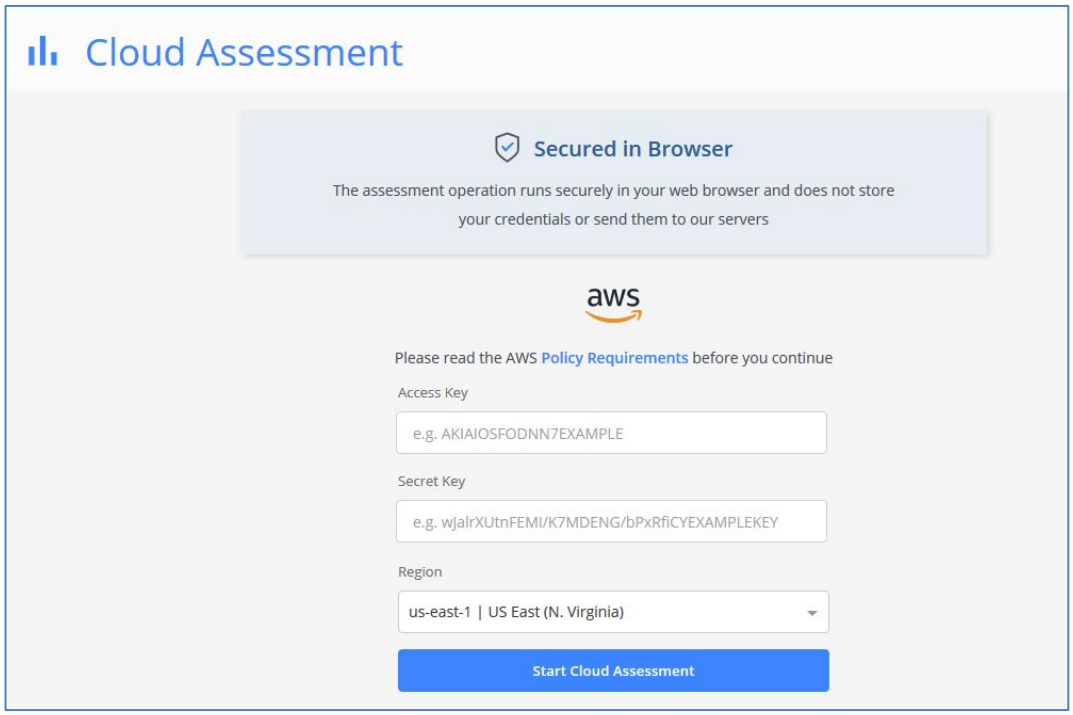
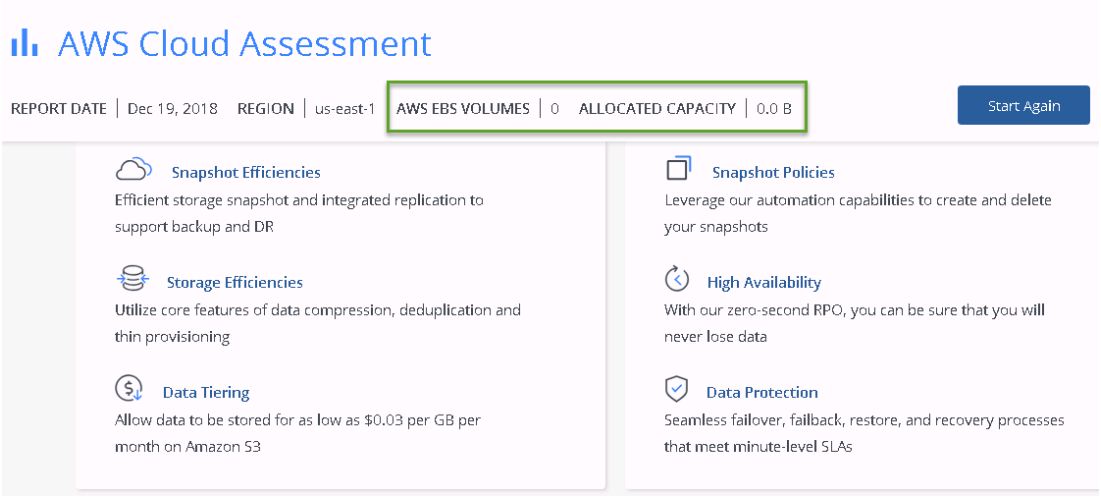
Task 1: Perform Cloud Assessments by Using Cloud Central

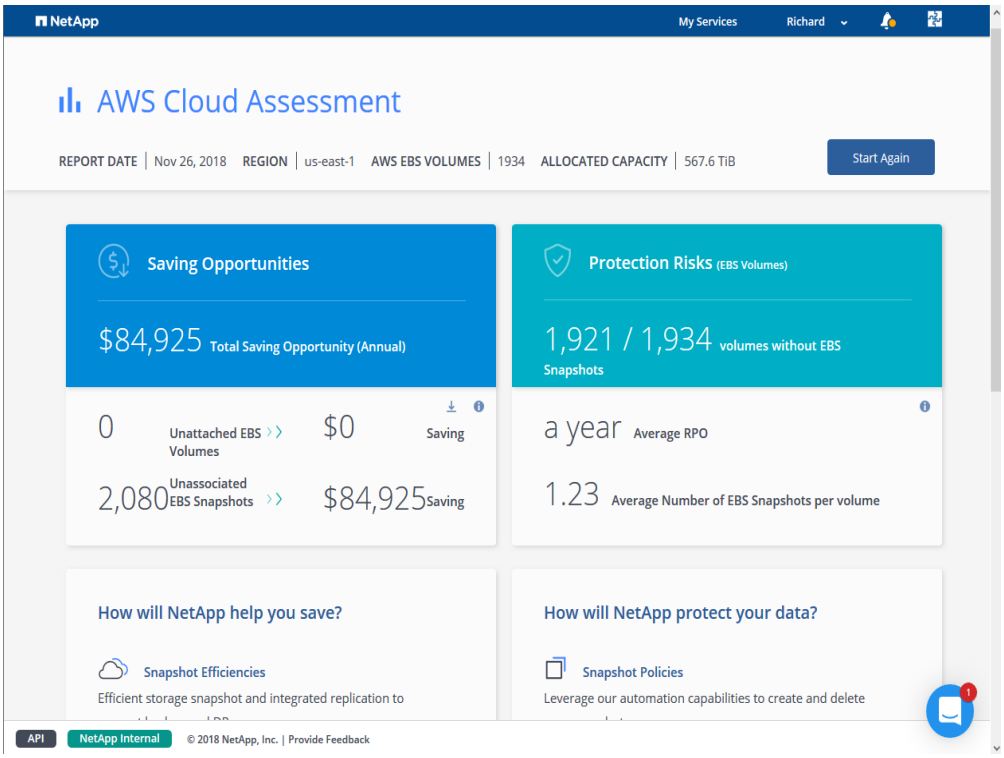
In this task, you run cloud assessments on your AWS and Azure accounts.

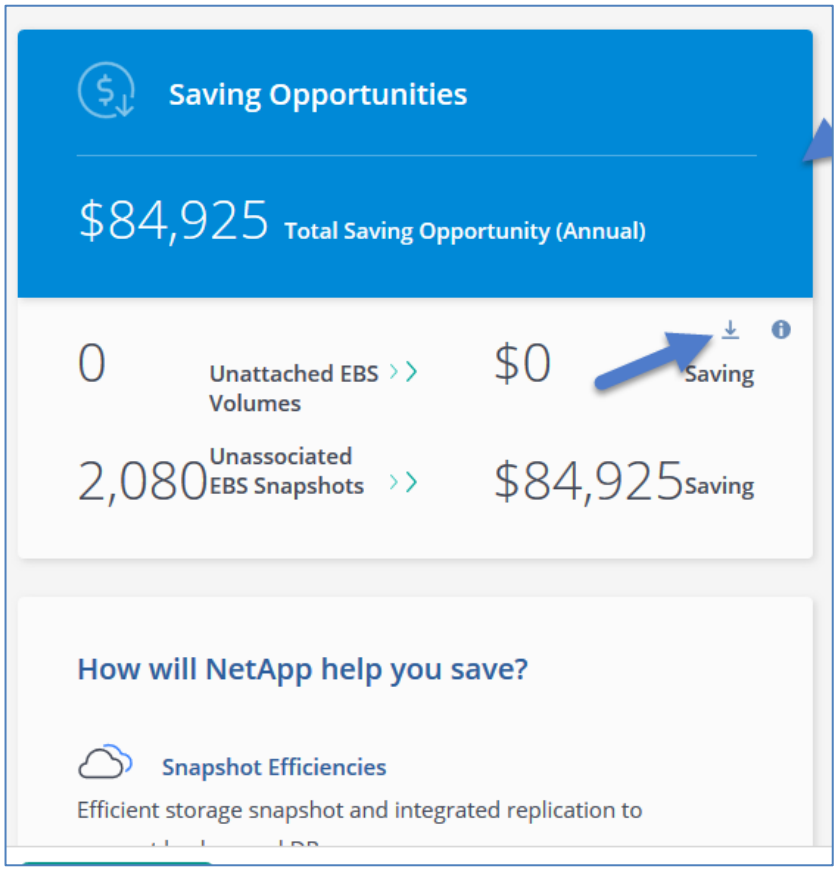
Step	Action
1-1	Navigate to **cloud.netapp.com**.
1-2	Click **SIGN UP**.

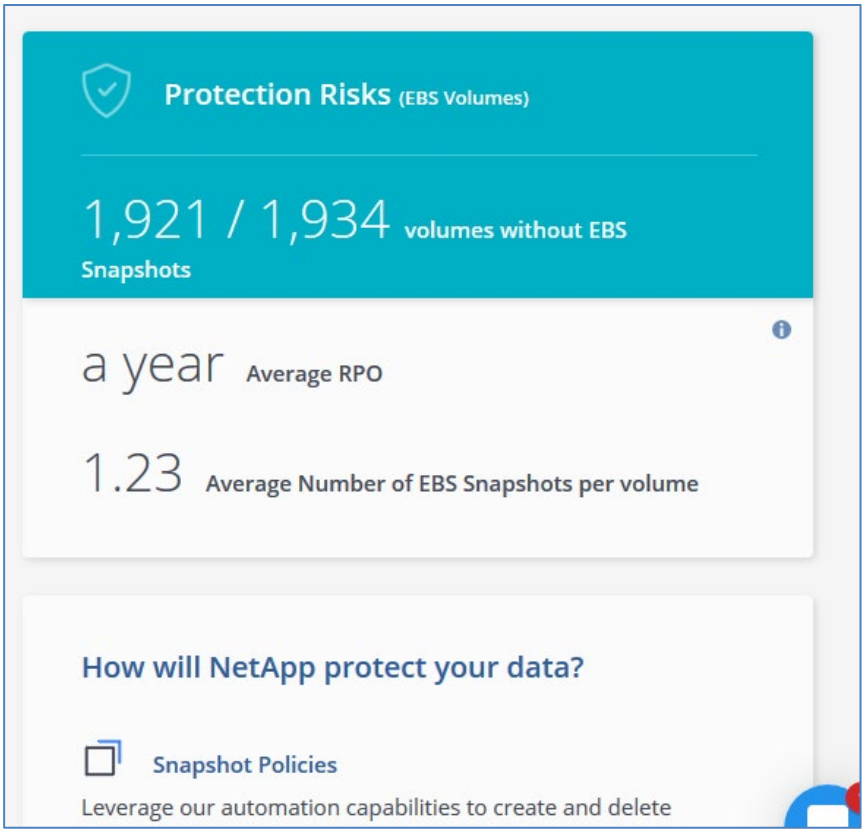
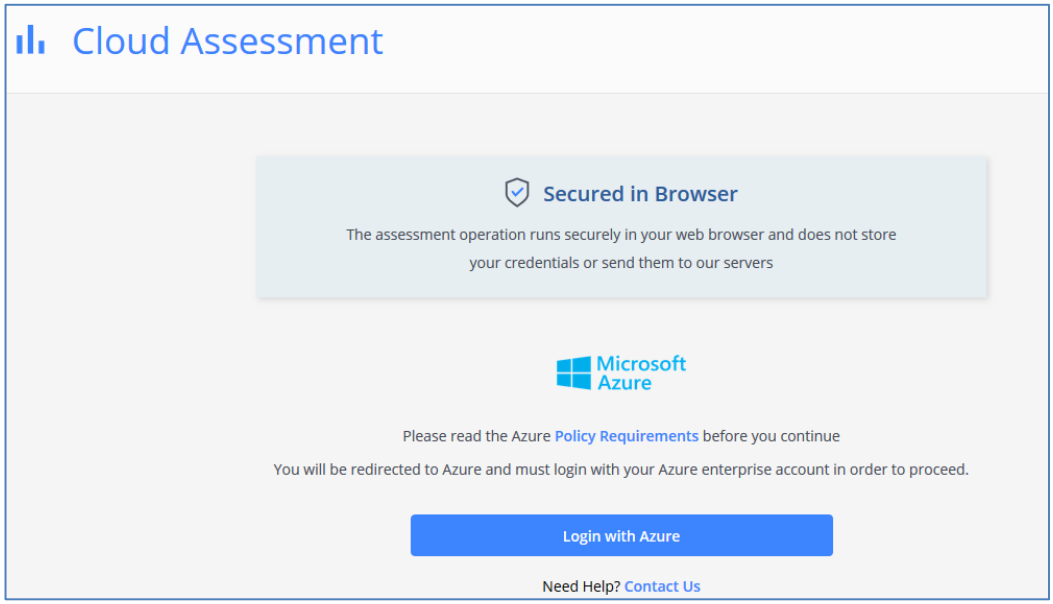
Step	Action
1-3	On the SIGN UP tab, enter the following information: • Email: <*your user name in the awslogin.txt file*>**@demo.netapp.com** • Password: **Netapp1!** • Company: **NetApp** • Full Name: <*your user name in the awslogin.txt file*> • Select **I accept the terms and conditions** check box. 
1-4	Click **SIGN UP**.

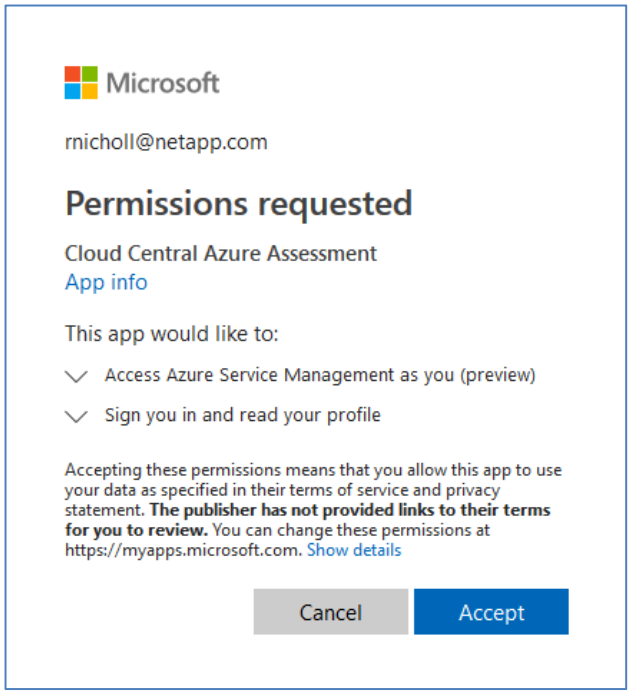
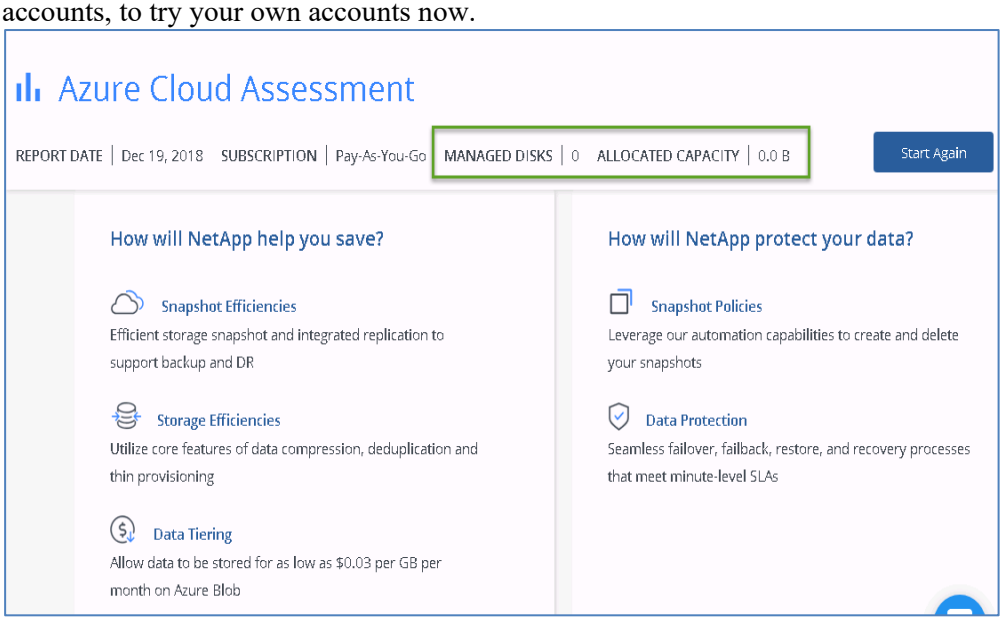
Step	Action
1-5	On the top of the window, click **ASSESSMENTS**. 
1-6	Click the AWS icon. 

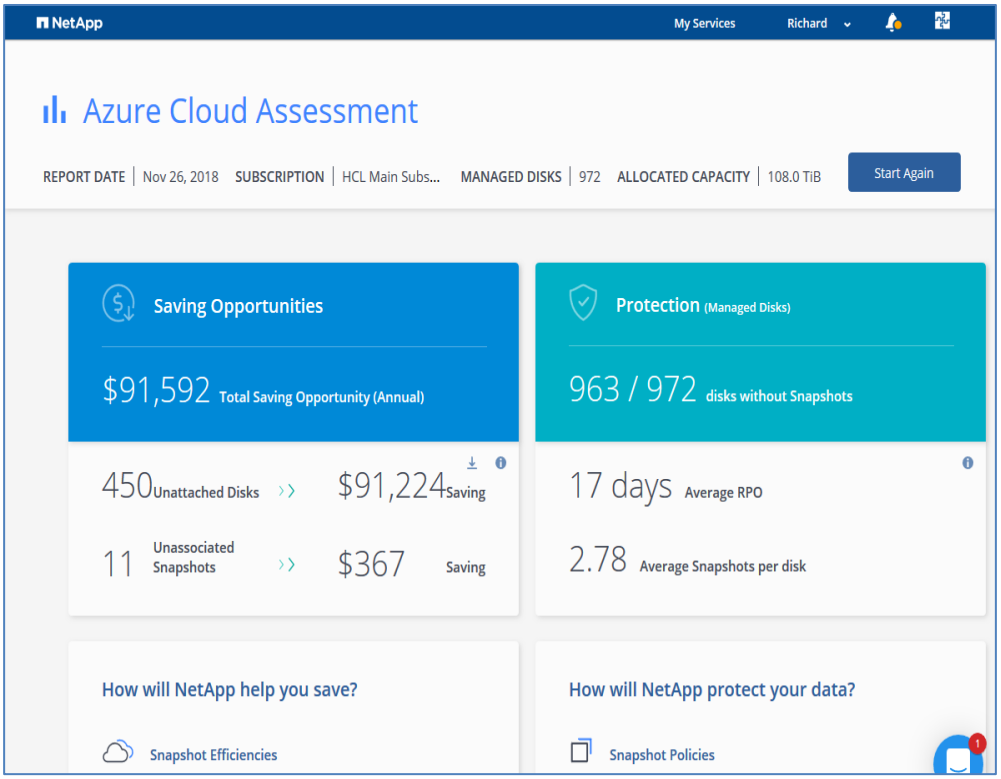
Step	Action
1-7	Enter the Access Key and Secret Key from the awslogin.txt file on your jump host desktop. 
1-8	Click **Start Cloud Assessment**.
1-9	This report comes back empty because there are no resources yet in your AWS account. You should either retry at the end of class or, if you have your own AWS accounts, to try your own accounts now. 

Step	Action
1-10	Following is what the report would look like with an AWS account with many active resources. 

Step	Action
1-11	If you have your own AWS account, in the Saving Opportunities section, you can click the download arrow to get a detailed report of Unattached EBS volumes and Unassociated EBS Snapshots.  Note, a concatenated example report, NetApp AWS Cloud Assessment - Unassociated EBS Snapshots.csv, is in the CourseFiles folder. This report was run on a system that had only unassociated EBS snapshots. To view this file with an appropriate editor, you can either copy it to your laptop and view with Excel or search online for a .csv viewer.

Step	Action
1-12	In the Protection Risks, review your average recovery point objective (RPO) and click the info icon to get an explanation of this calculation. 
1-13	Click the back arrow to return to the top-level Cloud Assessment page and click the Microsoft Azure icon.
1-14	Click **Login with Azure**. 

Step	Action
1-15	If you have signed out, you will be queried to log in with the Azure account. Remember that your username is in the azurelogin.txt.
1-16	Click **Accept**. 
1-17	Select your subscription, and then click **Start Cloud Assessment**.
1-18	This report comes back empty, because there are no resources yet in our Azure account. You should either retry at the end of class or, if you have your own Azure accounts, to try your own accounts now. 

Step	Action
1-19	Following is what the report would look like with an Azure account with many active resources: 
1-20	Note, a concatenated example report, NetApp Azure Cloud Assessment - Unassociated Snapshots.csv, is in the CourseFiles folder. This report was run on a system that had only unattached disks. To view this file with an appropriate editor, you can either copy it to your laptop and view with Excel or search online for a .csv viewer.

End of Exercise

Module 2: Amazon Web Services Virtual Private Cloud and Connectivity to Other Networks

Exercise 1: Configure Amazon Web Services Virtual Private Cloud Resources

In this exercise, you create an Amazon Web Services (AWS) Virtual Private Cloud (VPC) and configure the resources that it requires, including subnets, internet gateways, and network address translation (NAT) gateways. You configure security groups and routes to provide necessary security and access controls. You also verify connectivity between subnets.

Objectives

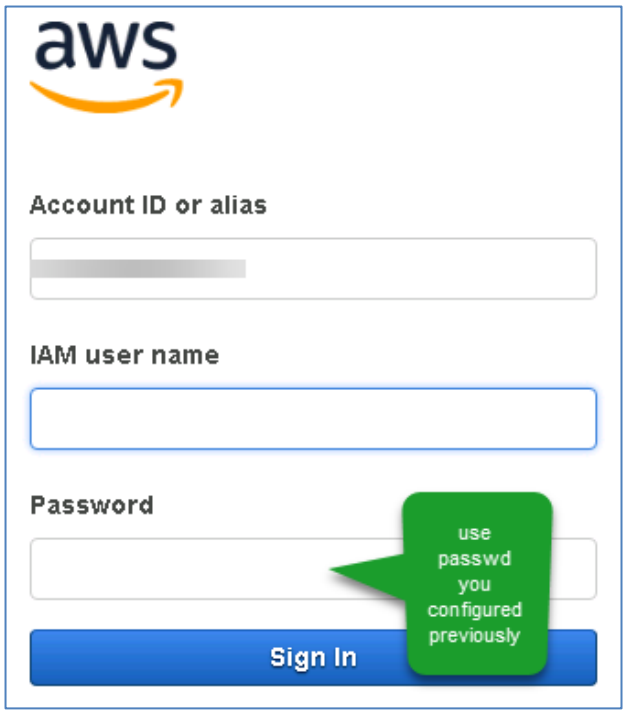
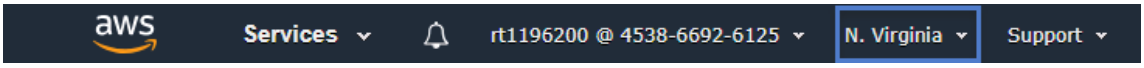
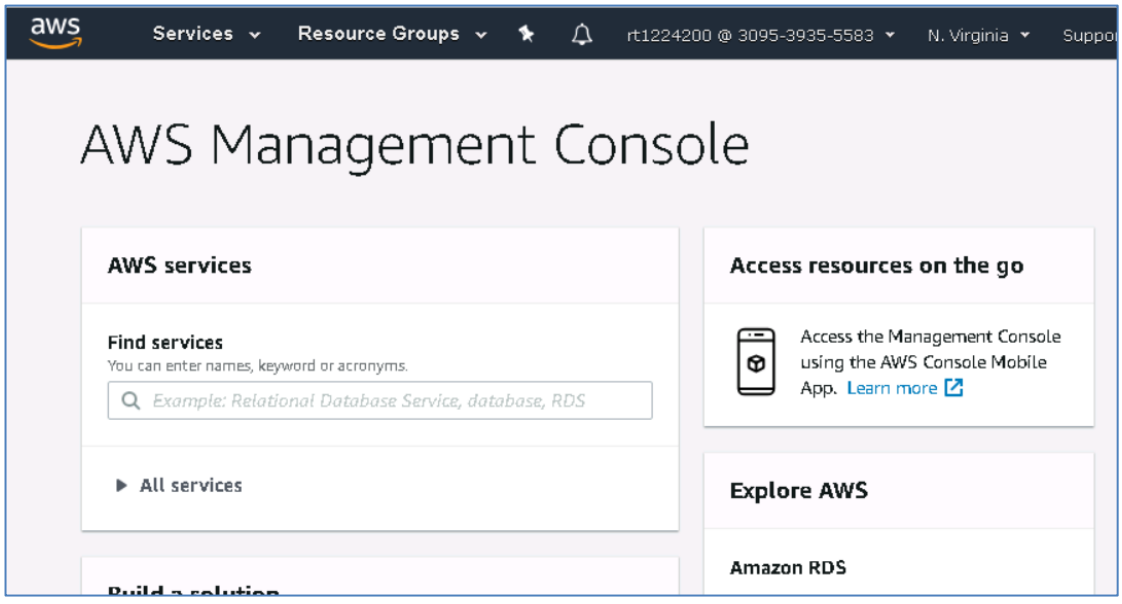
This exercise focuses on enabling you to do the following:

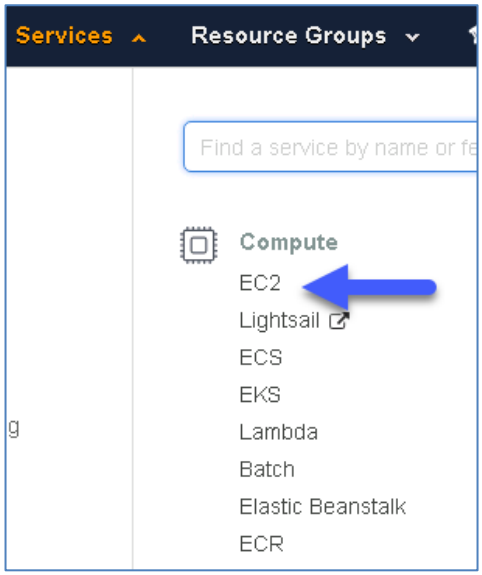
- Create an AWS VPC and associated subnets, internet gateways, and NAT gateway
- Provide security, routes, and access controls for the VPC
- Launch virtual machines VMs in private and public subnets and verify access between subnets

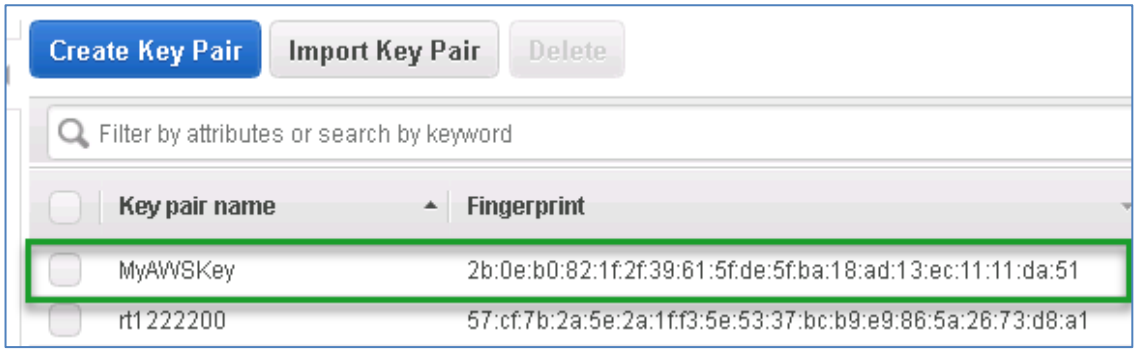
Task 1: Create a Key Pair for Use by CloudFormation Stack

The CloudFormation stack that you create in the next task needs a key pair to create Amazon Elastic Compute Cloud (Amazon EC2) instances. You create the key pair by using AWS Console in this task and pass it as a parameter to the CloudFormation stack.

Step	Action
1-1	If you have logged out of the AWS management console, double click the AWS Console icon on the jump host desktop. 

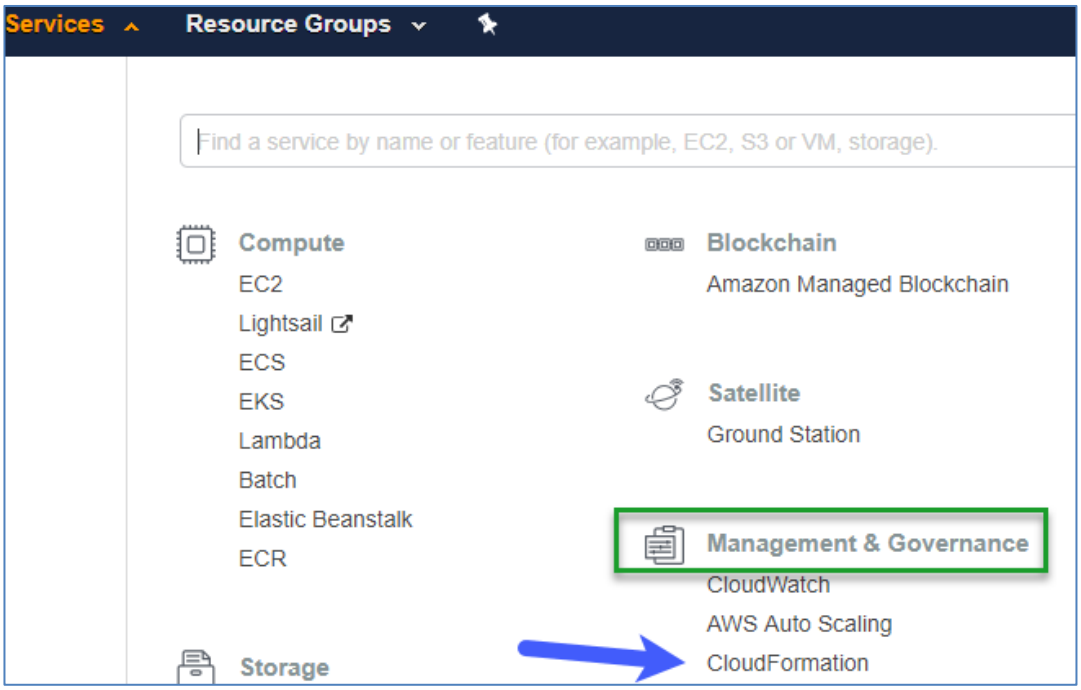
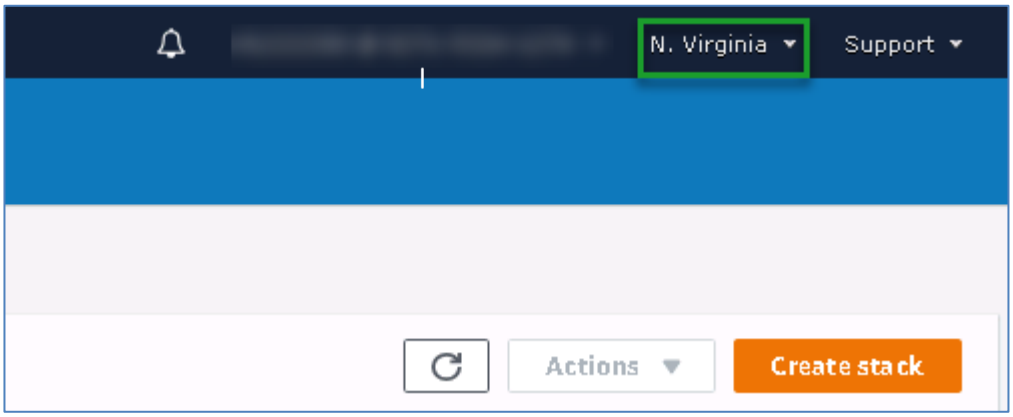
Step	Action
1-2	
1-3	Verify that you are in the N. Virginia region. If you are not in N. Virginia, select that region in the list. The NetApp University labs are in the same region, so making this selection decreases latency. 
1-4	Verify that the Console home page appears. 

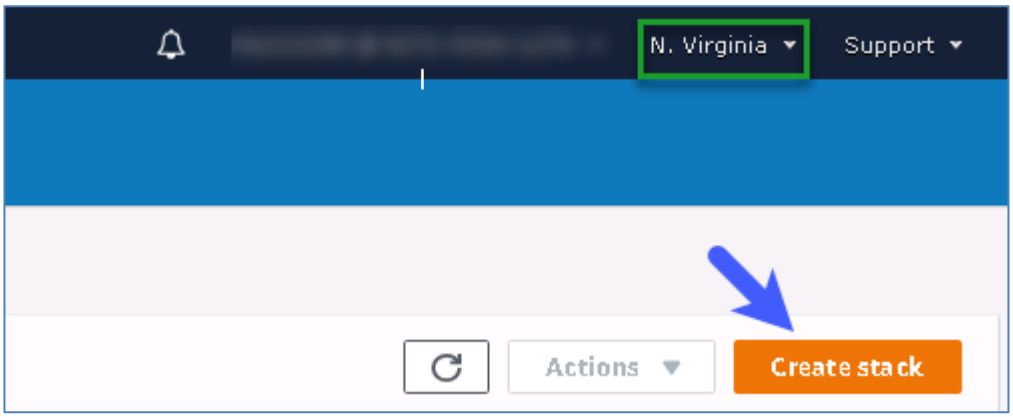
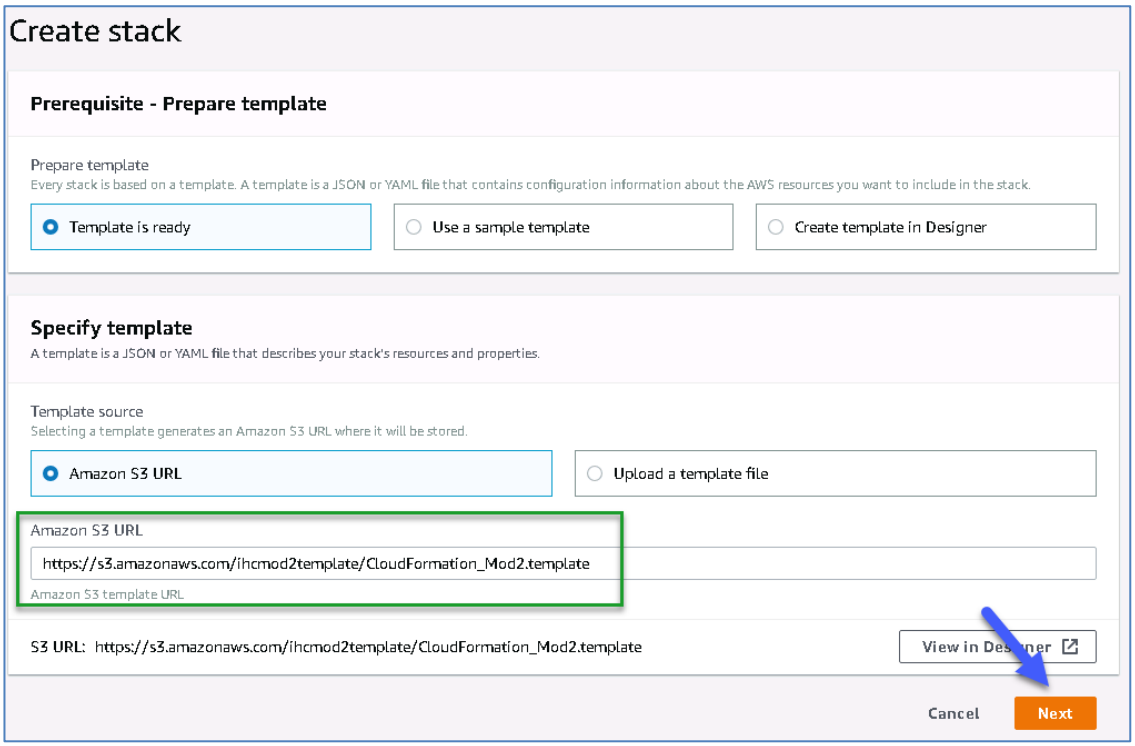
Step	Action
1-5	Select **Services** > **EC2**. 
1-6	You can start to type the name of the service, and it appears. After you have used a service, it appears on the History menu as well.
1-7	In the EC2 dashboard, select **Key Pairs**. 
1-8	Click **Create Key Pair.**
1-9	In the Create Key Pair dialog box, enter the Key Pair Name **MyAWSKey**, and then click **Create**.

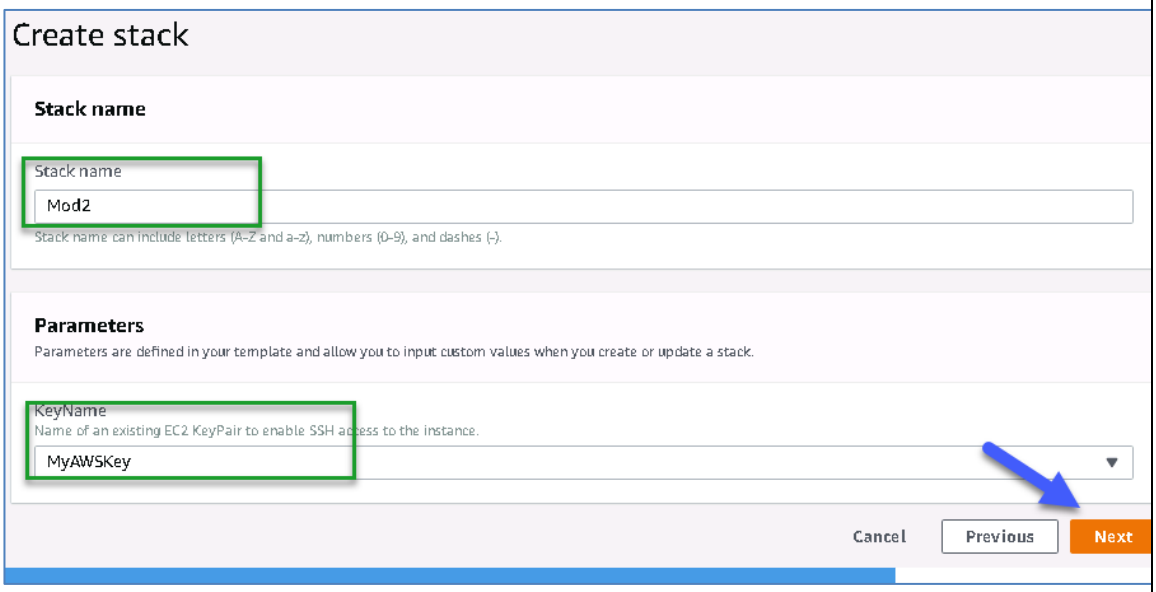
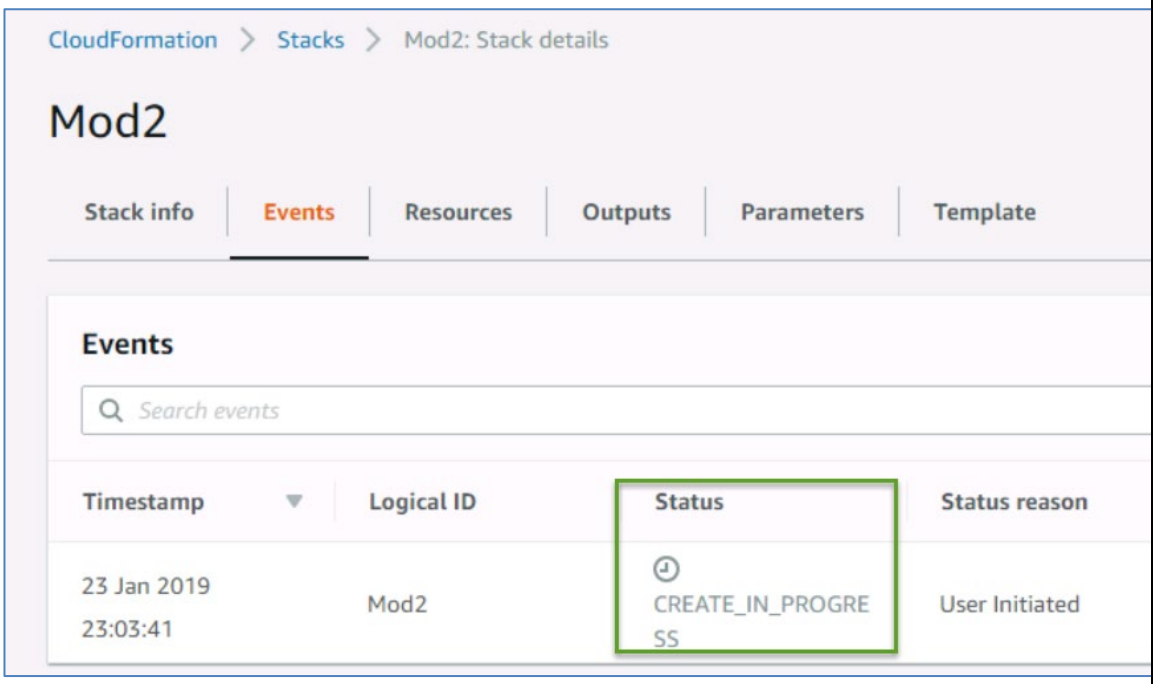
Step	Action
1-10	Verify that a Key Pair with the name **MyAWSKey** is created. 
1-11	The file MyAWSKey is automatically downloaded and is in your Downloads directory
1-12	Move the MyAWSKey.pem file from the Downloads folder to the CourseFiles folder.

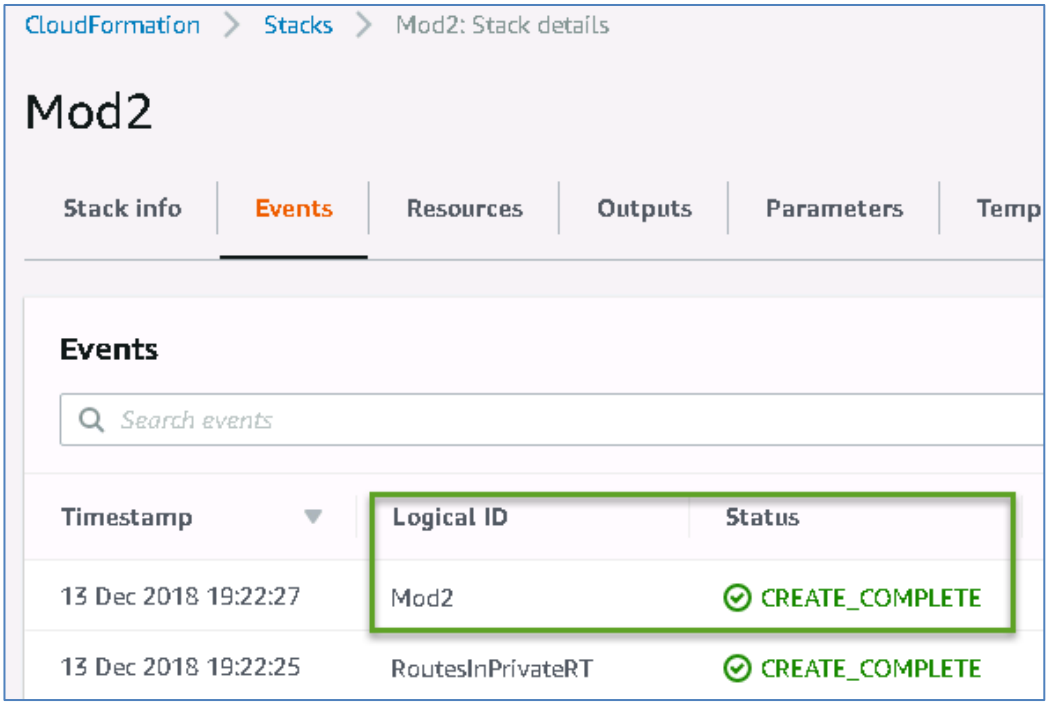
Task 2: Use a CloudFormation Template to Create a CloudFormation Stack

Use a CloudFormation template that is provided to create a CloudFormation stack. This stack runs and creates a VPC with public and private subnets, an internet gateway, a NAT gateway, and Amazon EC2 instances. All required route tables with appropriate route entries and security groups are also created.

Step	Action
2-1	Select **Services** > **CloudFormation**. 
2-2	If you see the following message, click **Try it out now**. 
2-3	Verify you are still in the N.Virginia region. 

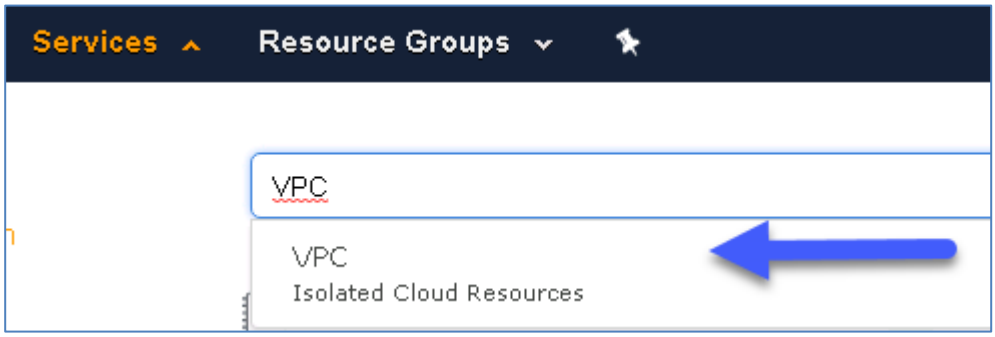
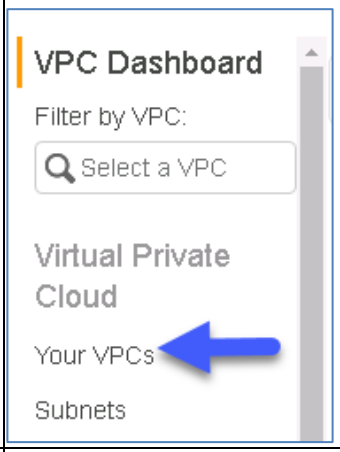
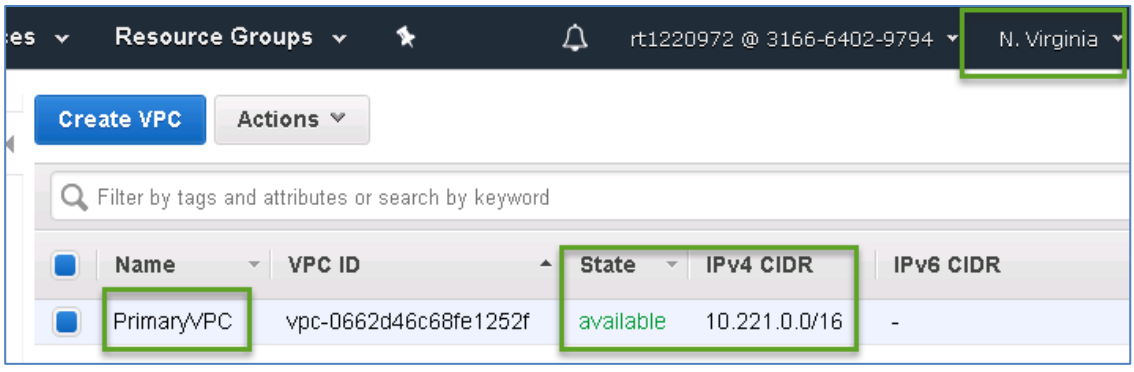
Step	Action
2-4	CloudFormation stack creates resources in the region in which it runs. Because you need all your resources for this class to be in the N.Virginia region, you create the stack in the N.Virginia region.
2-5	Click **Create stack**. 
2-6	In the Specify template section, enter the following URL, and then click **Next.** Amazon S3 URL: **https://s3.amazonaws.com/ihcmod2template/CloudFormation_Mod2.template** 
2-7	To create a CloudFormation stack, a CloudFormation template must be uploaded to an Amazon Simple Storage Service (Amazon S3 or S3) bucket. The template that is required to create a stack for this exercise is already uploaded to the URL that was mentioned in the previous step.

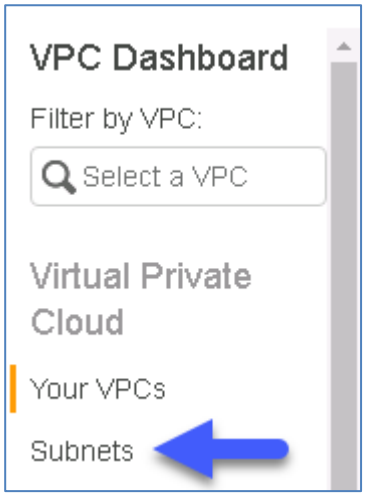
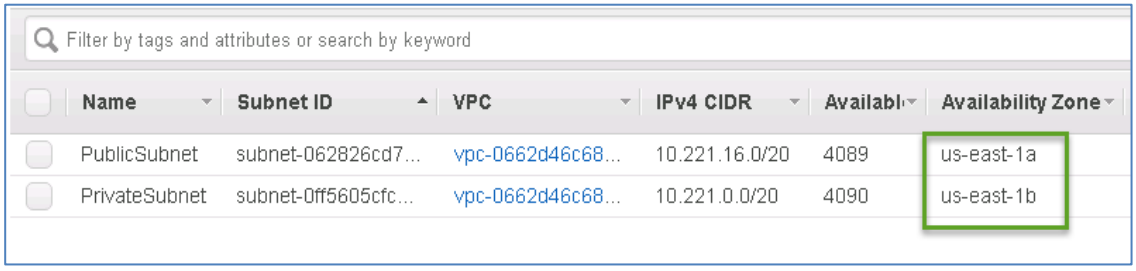
Step	Action
2-8	In the Create stack page, enter the following information, and click **Next**. • Stack Name: **Mod2** • KeyName: Select **MyAWSKey** from the list. 
2-9	In the Configure stack options page, accept the defaults, and click **Next**.
2-10	In the Review Mod2 page, review your information, scroll to the bottom, and then click **Create Stack**.
2-11	Verify that the status is CREATE_IN_PROGRESS. 

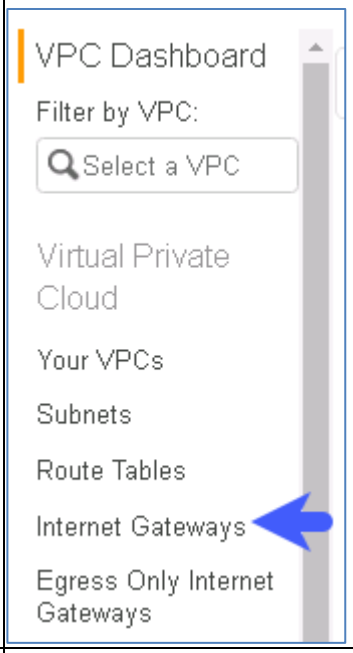
Step	Action
2-12	The stack starts running to create the resources that are specified in the template. When the stack finishes running, the status is CREATE_COMPLETE. This process should take no more than 3-5 minutes. Afterward, you review all the resources that are created.
2-13	Click the Refresh button until the status for Mod2 becomes **CREATE_COMPLETE**. 

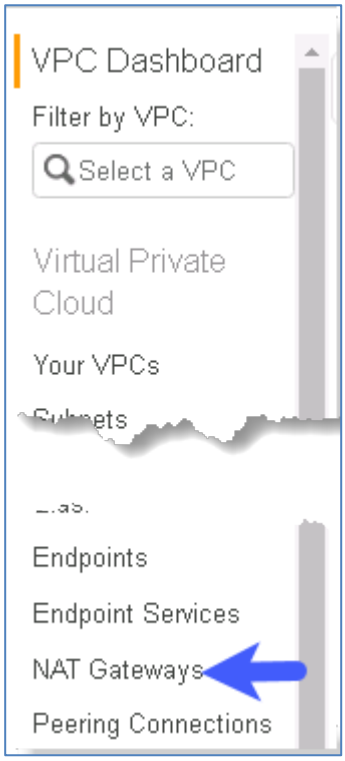
Task 3: Review VPC, Subnets, Internet Gateway, and NAT Gateway

In this task, you review some of the key objects and settings that are created by the CloudFormation stack.

Step	Action
3-1	Click **Services**, enter VPC in the search box, and when it appears, select **VPC**. 
3-2	In the VPC Dashboard, click **Your VPCs**. 
3-3	Verify that you see the following for the VPC that is created: • Name: PrimaryVPC • State: available • IPv4 CIDR: 10.221.0.0/16 • Region: N.Virginia 

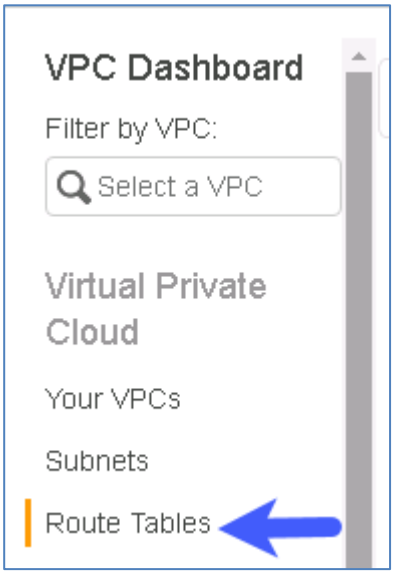
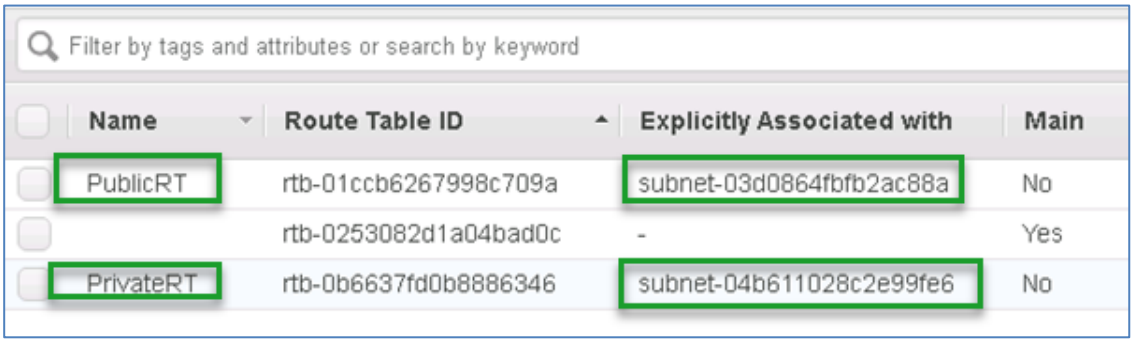
Step	Action
3-4	In the VPC Dashboard menu, click **Subnets**. 
3-5	Verify that you see two subnets and verify that the Availability Zones are unique between the two subnets: Names: PublicSubnet and PrivateSubnet IPv4 CIDR: 10.221.16.0/20 for PublicSubnet and 10.221.0.0/20 for PrivateSubnet 

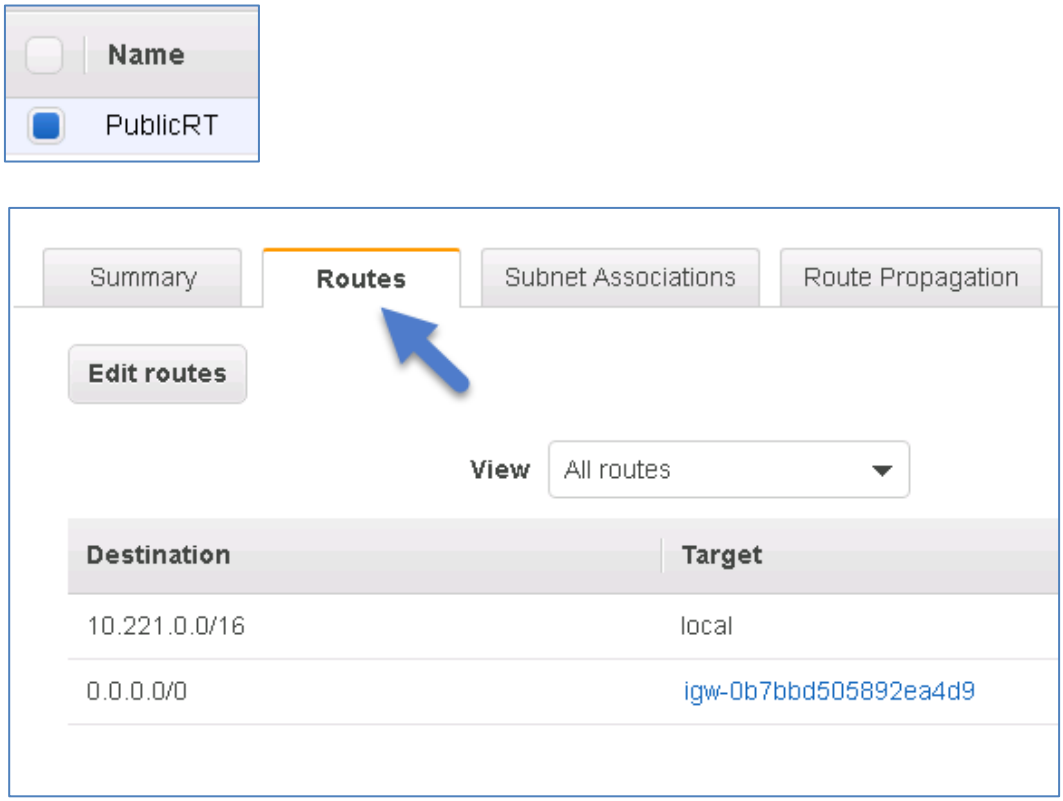
Step	Action
3-6	In the VPC Dashboard menu, click **Internet Gateways**. 
3-7	Verify that you see an IGW attached to the PrimaryVPC. 

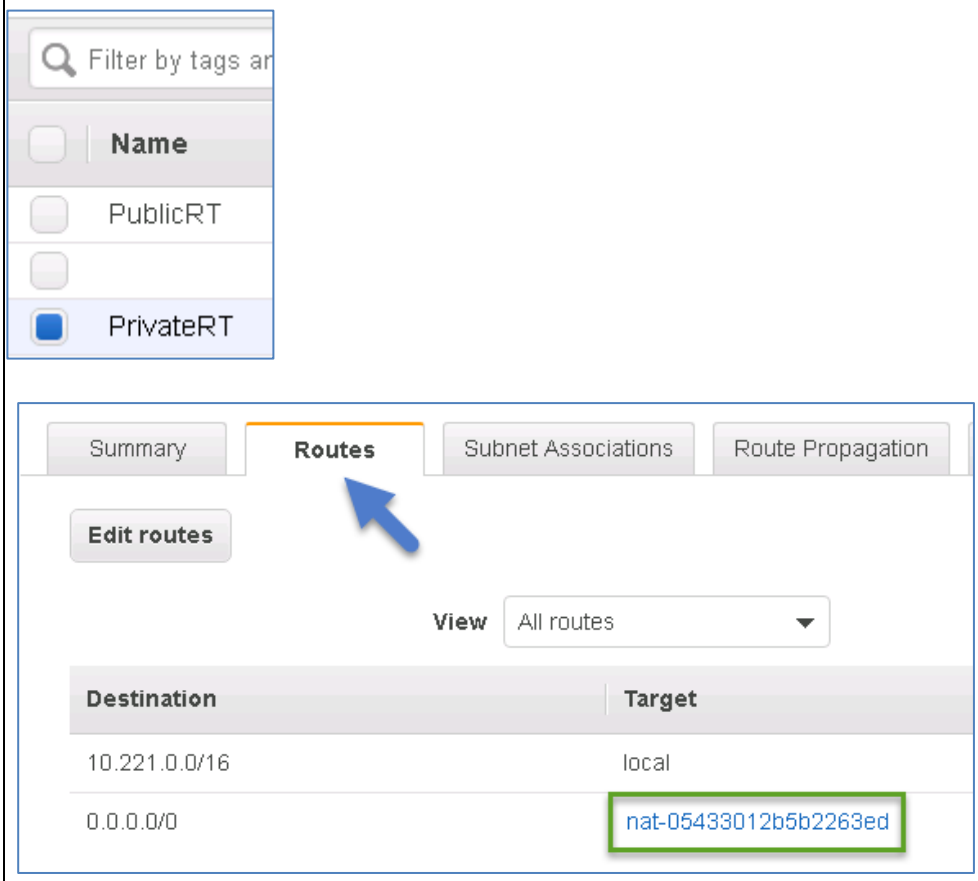
Step	Action
3-8	Click **NAT Gateways** 
3-9	Verify that you see a NAT gateway that is created in the public subnet. 
3-10	The NAT gateway has a public IP (elastic IP address) that is externally available and a private IP address. It is created in the public subnet so that traffic from the private subnet can be routed to the internet by using this address.

Task 4: Review Route Tables and Routes

In this task, you review the new route tables that are created and associated with the subnets. You also review the routes in each route table.

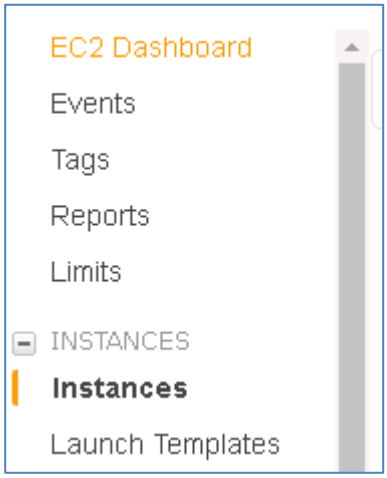
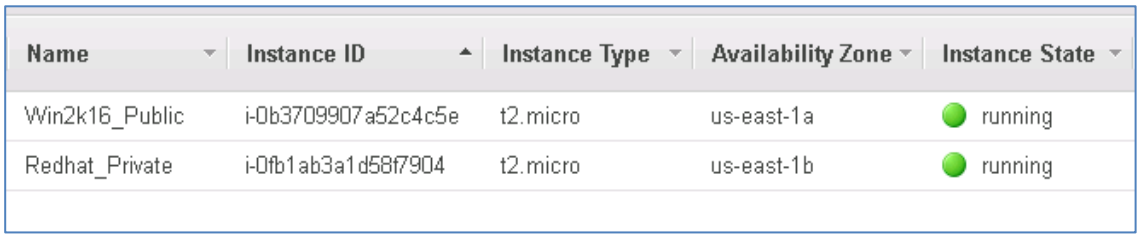
Step	Action
4-1	In the VPC Dashboard, click **Route Tables**. 
4-2	Verify that you see a PublicRT and PrivateRT and that they are explicitly associated with subnets. (You can check the subnets to which they are associated in a later step.) 

Step	Action
4-3	Select **PublicRT** and review the routes that are in the Routes tab. 
4-4	The first route entry routes traffic locally within the VPC between subnets. The second entry routes all other traffic for external destinations to the internet through the internet gateway.
4-5	Review the Subnet Associations for the PublicRT. 
4-6	This route table is explicitly associated with the public subnet to route traffic locally and to the internet

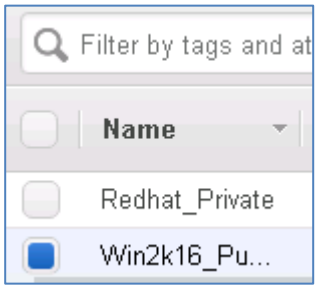
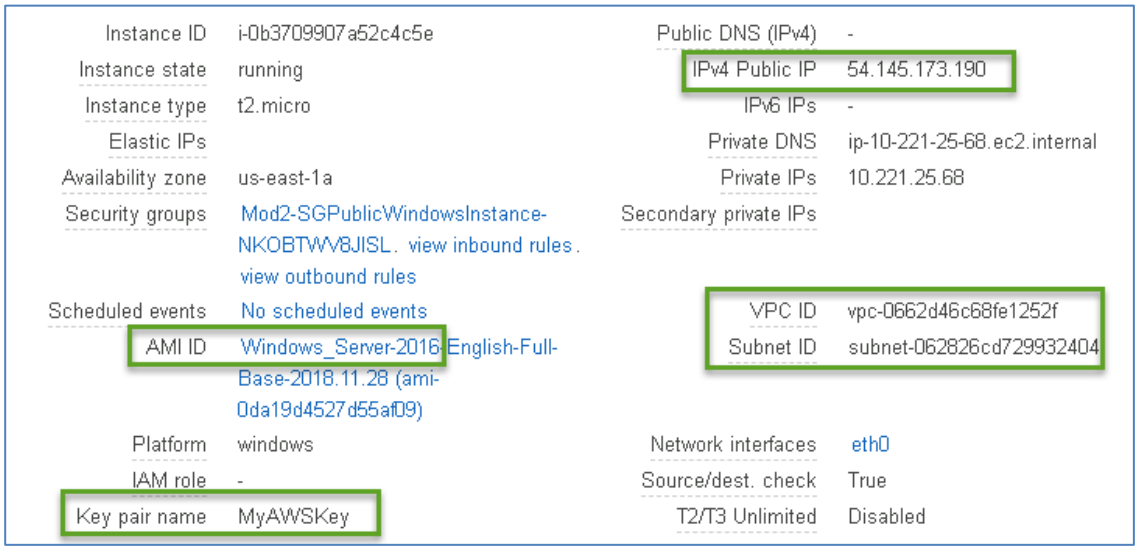
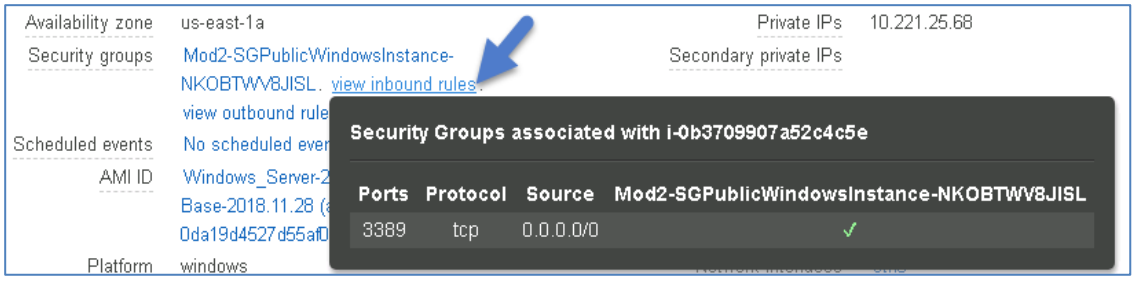
Step	Action
4-7	Select **PrivateRT** and review the routes in the bottom portion of the window. 
4-8	The first route entry routes traffic locally within the VPC between subnets. The second entry routes to all external destinations through the NAT gateway.
4-9	Review the Subnet Associations for the PublicRT. 
4-10	This route table is explicitly associated with the private subnet to route traffic locally and outbound to the internet through the NAT gateway.

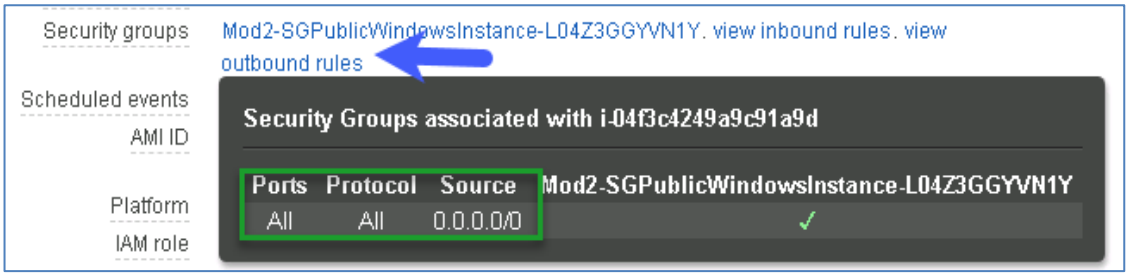
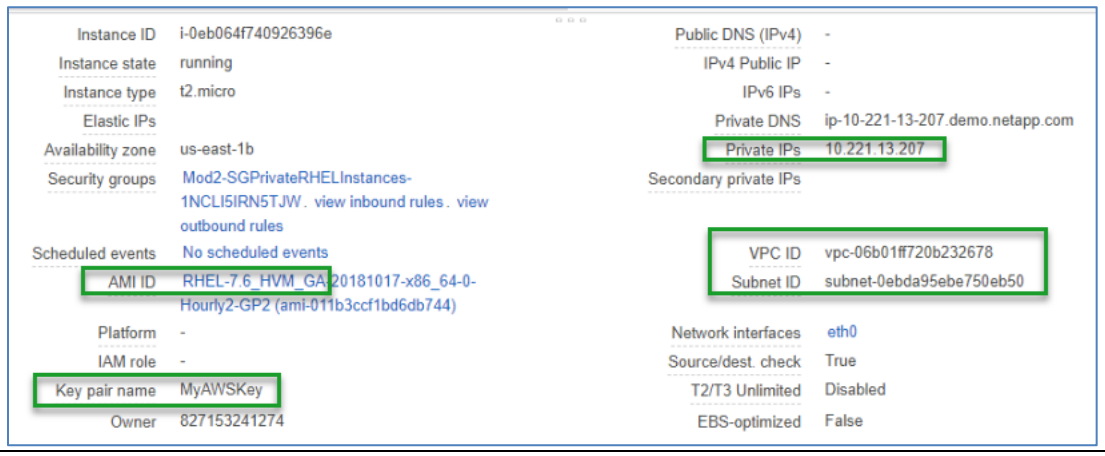
Task 5: Review Public and Private Amazon EC2 Instances That Are Created and the Security Groups with Which They Are Associated

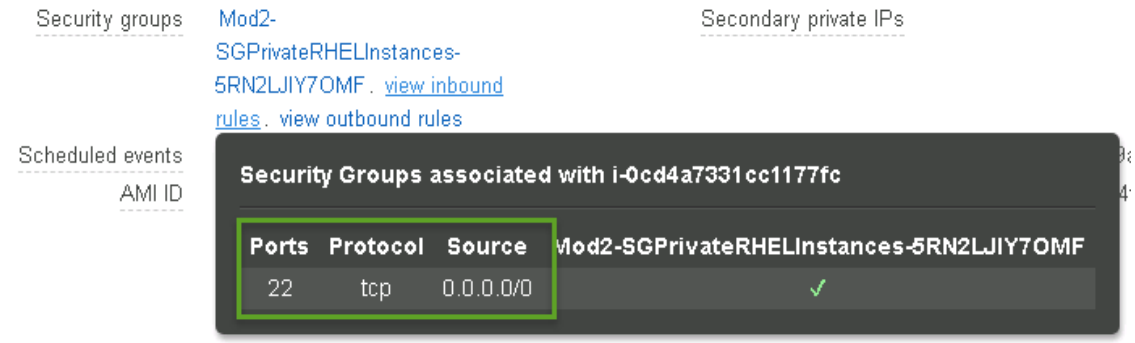
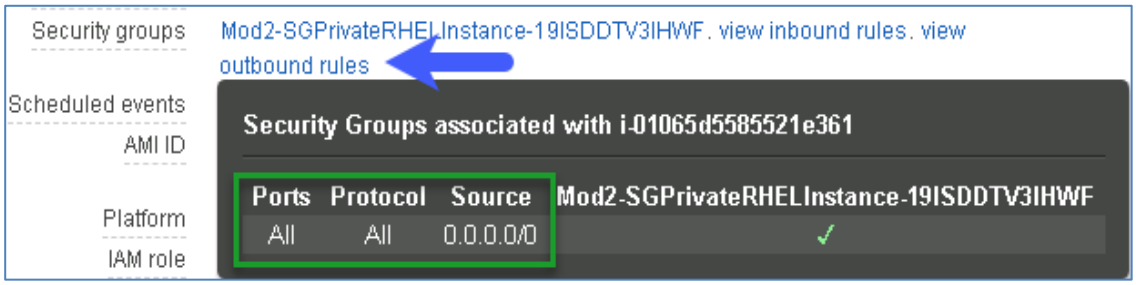
In this task, you review the Windows and the Linux Amazon EC2 instances that are created and the security groups with which they are associated.

Step	Action
5-1	Select **Services > EC2**. 
5-2	In the EC2 Dashboard, click **Instances**. 
5-3	Verify that you see the following instances and that the Instance State is running. 

Name	Instance ID	Instance Type	Availability Zone	Instance State
Win2k16_Public	i-0b3709907a52c4c5e	t2.micro	us-east-1a	running
Redhat_Private	i-0fb1ab3a1d58f7904	t2.micro	us-east-1b	running

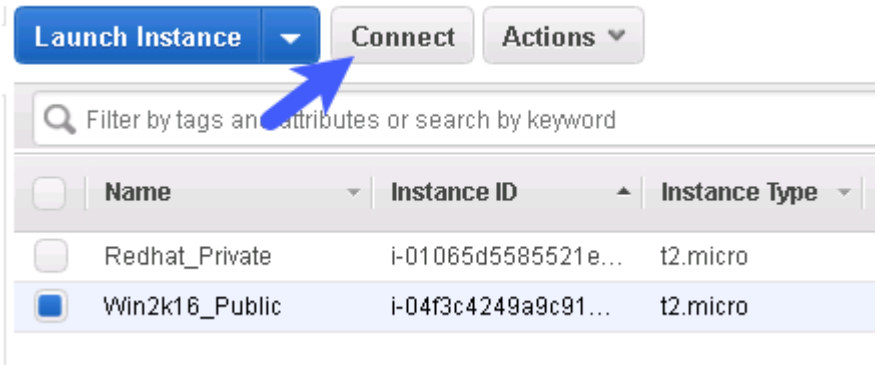
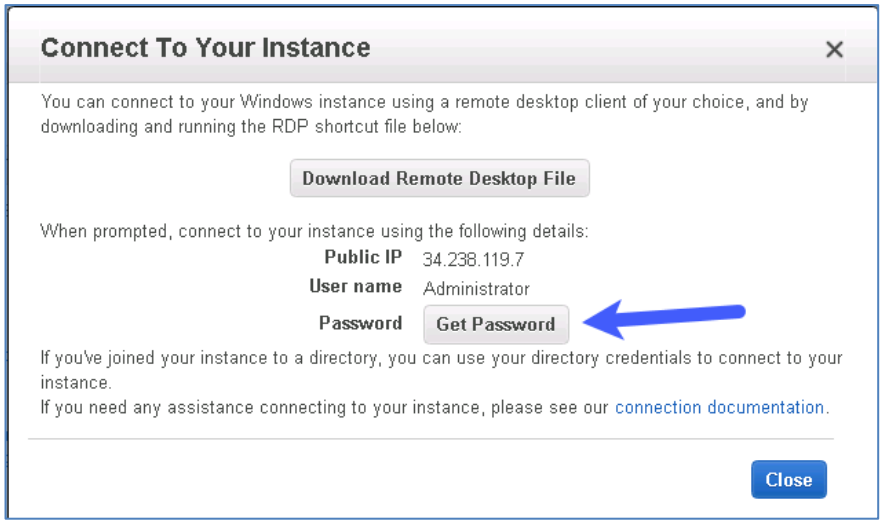
Step	Action
5-4	Select **Win2k16_Public**, and review the details in the bottom of the window: a. Verify that the instance is running the AMI Windows_Server-2016. b. Verify that VPC is PrimaryVPC and the subnet is Public Subnet by matching the IDs in the VPC Dashboard. c. Verify that the instance has a public IP. (The Public IP that you see might be different from what you see in the example.) d. Verify that the instance was deployed with the key pair MyAWSKey.pem  
5-5	Click **view inbound rules** of the security group. 

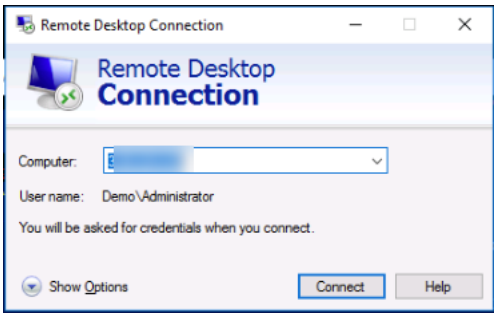
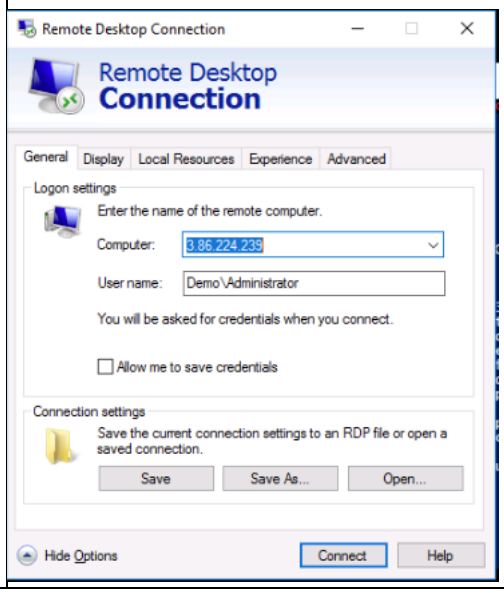
Step	Action
5-6	Click **view outbound rules** of the security group. 
5-7	The security groups act as a firewall for the instances that are associated with them. The security group that is shown here allows incoming Remote Desktop Protocol (RDP) traffic on port 3389 from any source to the Windows instance. You use RDP to log in to this instance in the next task. In the outbound direction from the Amazon EC2 instance, the security group allows all protocol traffic.
5-8	Select Redhat_Private, and review the details in the bottom of the window: a. Verify that the instance is running the AMI RHEL-7.6_HVM*. b. Verify that VPC is PrimaryVPC and the subnet is PrivateSubnet by matching the IDs in the VPC Dashboard. There is no Public IP. c. Make a note of the following information: Private IP:_____ d. Verify that the instance was deployed with the key pair MyAWSKey.pem  

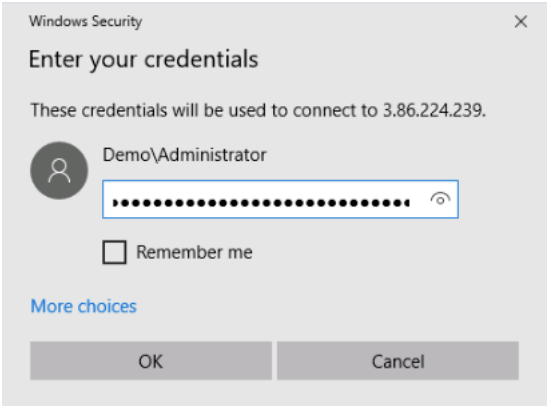
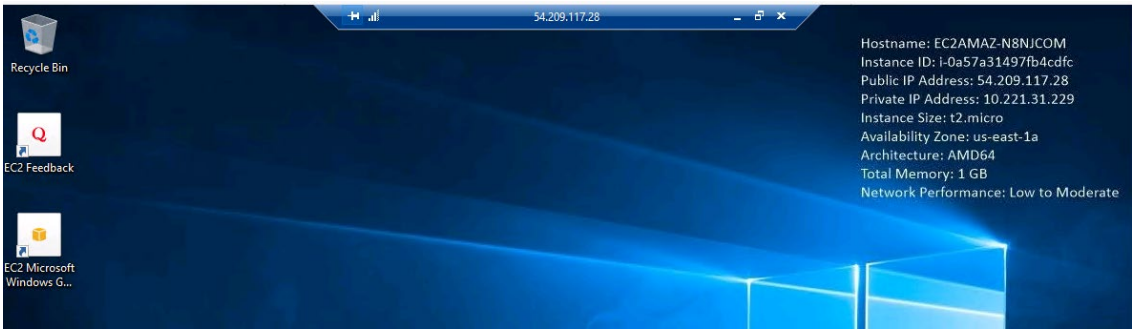
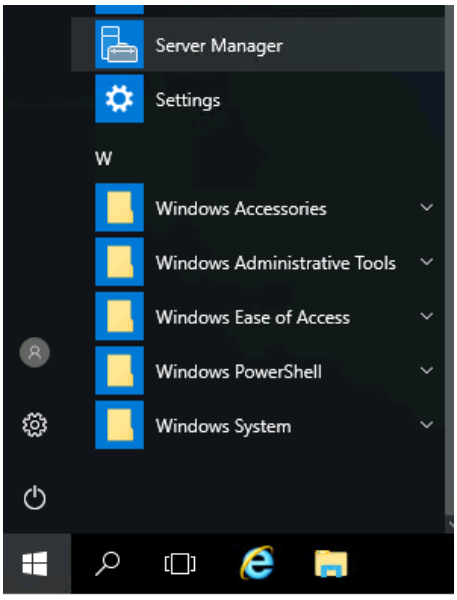
Step	Action
5-9	Click the **view inbound rules** of the security group. 
5-10	Click the **view outbound rules** of the security group. 
5-11	The security group that is shown here allows incoming Secure Shell (SSH) traffic on port 22 from any source to the Red Hat Enterprise Linux instance. You use SSH to log in to this instance in the next task. In the outbound direction from the Amazon EC2 instance, the security group allows all protocol traffic.

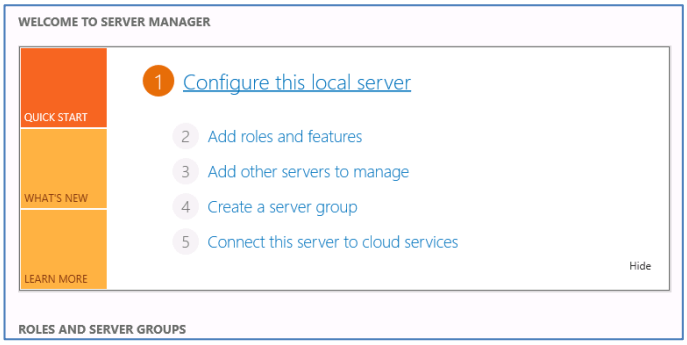
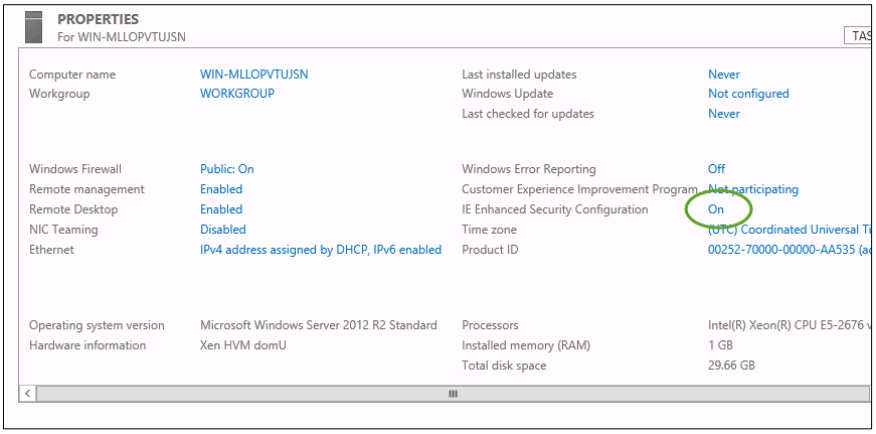
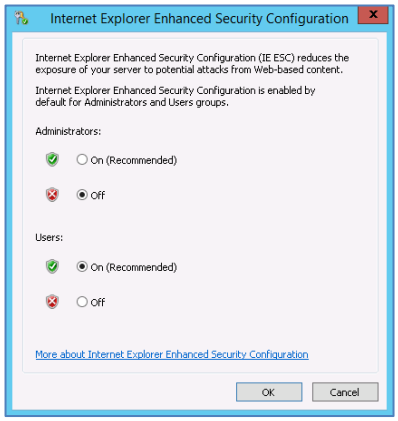
Task 6: Log In to the Windows Server Amazon EC2 Instances in Public Subnet

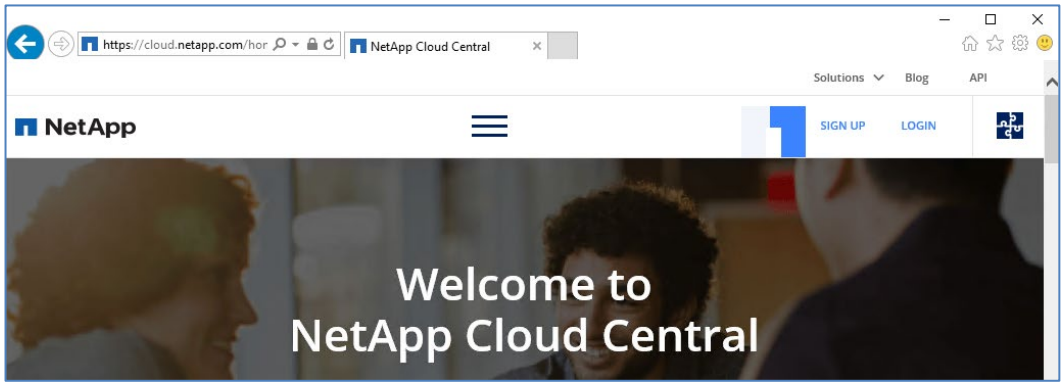
In this task, you connect to the Windows instance in the public subnet through RDP and verify access to the internet from this instance.

Step	Action
6-1	On the Instances dashboard, complete the following actions: a. Select the **Win2k16_Public** instance. b. Click **Connect**. 
6-2	In the Connect To Your Instance window, click **Get Password**. 
6-3	In the **Connect To Your Instance > Get Password** window, next to Key Pair Path, click **Choose File**.
6-4	Select the **MyAWSKey.pem** file that you saved in the CourseFiles folder, and then click **Open**.
6-5	Click **Decrypt Password**.

Step	Action
6-6	Save the following values in a text file called **Public_W2K16_Login.txt** in the CourseFiles folder: Public IP: _____ User name: _____ Password: _____
6-7	Click the Remote Desktop Connection icon on your jump host. 
6-8	In the Computer field, enter the public IP that you recorded in Step 6-6, and then click **Connect**. 
6-9	Click **Show Options.**
6-10	Provide the public IP and the username that you saved earlier in the **Public_W2K16_Login.txt** file and click **Connect.** 

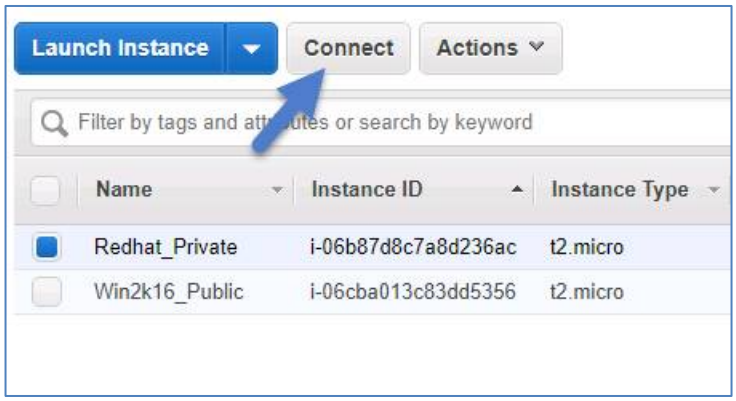
Step	Action
6-11	Provide the password that you saved in the **Public_W2K16_Login.txt** file and click OK. 
6-12	If a "The identity of the remote computer cannot be verified. Do you want to connect anyway?" window appears, click **Yes**.
6-13	Verify that the Windows Server desktop appears. 
6-14	Click the Windows icon, and then select **Server Manager**. 

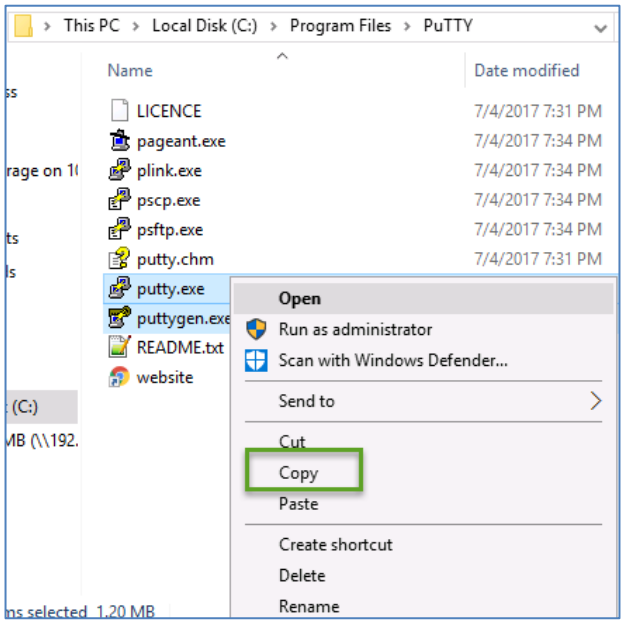
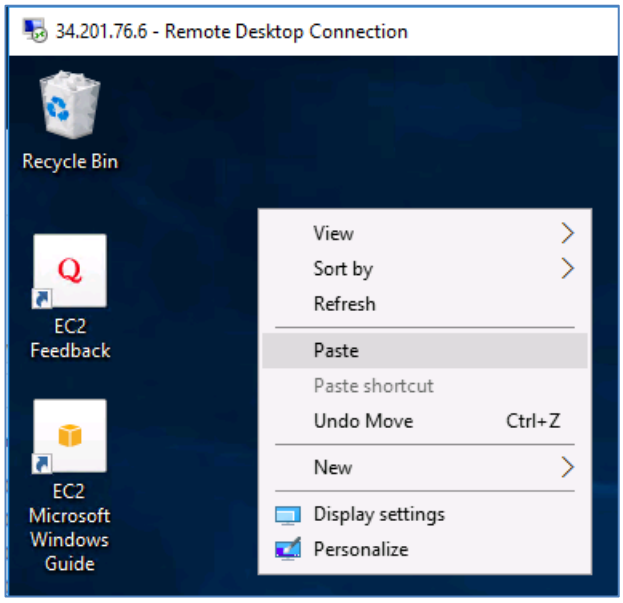
Step	Action
6-15	Click **Configure this local server**. 
6-16	In the Properties section, to the right of IE Enhanced Security Configuration, click **On**. 
6-17	In the Internet Explorer Enhanced Security Configuration window, complete the following actions to turn off Internet Explorer Enhanced Security Confirmation: a. Under Administrators, select **Off**. b. Click **OK**. 

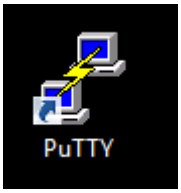
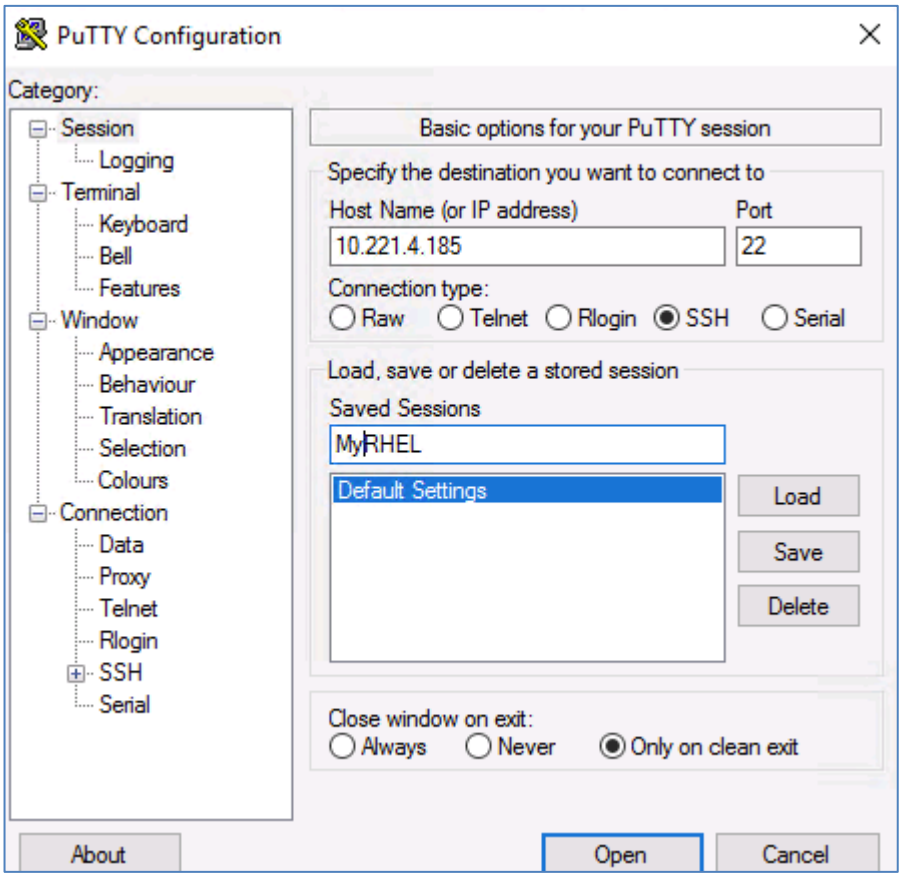
Step	Action
6-18	Click the **Start** menu. 
6-19	Click **Internet Explorer**.
6-20	In Internet Explorer, enter the URL **http://cloud.netapp.com** to verify that this Windows Server, which is in the public subnet, can reach the internet through the internet gateway.
6-21	Verify that the NetApp Cloud Central page appears. 

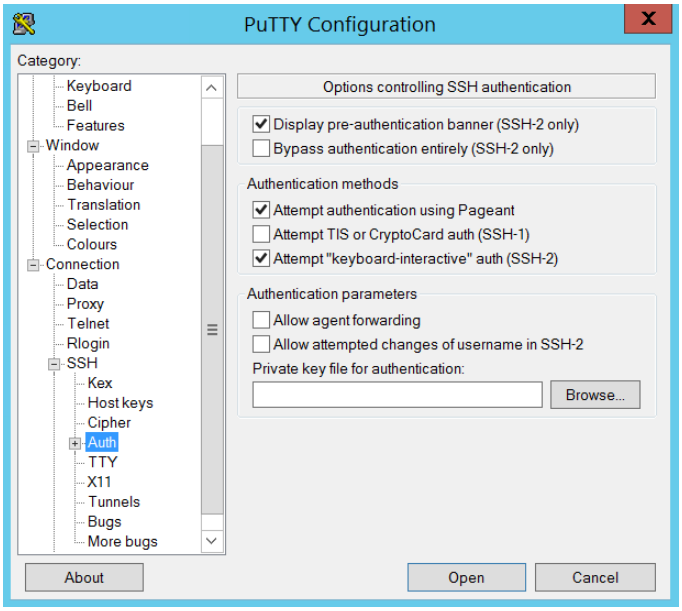
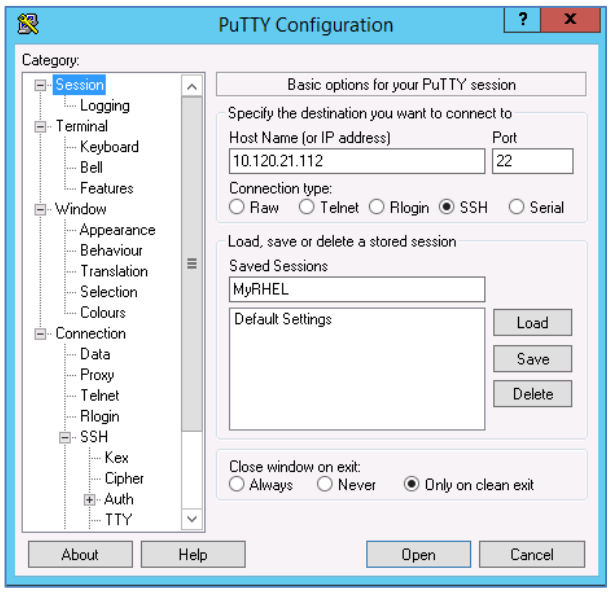
Task 7: Log In to the Linux Server Amazon EC2 Instances in Private Subnet

Use SSH to access the Linux instance from the Windows Server instance and verify access to the internet from this Linux Server instance.

Step	Action
7-1	On the AWS browser, on the Instance dashboard, select the **Redhat_Private** instance, and then click **Connect**. 
7-2	The Linux instance is in a private subnet and does not have an external IP address. Therefore, you need to connect to the Linux instance from the Windows Server instance that you created in the public subnet.
7-3	Use RDP to access your Public_W2K16 server (if you have disconnected from it).

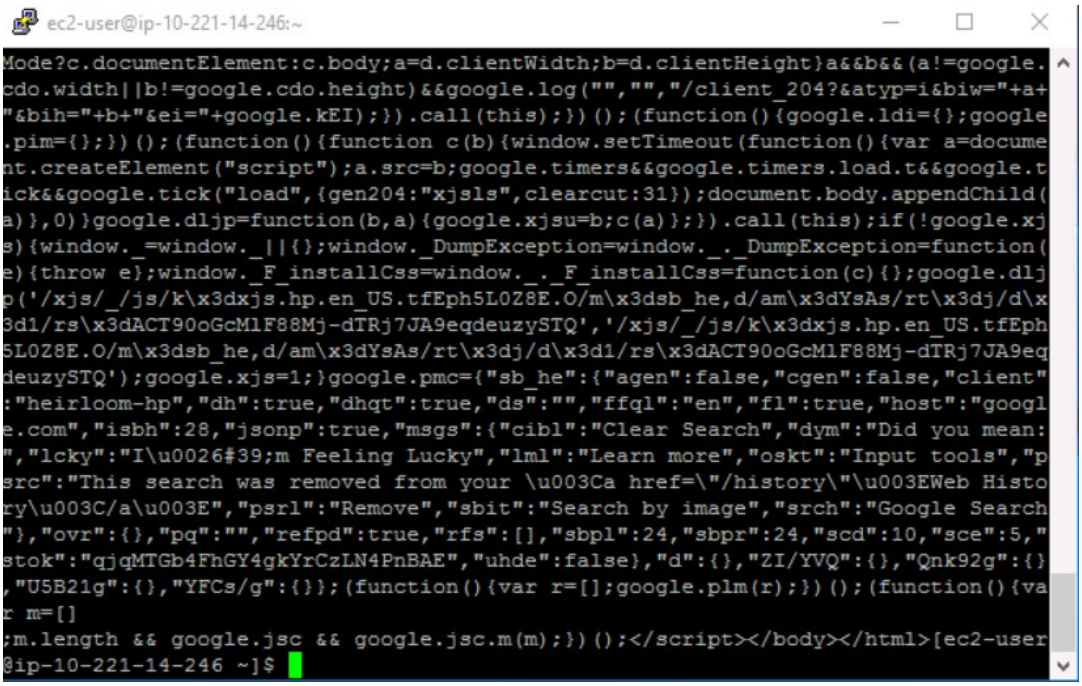
Step	Action
7-4	Copy the putty.exe and puttygen.exe files from your jumphost C:\Program Files\PuTTY to the Public_W2K16 desktop. (Note on the jumphost desktop the putty and puttygen are just links, so you cannot copy directly from the desktop.)  
7-5	Use either RDP copy method or a webmail from the Public_W2K16 server to copy the MyAWSKey.pem file in your jump host CourseFiles folder to your Public_W2K16 server.
7-6	Convert the MyAWSKey.pem file to a MyAWSKey.ppk file, by using the “Converting Your Private Key Using PuTTYgen” instructions that you can find on the following site: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html?icmpid=docs_ec2_console **Note:** You must ensure that your key size is at least 2048 bits when you generate the key.

Step	Action
7-7	Double-click the **PuTTY** icon. 
7-8	Use the following settings: • Host Name: private IP address of the Redhat_Private Record the Private IP address:_____ • Port: 22 • Connection type: **SSH** • Saved Sessions: MyRHEL 
7-9	Click **Save**.

Step	Action
7-10	In the Category Pane, select **Connections** > **SSH** > **Auth**. 
7-11	To the right of the Private key file for authentication box, click **Browse**.
7-12	Select the **MyAWSKey.ppk** file.
7-13	In the Category pane, select **Session**. 
7-14	Click **Save**.
7-15	Click **Open**.
7-16	When the PuTTY Security Alert appears, click **Yes**.

Step	Action
7-17	In the PuTTY shell, log in as **ec2-user**. (No password is requested because you are authenticating with the .pem file in a .ppk format for SSH.)
7-18	Verify that you are logged in to the Linux CLI. 

7-19	In the CLI, verify your path:
	`$ pwd`
	`/home/ec2-user`

7-20	Issue a **curl** command to get the webpage content for the Google website: `$ curl www.google.com` Sample output:  (You should note that the outbound internet traffic is routed through the NAT gateway route in the private route table).

End of Exercise

Module 2: Amazon Web Services Virtual Private Cloud and Connectivity to Other Networks

Exercise 2: Operationalize On-Premises to Cloud Connectivity

In this exercise, you configure a VPN Internet Protocol security (IPsec) connection between Amazon Web Services (AWS) and the on-premises data center. The on-premises data center connection uses a pfSense virtual router. You also extend the corporate Active Directory service to the cloud environment.

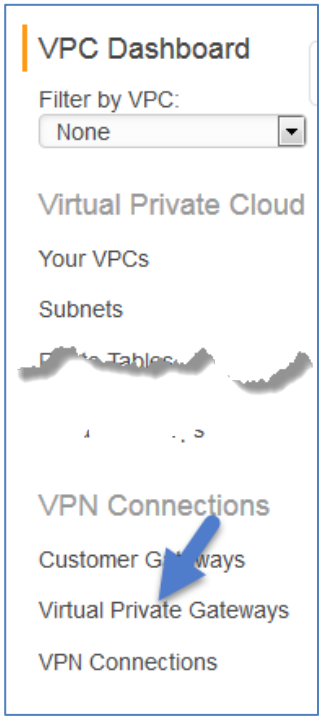
Objectives

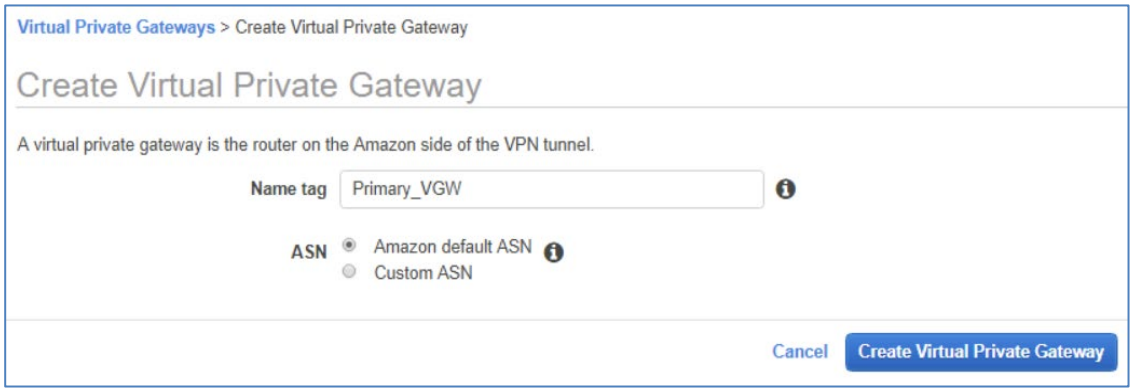
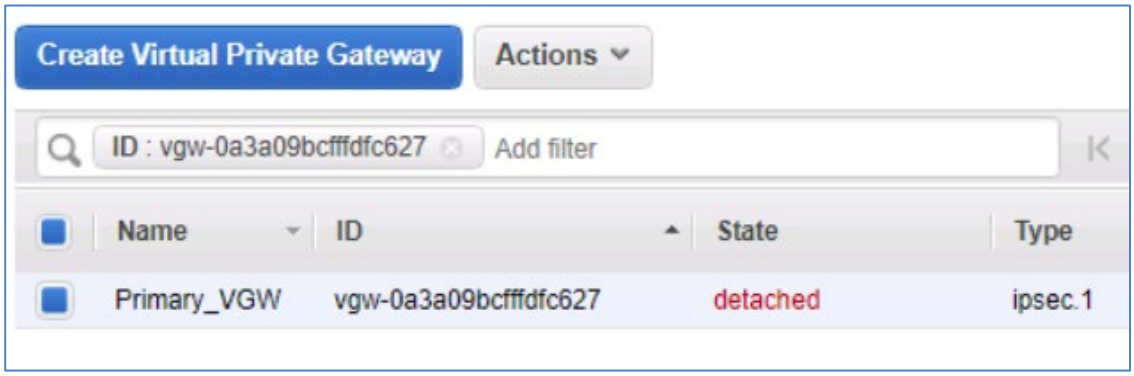
This exercise focuses on enabling you to do the following:

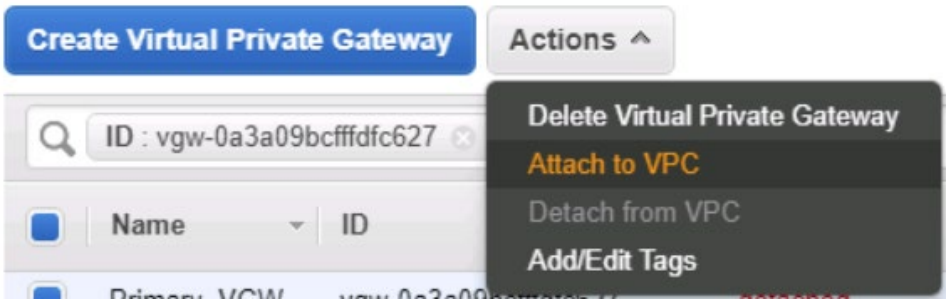
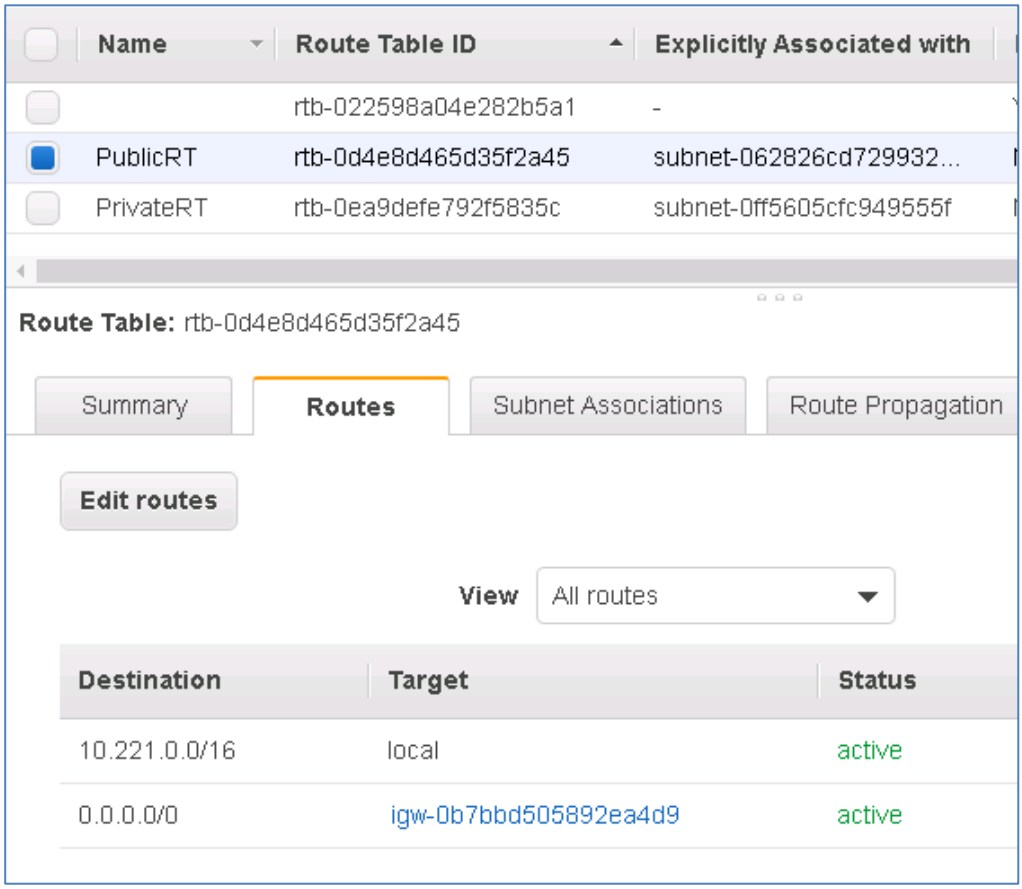
- Create a virtual private gateway for access from your VPC to the private network with the on-premises data center
- Create a customer gateway and establish a VPN IPsec connection to an on-premises data center
- Join an AWS virtual machine to the on-premises Active Directory service

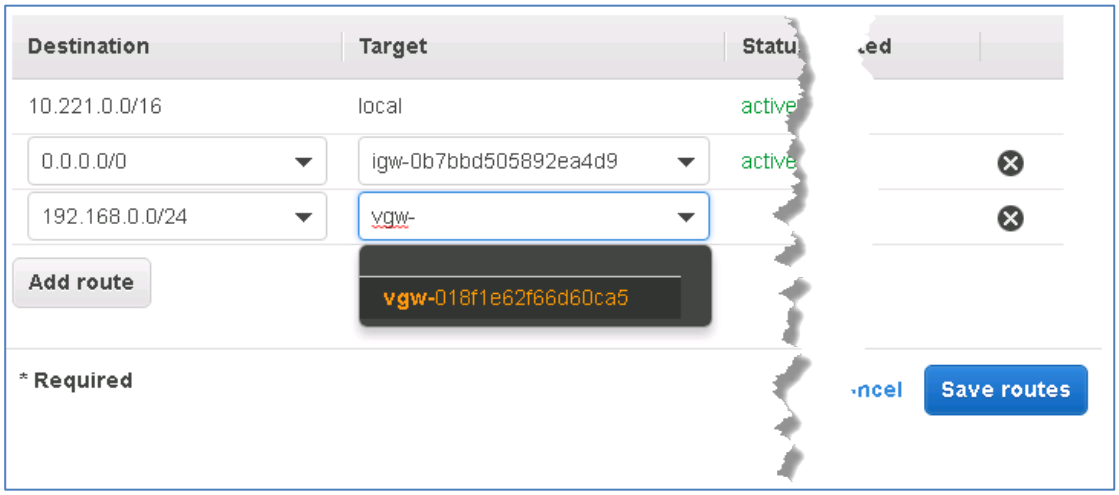
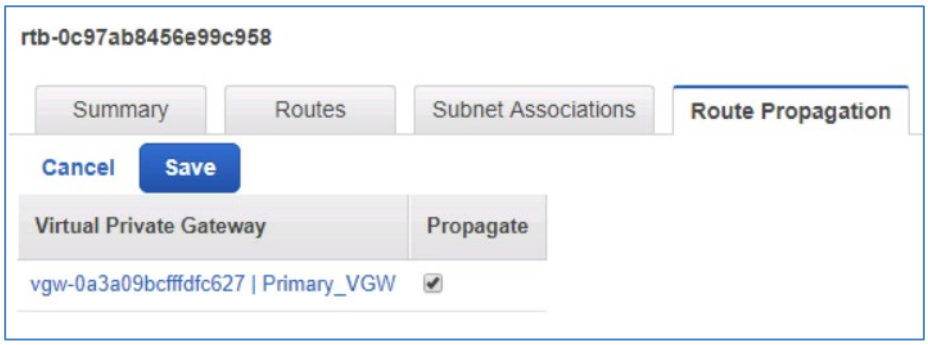
Task 1: Create a Virtual Private Gateway

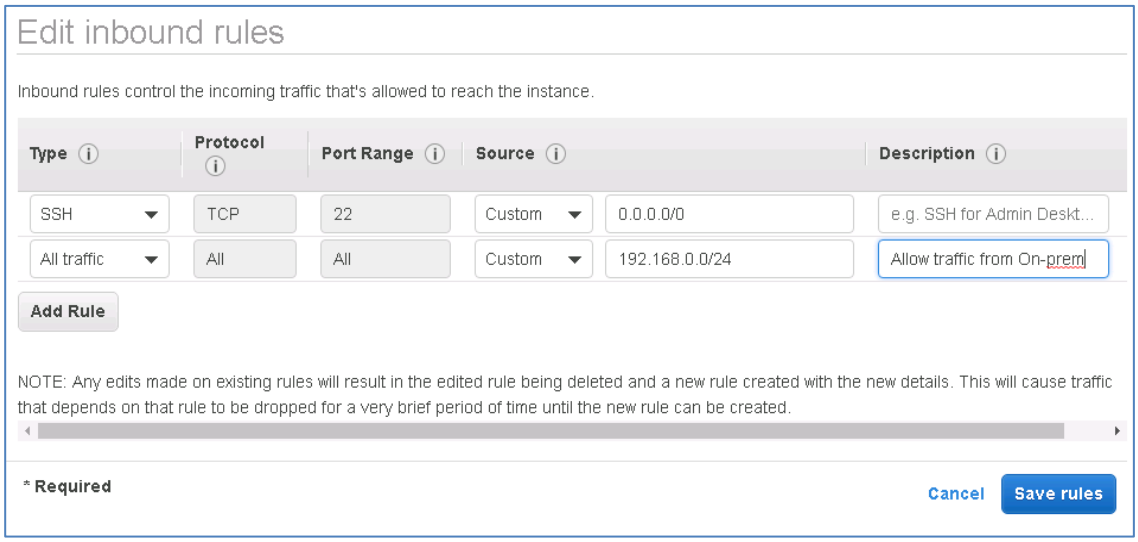
Create a virtual private gateway to use as a route between the VPC and the on-premises data center.

Step	Action
1-1	Select **Services** > **VPC**.
1-2	On the VPC Dashboard, click **Virtual Private Gateways**. 
1-3	Click **Create Virtual Private Gateway**.

Step	Action
1-4	On the Create Virtual Private Gateway window, do the following: a. Enter the name tag **Primary_VGW**. b. For the ASN, select **Amazon default ASN**. c. Click **Create Virtual Private Gateway**. 
1-5	Click the Virtual Private Gateway ID. 
1-6	Verify that the **Primary_VGW** was created and is detached. 

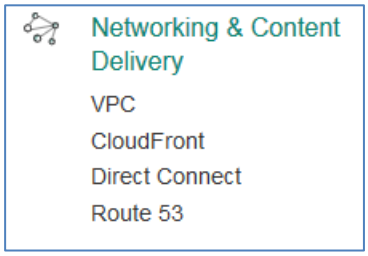
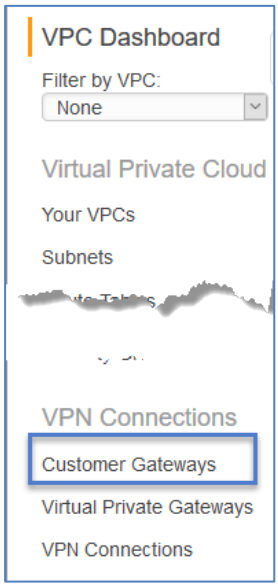
Step	Action
1-7	Select **Primary_VGW**, and then select **Actions** > **Attach to VPC**. 
1-8	In the Attach to VPC window, select **PrimaryVPC**, and then click **Yes, Attach**.
1-9	On the VPC Dashboard, select **Route Tables**, and then select **PublicRT**. 
1-10	Click the **Routes** tab, and then click **Edit routes**.
1-11	Click **Add route**.

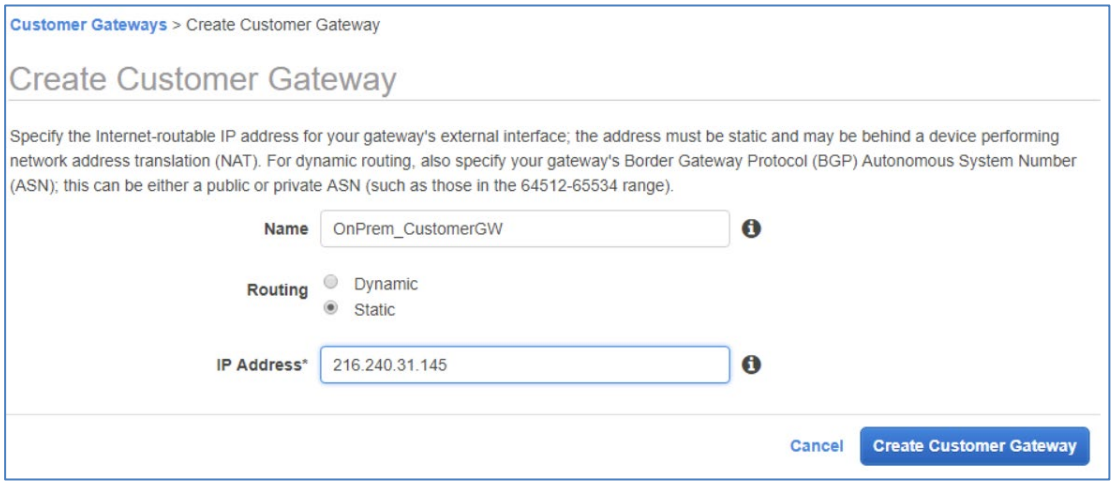
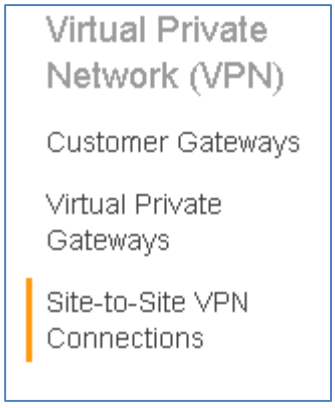
Step	Action
1-12	Enter the following values: • Destination: **192.168.0.0/24** • Target: Select **Virtual Private Gateway**, and then select your virtual private gateway ID**.** 
1-13	Click **Save routes**.
1-14	Click **Close**.
1-15	Click the **Route Propagation** tab.
1-16	Click **Edit route propagation**.
1-17	Select the **Propagate** checkbox, and then click **Save**. 
1-18	Repeat these steps for the PrivateRT route table in a similar manner, add the virtual private gateway route, and propagate the route.
1-19	On the VPC Dashboard, click **Security Groups**.
1-20	Select the **SGPrivateRHELInstances** security group, and then click the **Inbound Rules** tab.
1-21	Click **Edit rules**.
1-22	Click **Add Rule**.

Step	Action
1-23	In the rule row, use the following settings: • Type: **All traffic** • Protocol: **All** • Port Range: **All** • Source: **Custom** **192.168.0.0/24** • Description: **Allow traffic from On-prem** **Note:** These settings enable your on-premises data center traffic to reach all AWS instances that use this security group. 
1-24	Click **Save rules**.
1-25	Click **Close**.
1-26	Repeat these steps for the **SGPublicWindowsInstances** security group.
1-27	Double-check that you edited the route tables and the security groups for *both* the private and public subnets!

Task 2: Configure an AWS VPN and Customer Gateway

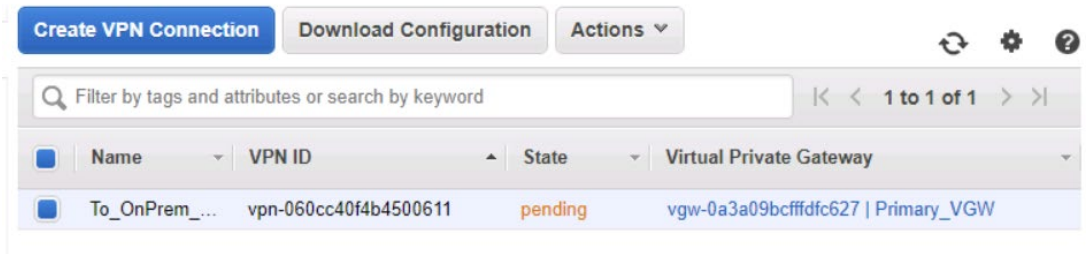
In this task, you configure the AWS elements of the VPN connection, including getting a pre-shared key to use for authentication.

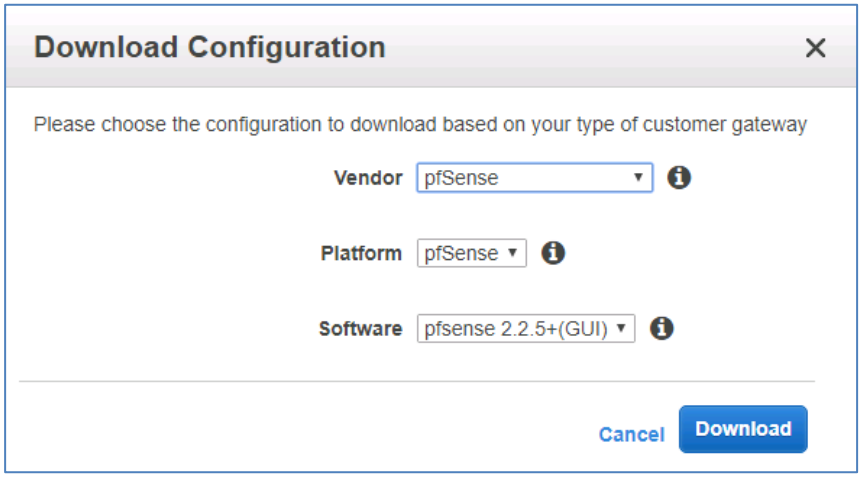
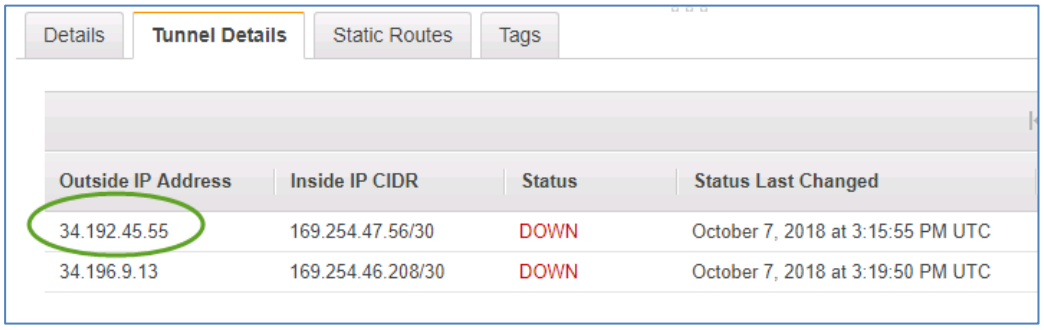
Step	Action
2-1	On the VPC Dashboard Select **Services** > **VPC**. 
2-2	On the VPC Dashboard, click **Customer Gateways**. 
2-3	Click **Create Customer Gateway**.

Step	Action
2-4	In the Create Customer Gateway window, enter the following values: • Name tag: **OnPrem_CustomerGW** • Routing: **Static** • IP address: <*Customer gateway address that is provided by your instructor*> (Your IP Address may differ from the image below) 
2-5	Click **Create Customer Gateway**.
2-6	Click **Close**.
2-7	On the VPC Dashboard, click **Site-to-Site VPN Connections**. 
2-8	Click **Create VPN Connection**.

Step	Action

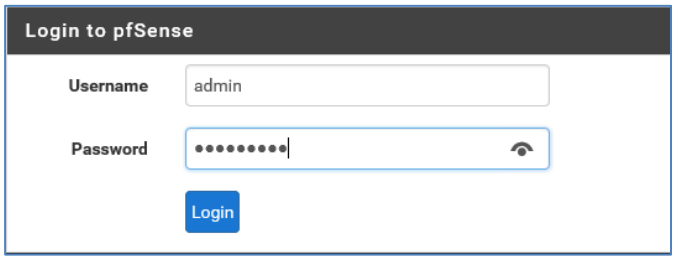
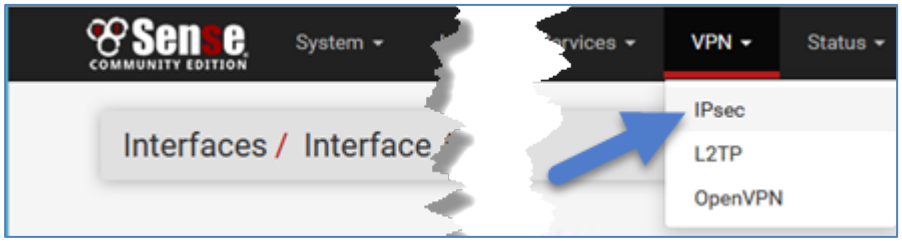
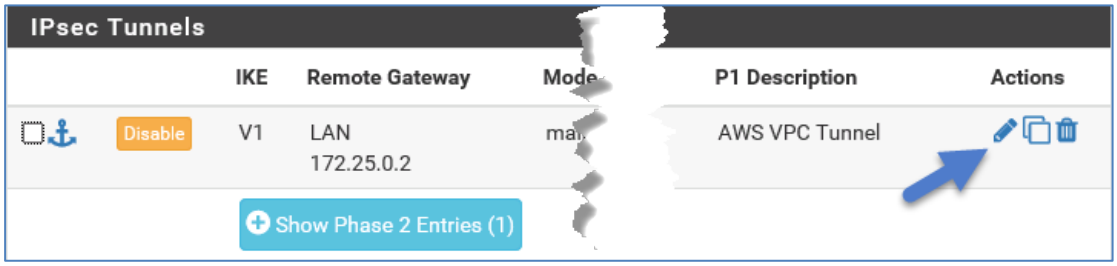
2-9	In the Create VPN Connection window, use the following settings:
	• Name tag: **To_OnPrem_VPN**
	• Virtual Private Gateway: Select the virtual private gateway ID for your primary VPC.
	• Customer Gateway:
	  ○ **Existing**
	  ○ Select the Customer Gateway ID.
	• Routing Options: **Static**
	• Static IP Prefixes**: 192.168.0.0/24**
	• Leave all Tunnel Options as their default values.
	 

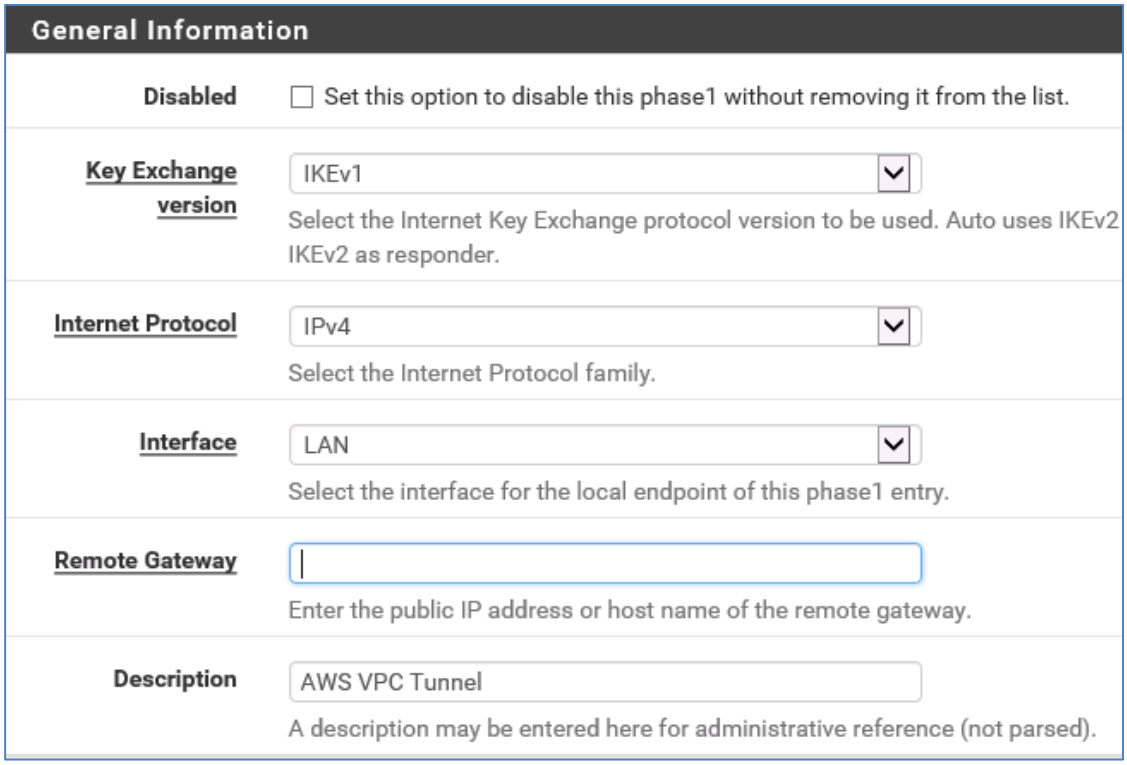
2-10	Click **Create VPN Connection**.
2-11	Click **Close**.
2-12	Wait for the VPN state to become available.  **Note:** The process might take up to five minutes.
2-13	Click **Download Configuration**.

Step	Action
2-14	In the Download Configuration window, select the following values: • Vendor: **pfSense** • Platform: **pfSense** • Software: **pfSense 2.2.5+ (GUI)**  (You are using pfSense in your on-premises environment as your secure gateway and router into the on-premises environment.)
2-15	Click **Download**.
2-16	Copy the file vpn-xxxx.txt from the Downloads folder to the CourseFiles folder on your desktop.
2-17	Click **x** to close the Download Configuration window.
2-18	Click the **Tunnel Details** tab.
2-19	Record the IP address of the Outside IP Address of Tunnel 1: _____  Although there are two tunnels for this course, you configure only one. In a production environment, you configure both tunnels for redundancy.

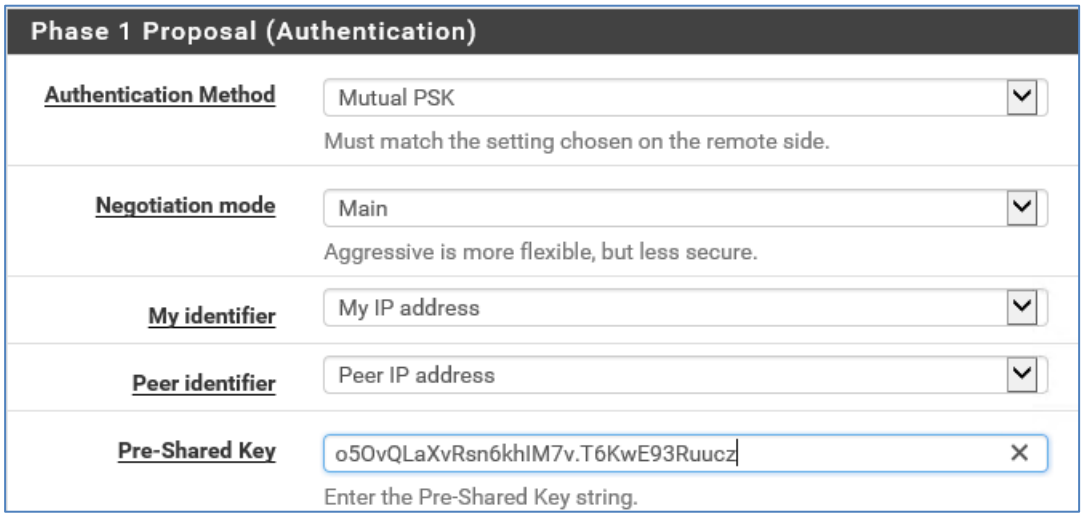
Task 3: Configure VPN IPsec Tunnels

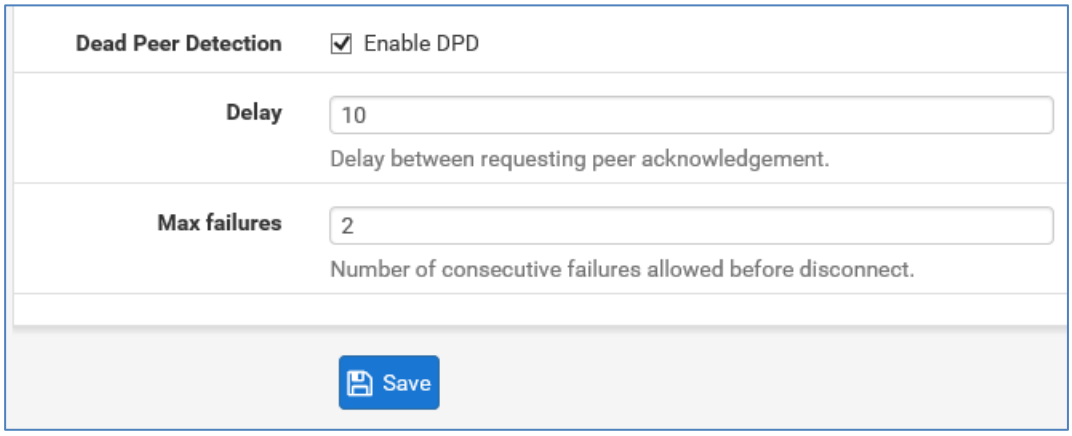
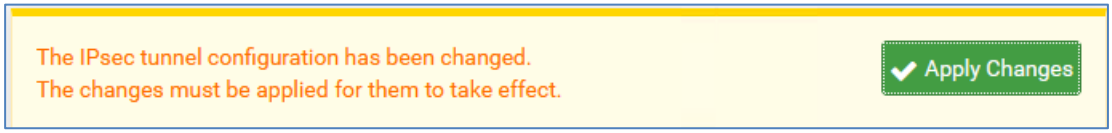
In this task, you create a VPN tunnel in the on-premises data center to connect the AWS environment (through the virtual private gateway) to your on-premises cluster.

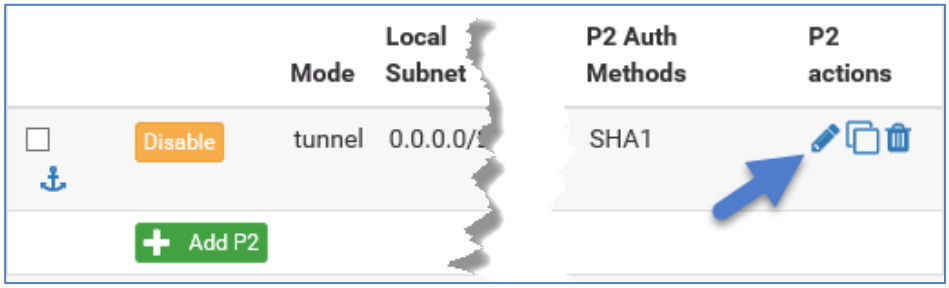
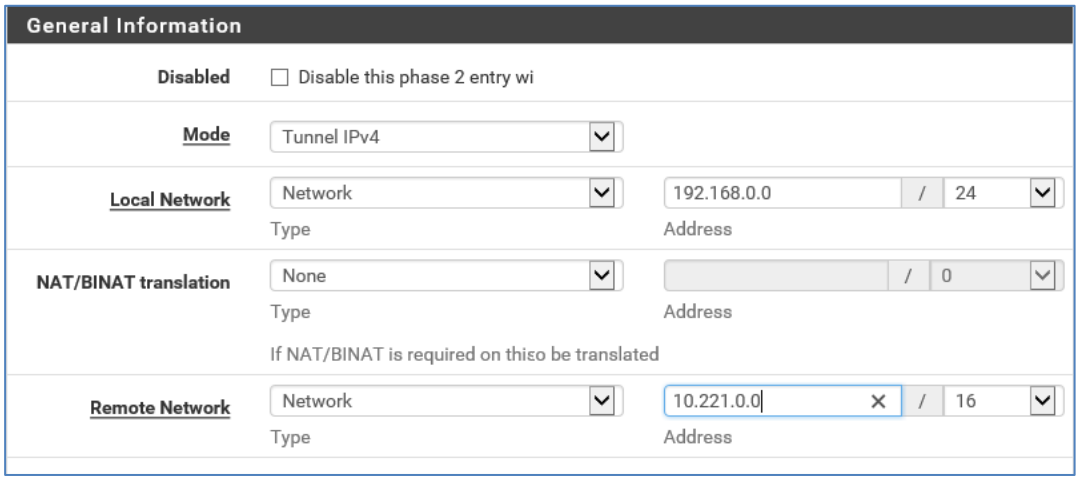
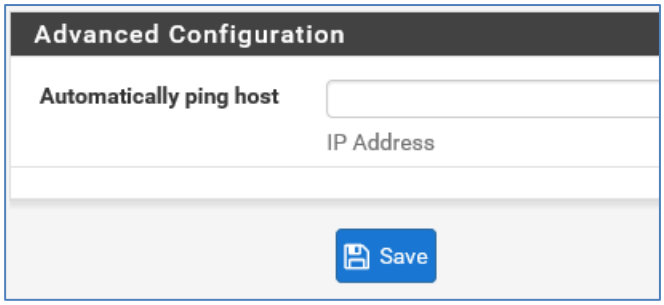
Step	Action
3-1	On your Windows Server jump host, double click the **pfSense** shortcut. 
3-2	If a security warning appears, click **Advanced** and then click **Proceed to 192.168.0.1 (unsafe)**.
3-3	Enter the following credentials: Username: **admin** Password: **Netapp1!** 
3-4	Click **Login**.
3-5	Select **VPN** > **IPsec**. 
3-6	Click the Edit icon for the AWS VPC Tunnel entry. 

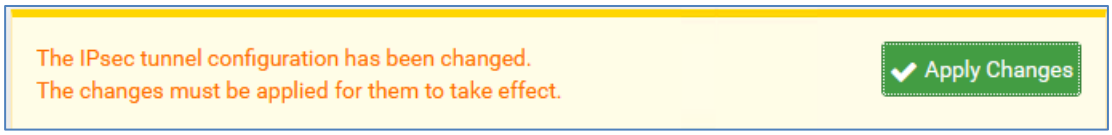
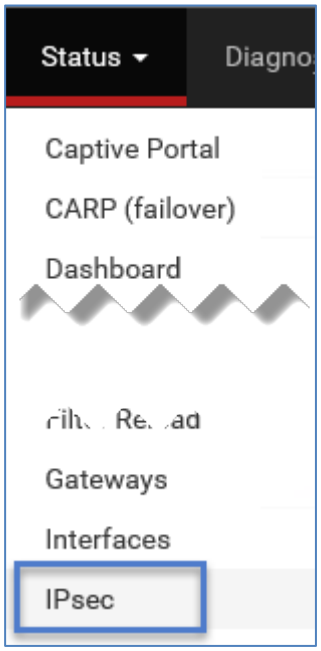
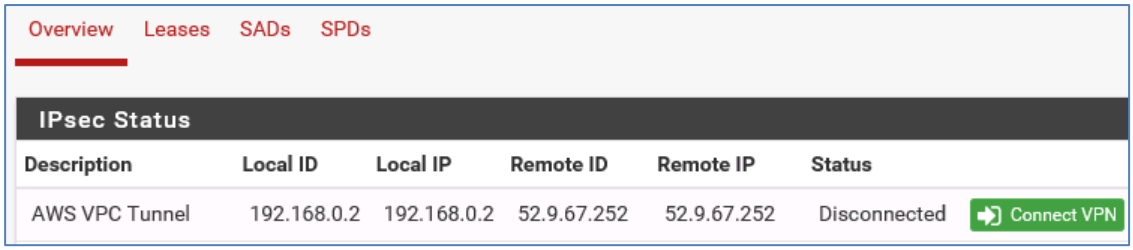
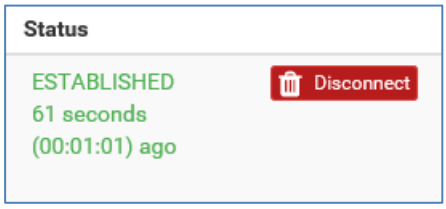
Step	Action
3-7	In the General Information section, replace the Remote Gateway value with the Tunnel 1 IP address that you recorded in Step 2-19. 
3-8	Open the file vpn-xxxx.txt.

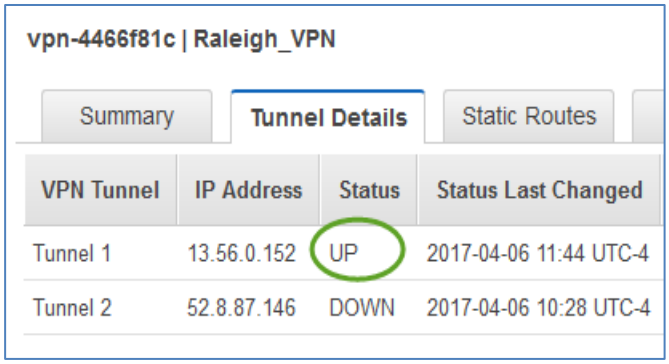
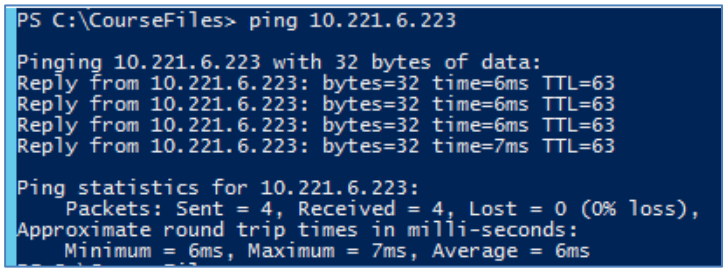
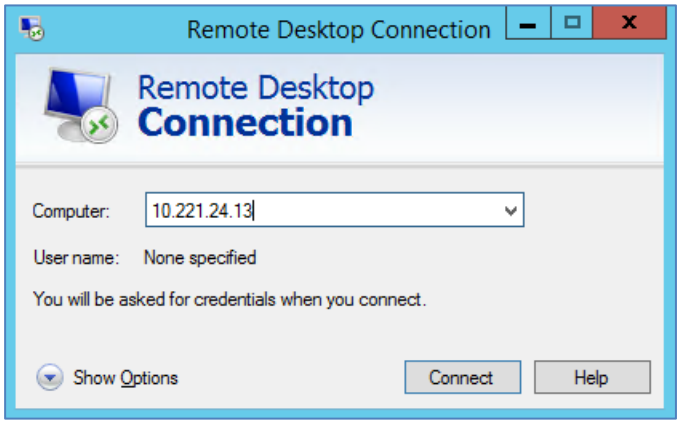
Step	Action

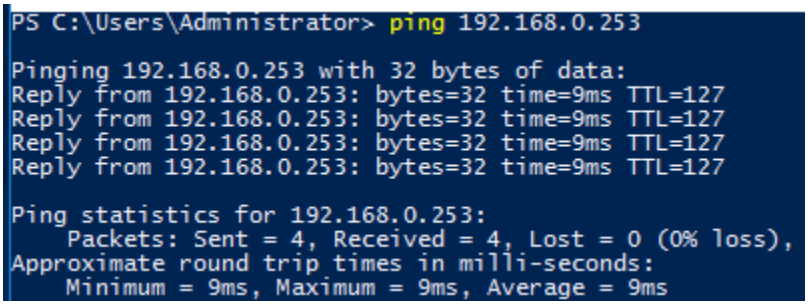
3-9	Scroll to the Phase 1 proposal (Authentication) section, and then replace the Pre-Shared Key value with the Pre-Shared Key value in the vpn-xxxx.txt file that you saved to the CourseFiles folder.
	
	`Phase 1 proposal (Authentication)`
	`a. Authentication Method: Mutual PSK`
	`b. Negotiation mode : Main`
	`c. My identifier : My IP address`
	`d. Peer identifier : Peer IP address`
	`e. Pre-Shared Key: o5OvQLaXvRsn6khIM7v.T6KwE93Ruucz`
	
	 

3-10	Be sure to copy the Pre-Shared Key value for Tunnel 1, not Tunnel 2. Both values exist in the vpn-xxxx.txt file.
3-11	Accept the default values for all the other settings, scroll to the bottom of the page, and then click **Save**. 
3-12	Click **Apply Changes**. 

Step	Action
3-13	For the AWS VPC Tunnel, click **Show Phase 2 Entries (1)**. 
3-14	Click the Edit icon for the Phase2 entry. 
3-15	In the General Information section, complete the following actions: a. Replace the Local Network IP address with **192.168.0.0/24**. b. Replace the Remote Network IP address with **10.221.0.0/16**. 
3-16	Accept the default values for all the other settings, scroll to bottom of the page, and then click **Save**. 

Step	Action
3-17	Click **Apply Changes**. 
3-18	From the pfSense menu, select **Status** > **IPsec**. 
3-19	For AWS VPC Tunnel, click **Connect VPN**. 
3-20	Verify that the session status is Established. 

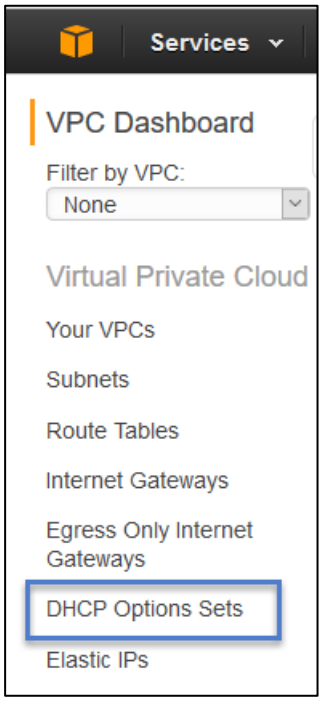
Step	Action
3-21	Return to the AWS Console, select **VPC** > **Site-to-Site VPN Connections**, and then verify that the tunnel status is UP. Note: It might take up to 10 minutes for the Status to appear as UP. 
3-22	The following steps are used to verify that you have connectivity from your on-premises environment to the public subnet and the private subnet in AWS VPC through the VPN. You also verify that you can reach the on-premises environment from the AWS VPC that is using the VPN.
3-23	On the jump host, open a Windows PowerShell (or CLI) window, and then ping the private IP address of the Redhat_Private Amazon Elastic Compute Cloud (Amazon EC2) instance in AWS. 
3-24	Instantiate a Remote Desktop Connection from the jump host by using the private IP address of the Win2k16_Public Amazon EC2 instance in AWS. **Note:** You might need to decrypt the password again by using the MyAWSKey.pem file 

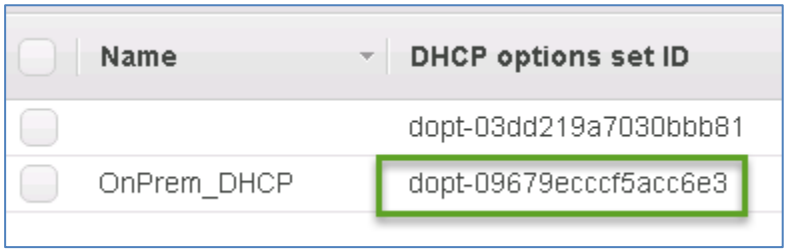
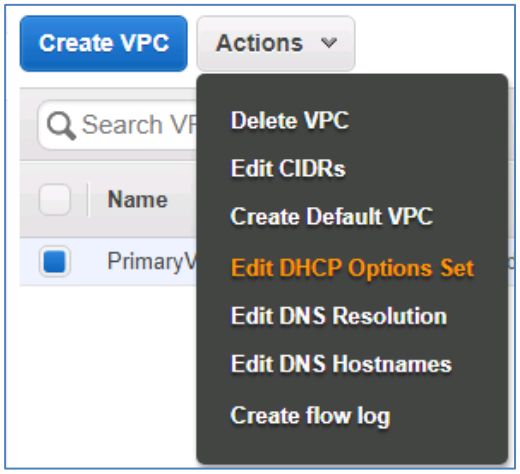
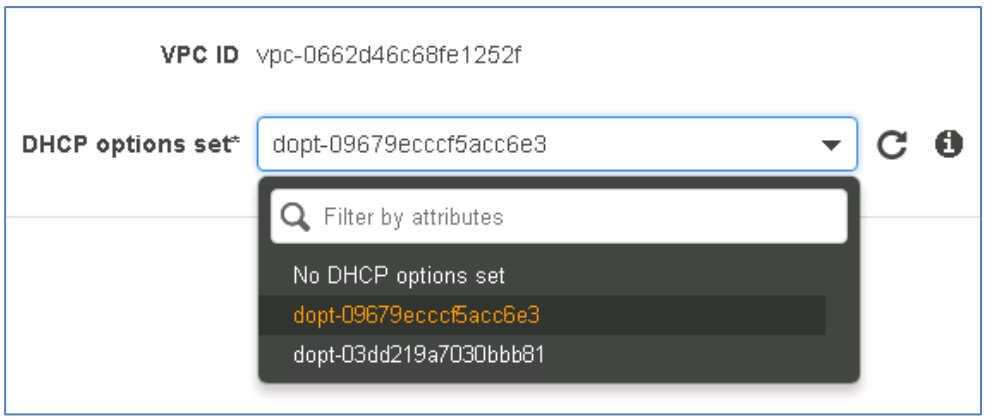
Step	Action
3-25	Open a PowerShell window from the Win2k16_Public desktop, and then verify that you can ping the domain controller: C:> **`ping 192.168.0.253`** 

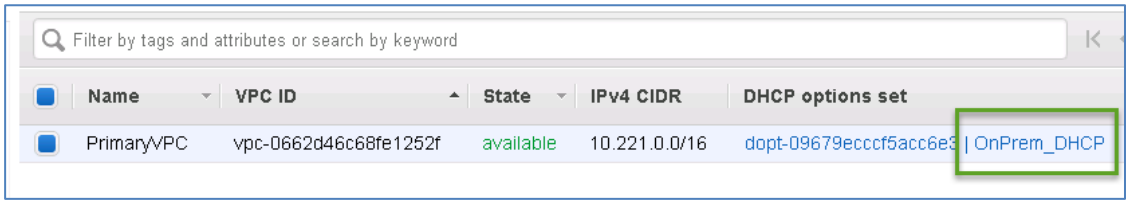
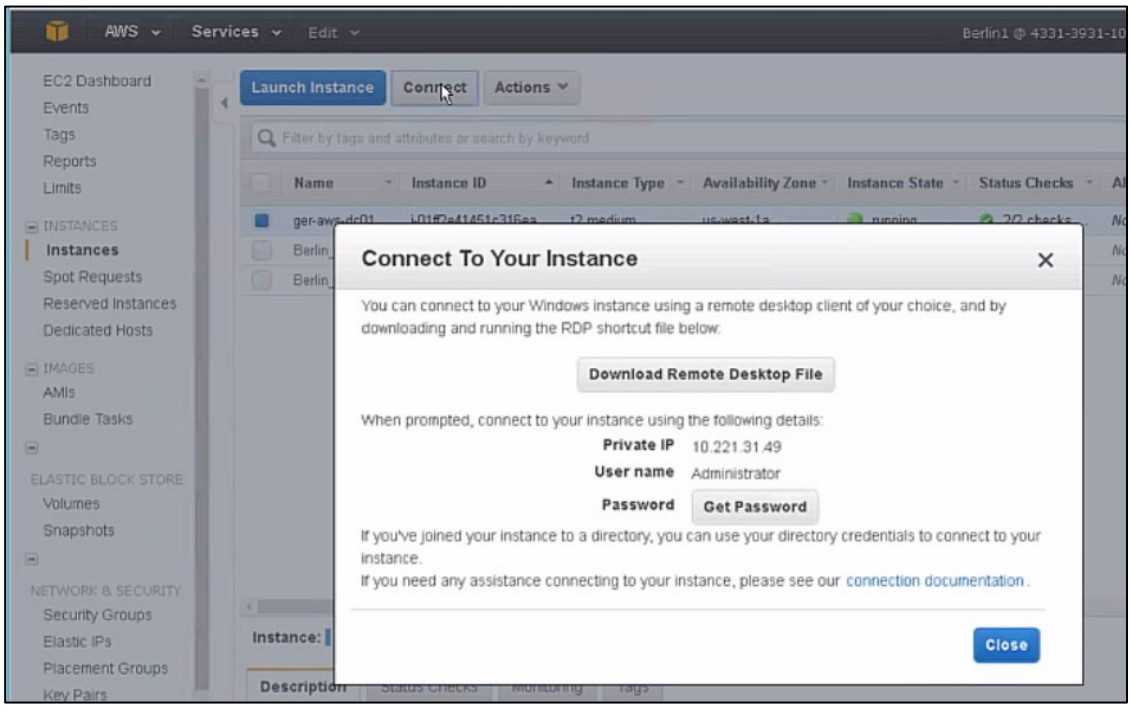
```
PS C:\Users\Administrator> ping 192.168.0.253

Pinging 192.168.0.253 with 32 bytes of data:
Reply from 192.168.0.253: bytes=32 time=9ms TTL=127
Reply from 192.168.0.253: bytes=32 time=9ms TTL=127
Reply from 192.168.0.253: bytes=32 time=9ms TTL=127
Reply from 192.168.0.253: bytes=32 time=9ms TTL=127

Ping statistics for 192.168.0.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 9ms, Average = 9ms
```

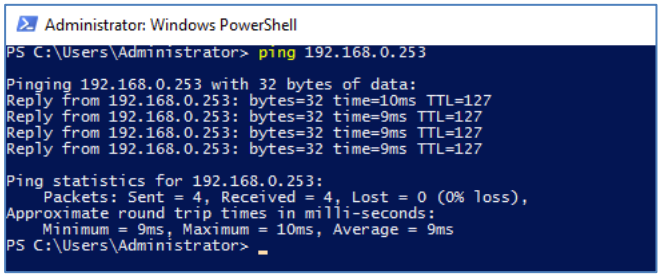
Task 4: Configure an AWS VPC to Use the Corporate Network Dynamic Host Configuration Protocol

In this task, you create custom Dynamic Host Configuration Protocol (DHCP) options and deploy a Windows instance that uses those options.

Step	Action
4-1	Return to the AWS Console, and select **Services** > **VPC**.
4-2	All instances that are created automatically are assigned to the Amazon DHCP domain. In this task, you create an option set to alter the settings so that new instances automatically join your private domain. (demo.netapp.com)
4-3	On the VPC Dashboard, click **DHCP Options Sets**. 
4-4	Click **Create DHCP option set**.
4-5	Enter the following values: • Name tag: **OnPrem_DHCP** • Domain name: **demo.netapp.com** • Domain name servers: **192.168.0.253** • NTP servers: **192.168.0.253** • NetBIOS name servers: Leave blank. • NetBIOS node type: Leave blank.
4-6	Click **Create DHCP options set**.
4-7	Click **Close**.

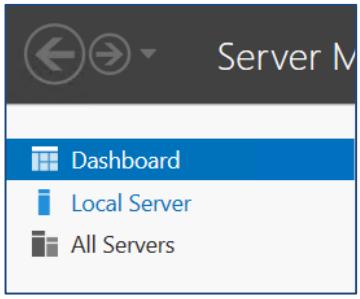
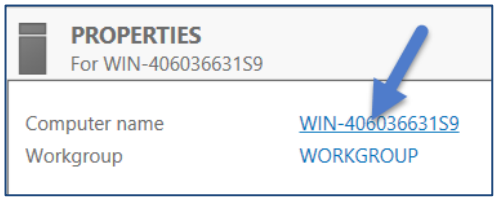
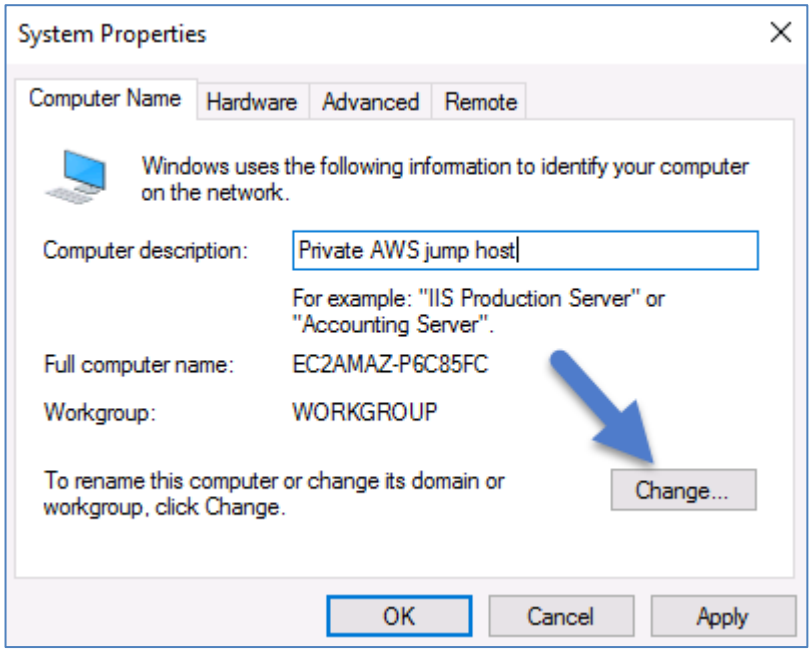
Step	Action
4-8	Record the DHCP options set ID for the OnPrem_DHCP. 
4-9	On the VPC Dashboard, click **Your VPCs**.
4-10	Select the **PrimaryVPC** checkbox.
4-11	Select **Actions** > **Edit DHCP Options Set**. 
4-12	In the Edit DHCP Options Set window, select the DHCP options set ID for the OnPrem_DHCP, and then click **Save**. 
4-13	Click **Close**.

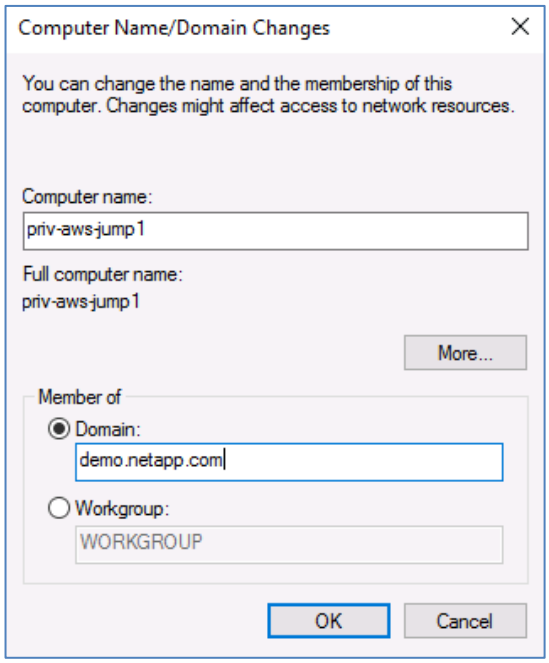
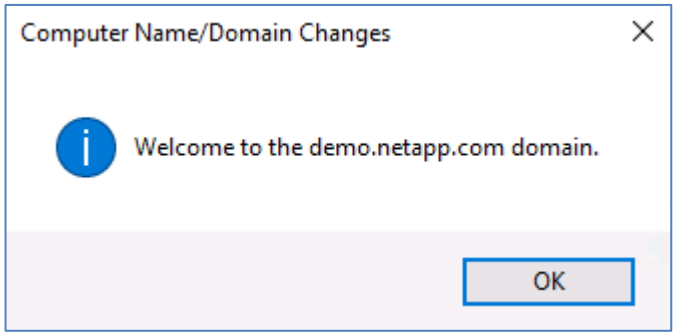
Step	Action
4-14	Verify that you see OnPrem_DHCP as the option set for PrimaryVPC. 
4-15	Create an Amazon EC2 for Windows Server instance (Microsoft Windows Server 2016) in the private subnet by using the following key data: • AMI: **Microsoft Windows Server 2016 Base** • Name: **Win2k16_Private** • VPC: **PrimaryVPC** • Subnet: **PrivateSubnet** • Tags: Key: **Name** Value: **Win2k16_Private** • Security Group**:** Create a new Security Group with the following details: a. Name: **SGPrivateWindowsInstances** b. Rule: allow Remote Desktop Protocol (**RDP**) from within the VPC (**10.221.0.0/16**) c. Rule: allow **all traffic** from **192.168.0.0/24** • On launch choose key pair: **MyAWSKey** **Note:** This Windows Server is now assigned the DNS servers in the on-premises data center.
4-16	After the instance finishes booting, click the **Connect** button to log in to the instance. 

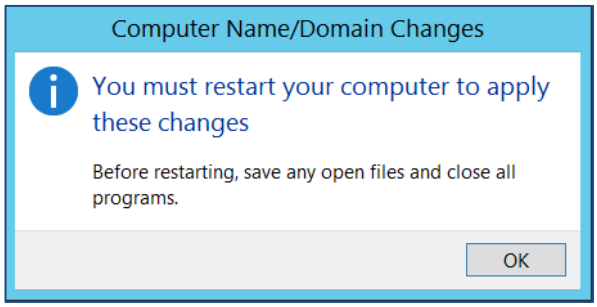
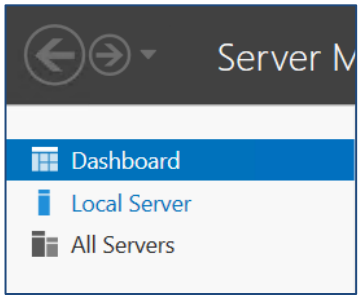
Step	Action
4-17	In the Connect To Your Instance window, use the following settings: a. Click **Get Password**. b. Select the key file in your CourseFiles folder. c. Click **Decrypt password**. d. Copy the private IP, user account name and password to a text file that is named **Win2k16_Private_Login.txt**.
4-18	Open a Remote Desktop Connection from the jump host to the Amazon EC2 instance by using the private IP, user name and password from the previous step.
4-19	From the private Window Server Amazon EC2 instance, open a PowerShell (or CLI) window, and then ping the DNS servers. C:> **`ping 192.168.0.253`** 

Task 5: Join the On-Premises Active Directory Domain

In this task, you configure the AWS instance to be a member of the on-premises Active Directory domain.

Step	Action
5-1	On your Private_W2K16 desktop, from the Start menu, open Server Manager. 
5-2	On the Dashboard, click **Local Server**. 
5-3	Click the Computer name value. 
5-4	In the Computer description field, enter **Private AWS jump host**, and then click **Change.** 
5-5	Change the Computer name value to **priv-aws-jump1**.

Step	Action
5-6	Select the **Domain** option button, and then enter **demo.netapp.com**. 
5-7	Click **OK**.
5-8	In the Windows Security window, enter the following values: • User name: **Demo\Administrator** • Password: **Netapp1!**
5-9	Click **OK**.
5-10	Verify that a Welcome to the domain message appears. **Note:** The message might take several minutes to appear. 
5-11	Click **OK**.

Step	Action
5-12	When the "You must restart your computer to apply these changes" message appears, click **OK**. 
5-13	In the System Properties window, click **Close**.
5-14	Click **Restart Now**.
5-15	After the RDP session closes, wait a few minutes for the Private_W2K16 instance to restart.
5-16	Open a Remote Desktop Connection from your jump host to this Amazon EC2 instance by using the following credentials: • User name: **Demo\Administrator** • Password: **Netapp1!**
5-17	You can now log in by using the user name and password that is authenticated by the on-premises domain controller. You do not need to use the user name and password that was generated by AWS.
5-18	Open Server Manager by clicking the icon to the right of the Start icon. 
5-19	On the Dashboard, click **Local Server**. 
5-20	Verify that the computer is a member of the demo.netapp.com domain. 

End of Exercise

Module 3: NetApp Cloud Volumes ONTAP

Exercise 1: Using OnCommand Cloud Manager to Deploy Cloud Volumes ONTAP

In this exercise, you use OnCommand Cloud Manager to deploy a Cloud Volumes ONTAP instance.

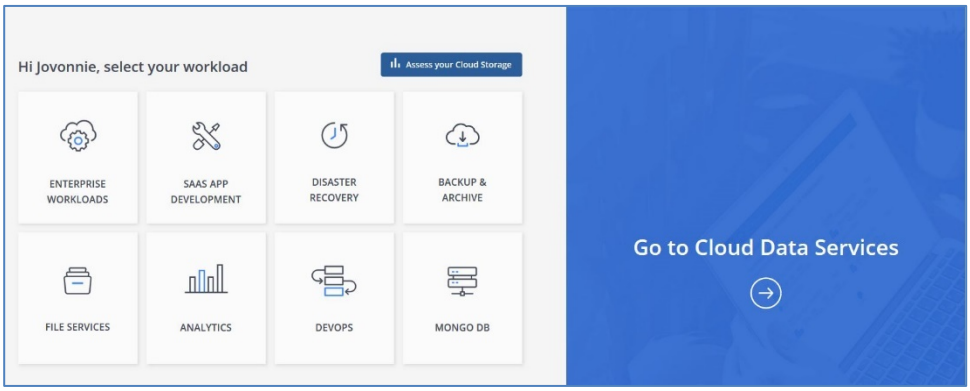
Objectives

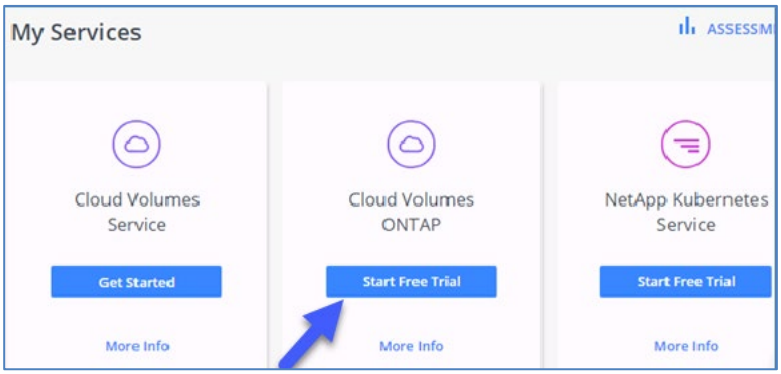
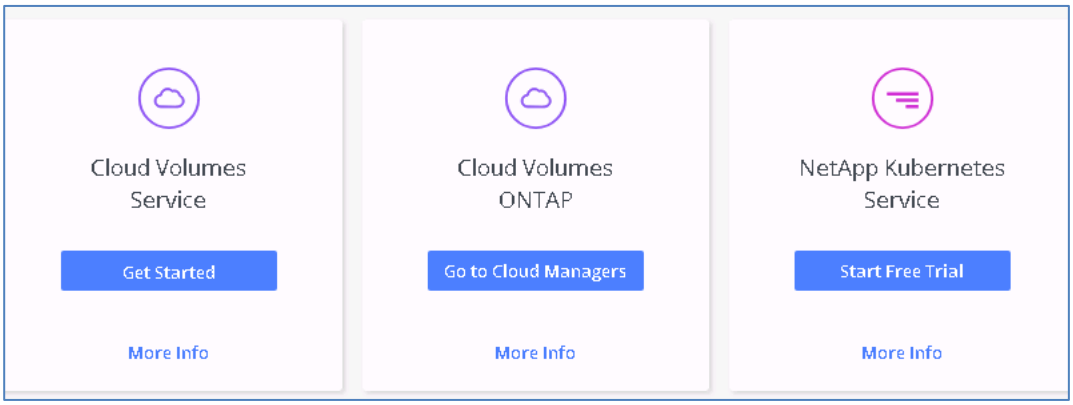
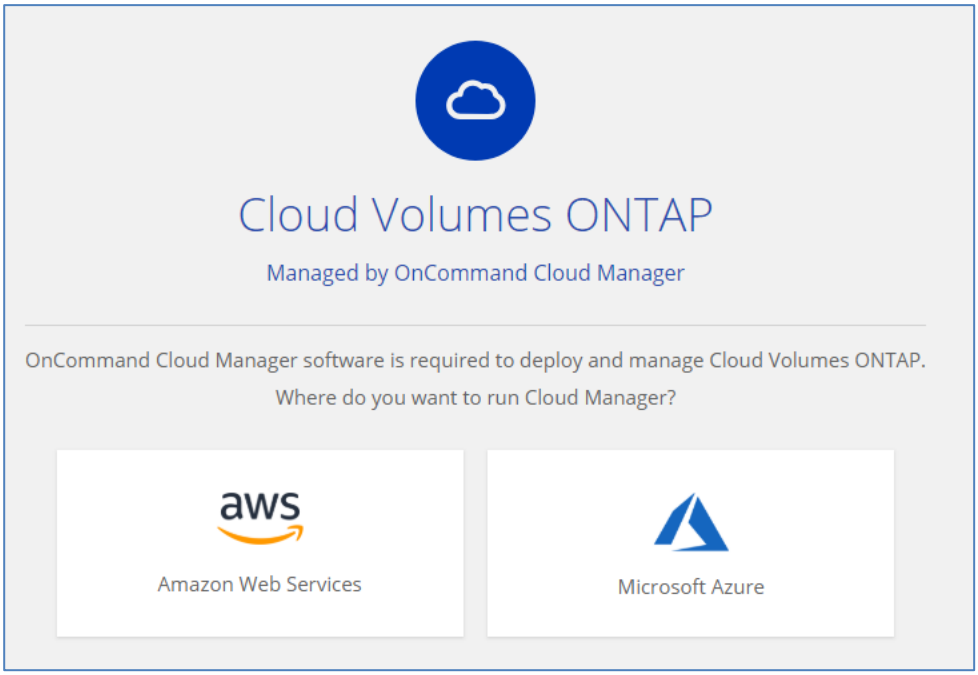
This exercise focuses on enabling you to do the following:

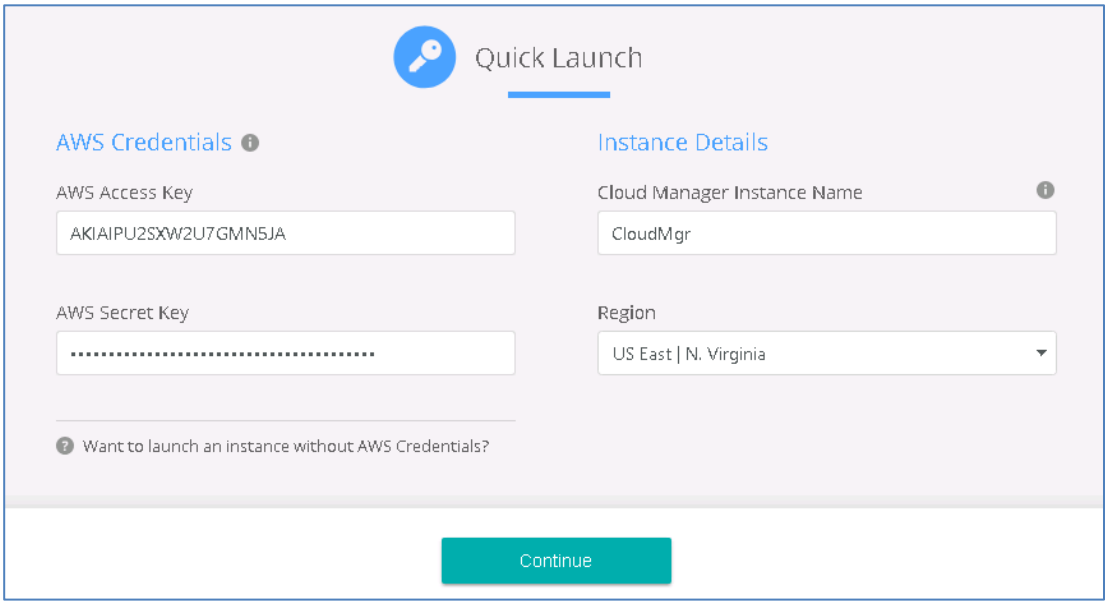
- Deploy Cloud Manager
- Configure Amazon Web Services (AWS) Identity and Access Management (IAM) permissions for Cloud Manager
- Deploy Cloud Volumes ONTAP instances by using Cloud Manager
- Create volumes and prepare the CIFS protocol for a Cloud Volumes ONTAP instance

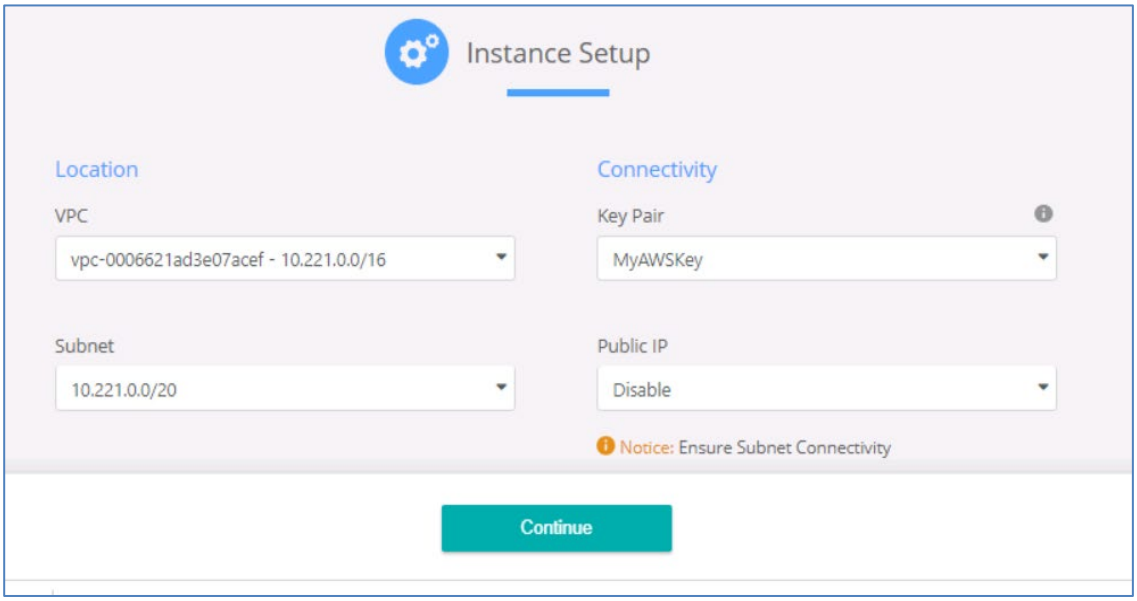
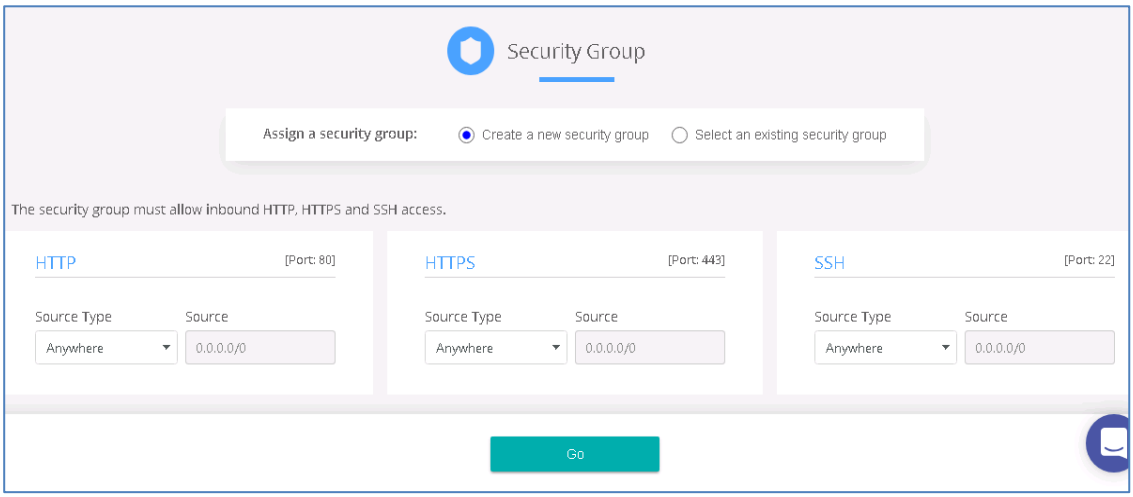
Task 1: Deploy and Configure Cloud Manager

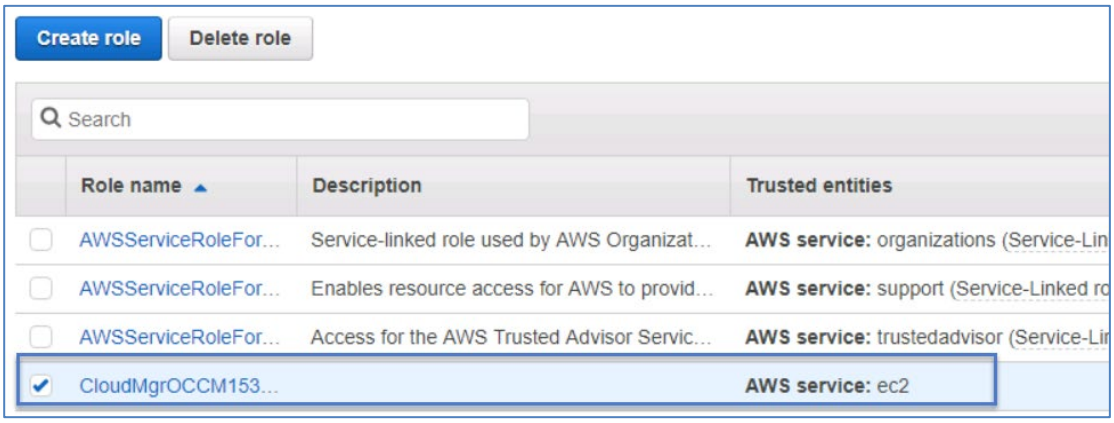
In this task, you use NetApp Cloud Central to deploy Cloud Manager as an AWS Amazon Machine Image (AMI) instance.

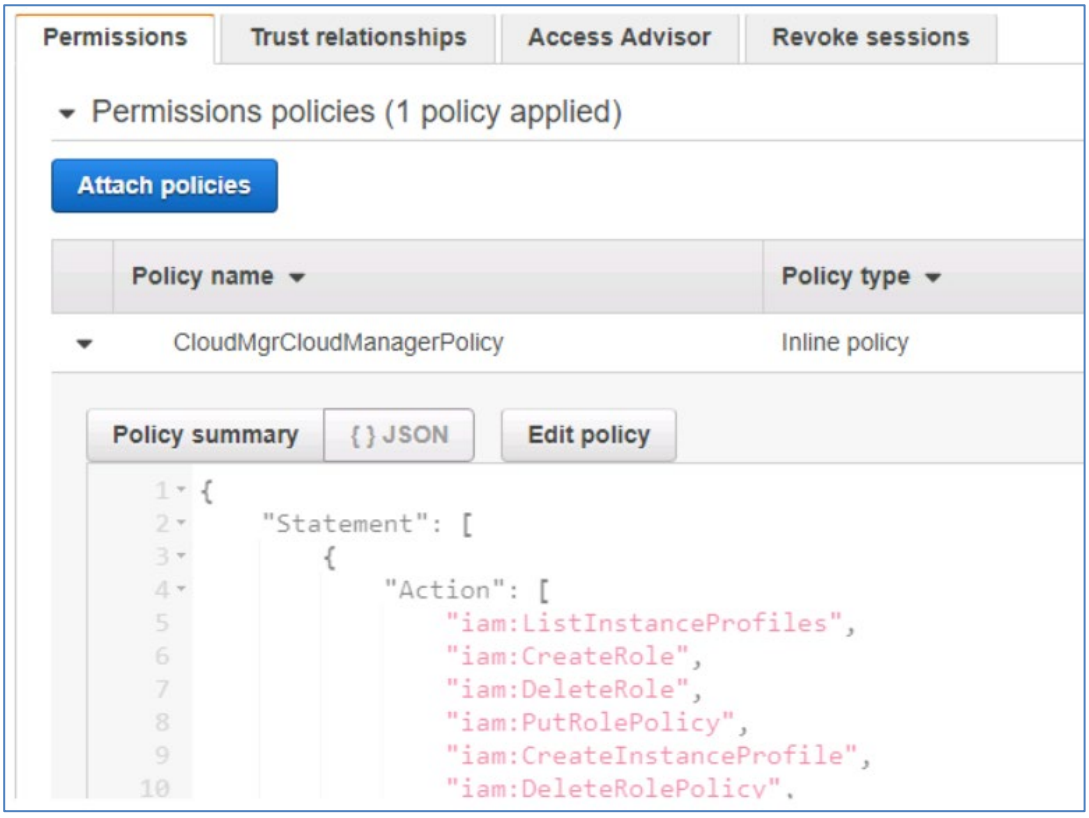
Step	Action
1-1	Log in to the on-premises jump host (Windows Server).
1-2	Navigate to cloud.netapp.com. (Note it runs best in Chrome so you might want to download Chrome to your Windows Server.)
1-3	Click **LOGIN**.
1-4	On the LOGIN page, enter the following: • Email: <*your user name in the awslogin.txt file*>**@demo.netapp.com** • Password: **Netapp1!**
1-5	Click **LOGIN**.
1-6	On the right of the window, click **Go to Cloud Data Services**. 

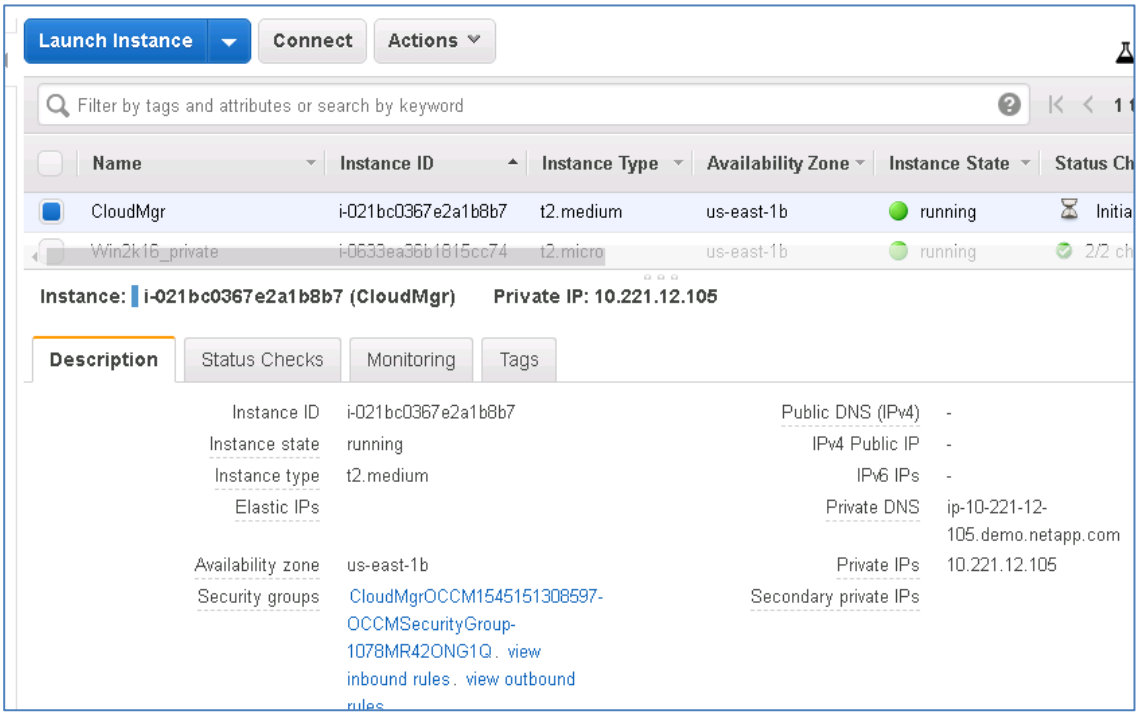
Step	Action
1-7	Click the **Start Free Trial** button under **Cloud Volumes ONTAP** 
1-8	If you have previously created Cloud Manager from Cloud Central, you see Go to Cloud Managers instead of Create Cloud Manager. 
1-9	Click the **Amazon Web Services** tile to deploy Cloud Manager in AWS. 

Step	Action
1-10	Complete the **Quick Launch** form by entering the appropriate information in the AWS Credentials and Instance Details fields: • AWS Access Key ID: *<found in awslogin.txt file on the desktop of your jumphost>* • AWS Secret Access Key: *<found in awslogin.txt file on the desktop of your jumphost>* • Cloud Manager Instance Name: **CloudMgr** • Region: Select **US East | N. Virginia** 
1-11	Click **Continue**.

Step	Action
1-12	In the Instance Setup page, select the following elements from the lists: • VPC: Select **PrimaryVPC**. • Key Pair: Select **MyAWSKey**. • Subnet: Select the **PrivateSubnet**. • Public IP: Select **Disable**. • Click **Continue**. 
1-13	In the Security Group page, configure the Cloud Manager security group. • Assign a security group: Select **Create a new security group**. • HTTP: Select **Anywhere** in the Source Type field. • HTTPS: Select **Anywhere** in the Source Type field. • SSH: Enter Select **Anywhere** in the Source Type field. 
1-14	Click **Go**.

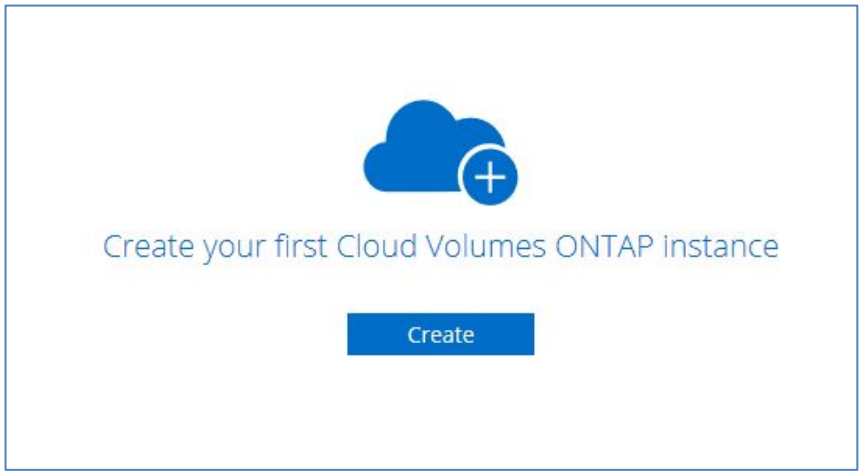
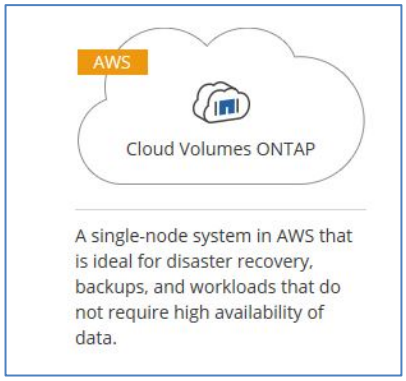
Step	Action
1-15	Verify that Cloud Manager starts to deploy. Do not wait for Cloud Manager to deploy, go on to the next step in this guide. 
1-16	Cloud Manager automatically deploys in about seven minutes. Your web browser directs you to the Cloud Manager interface in which you can deploy Cloud Volumes ONTAP instances.
1-17	Return to the AWS Console and navigate to **Services** > **IAM** > **Roles**.
1-18	Verify that a Role was created for your Cloud Manager. 
1-19	Click the Cloud Manager Role name.

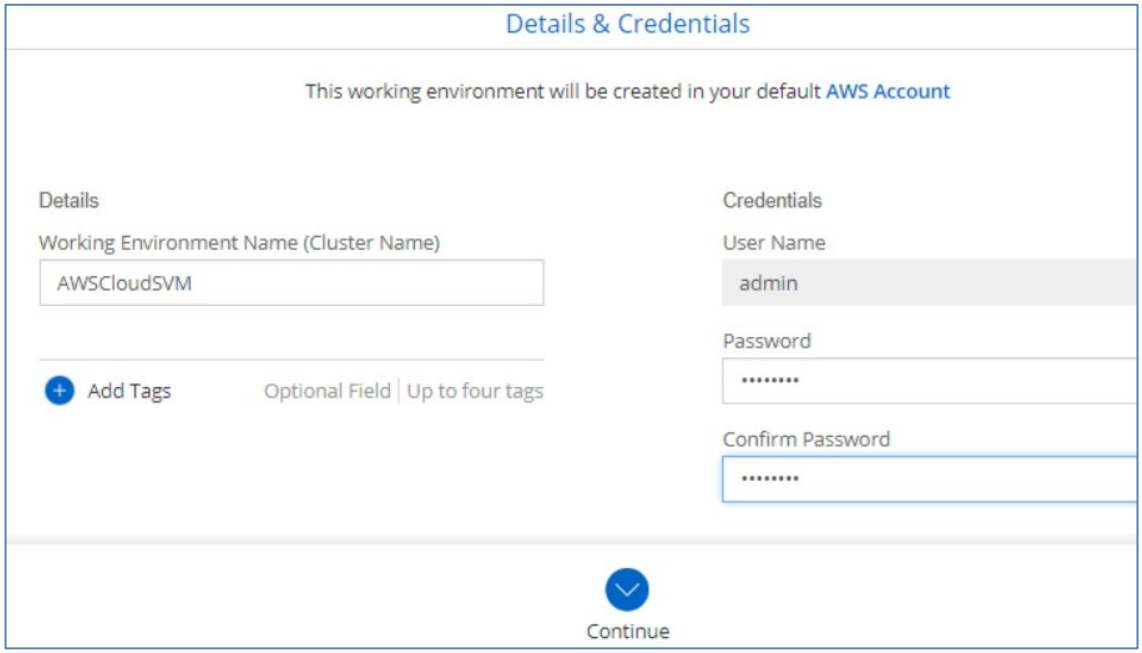
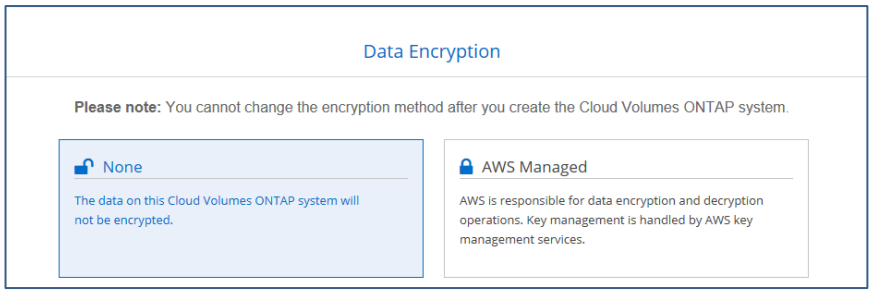
Step	Action
1-20	Expand the policy and then click the **JSON** tab. 
1-21	These are permissions that Cloud Central configures for Cloud Manager so that it has the necessary AWS permissions to perform operations, such as deploying virtual machines (VMs) and provisioning storage. These steps were informational so you understand how Cloud Manager handles AWS permissions, there is no action you need to perform in IAM.

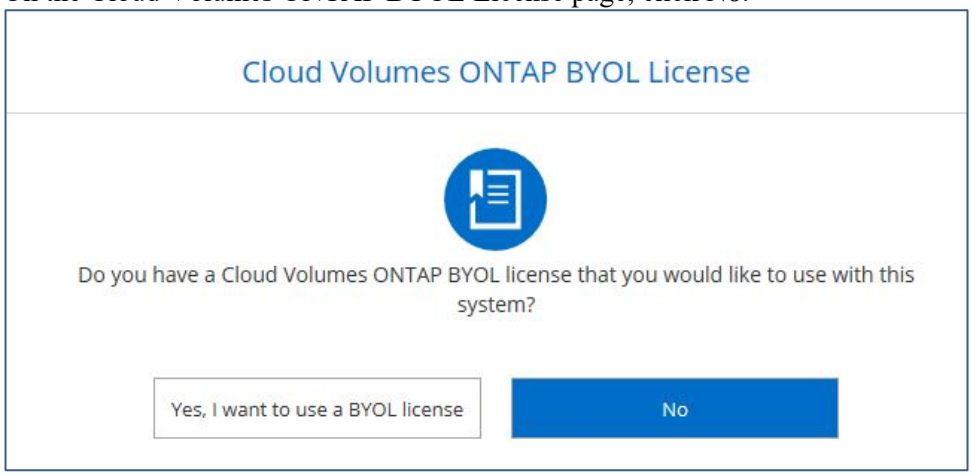
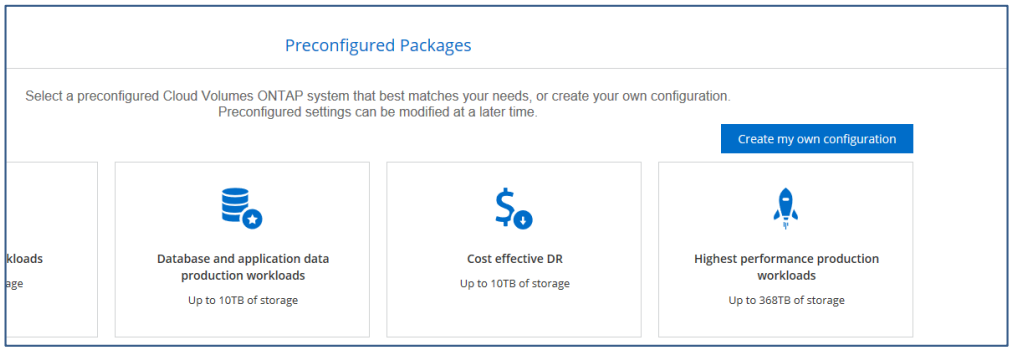
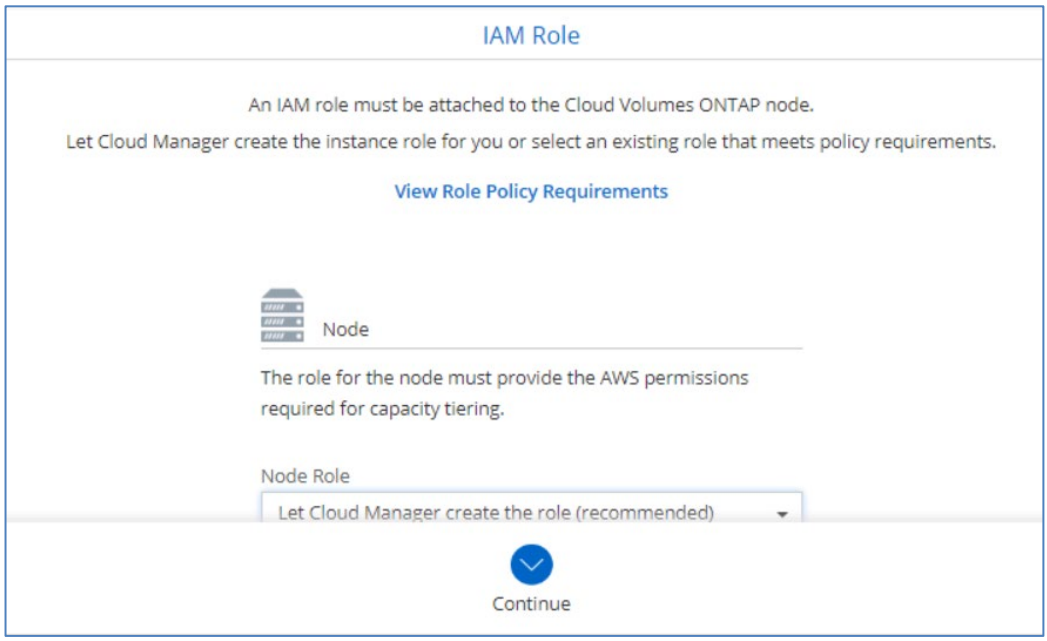
Step	Action
1-22	Select **Services** > **EC2** and note that an Amazon Elastic Compute Cloud (Amazon EC2) instance with the name CloudMgr is deployed, with an instance type of t2.medium. It is deployed in the private subnet and is associated with the security group that you configured in the Cloud Manager wizard. 
1-23	Return to Cloud Central and wait for Cloud Manager to finish deploying.

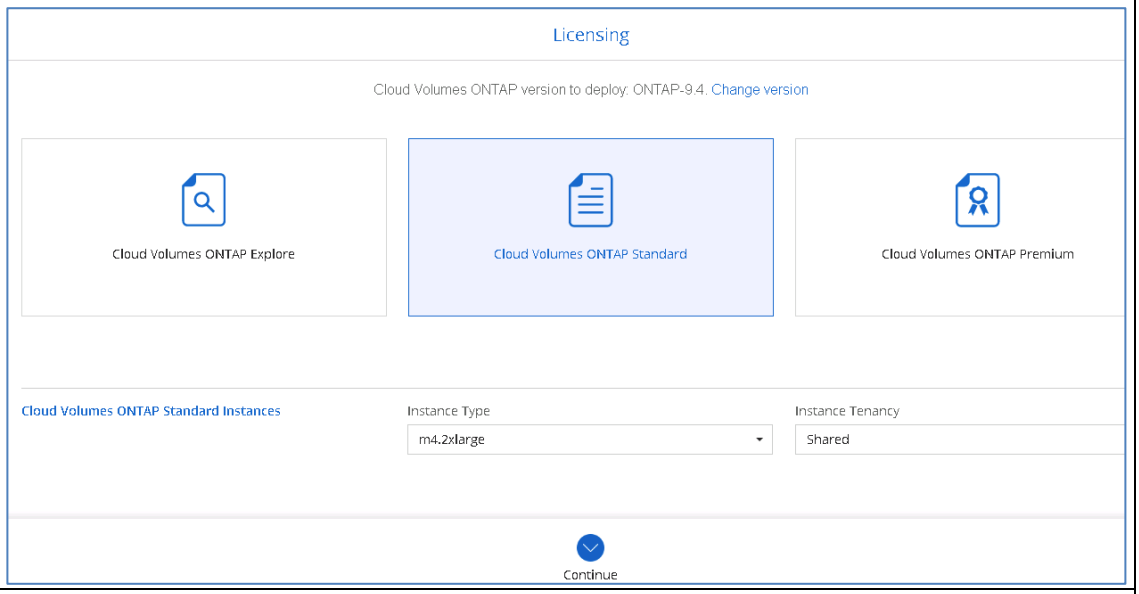
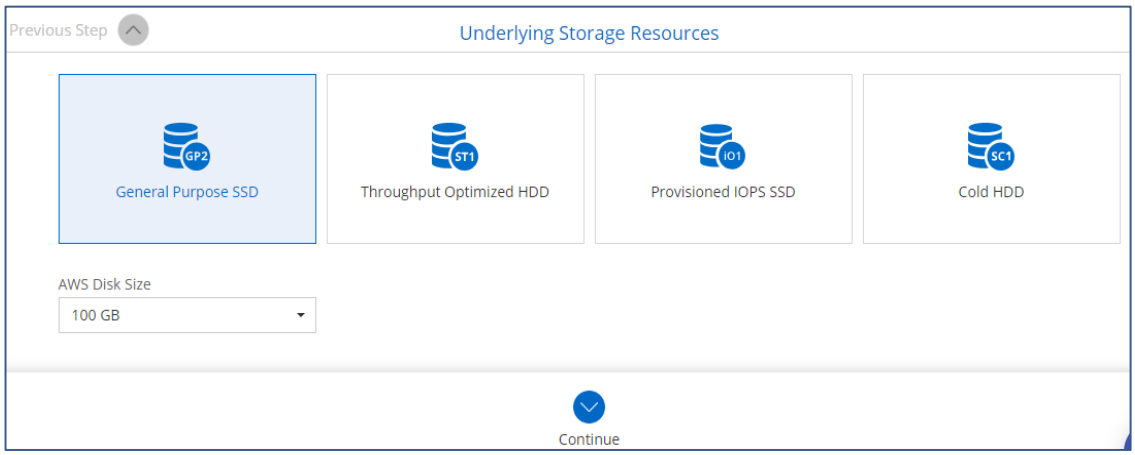
Task 2: Deploy Cloud Volumes ONTAP

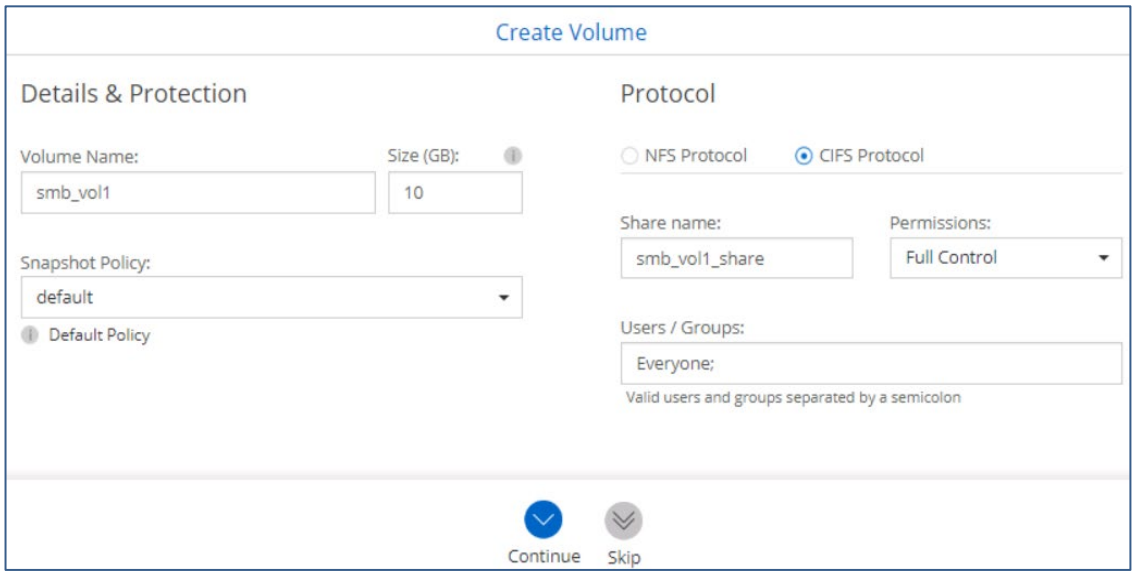
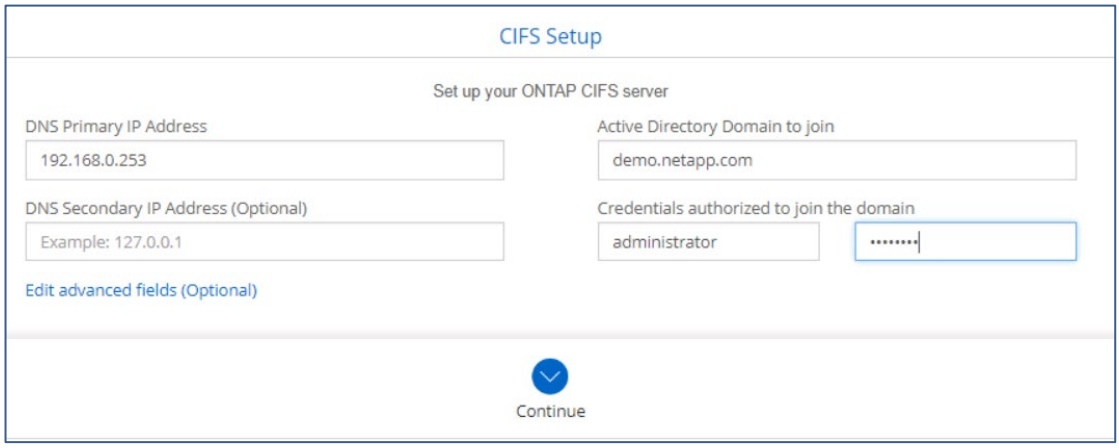
In this task, you deploy your first Cloud Volumes ONTAP instance.

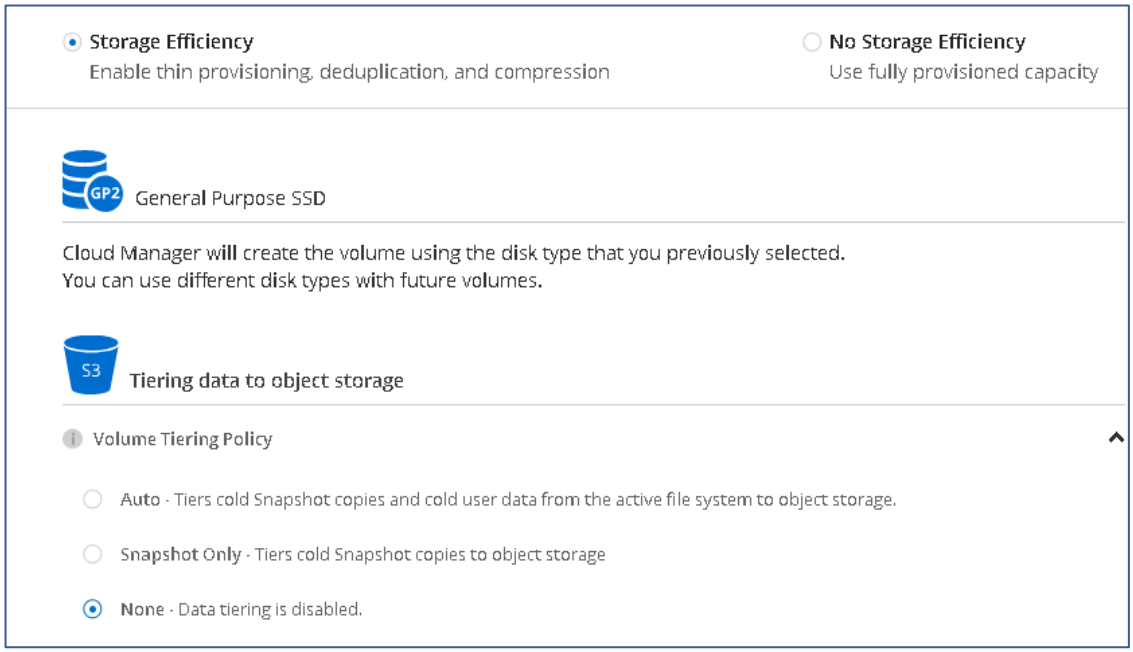
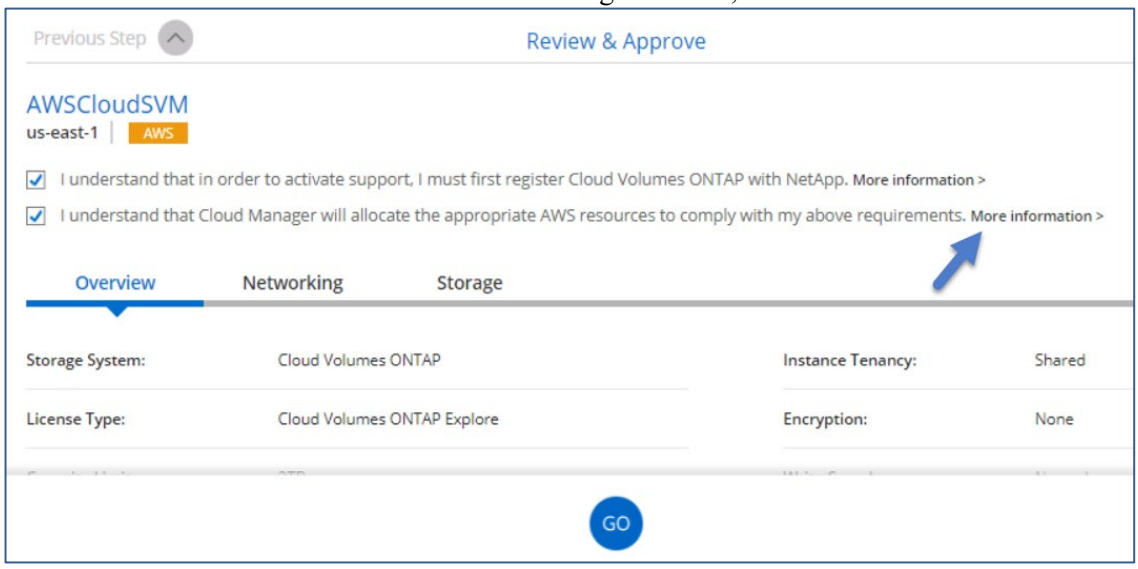
Step	Action
2-1	In Cloud Manager, click **Create**. 
2-2	Select **Cloud Volumes ONTAP.** 
2-3	In a production environment, depending on customer availability requirements, you might want to select Cloud Volumes ONTAP HA to ensure high availability of Amazon Elastic Block Store (Amazon EBS) storage.

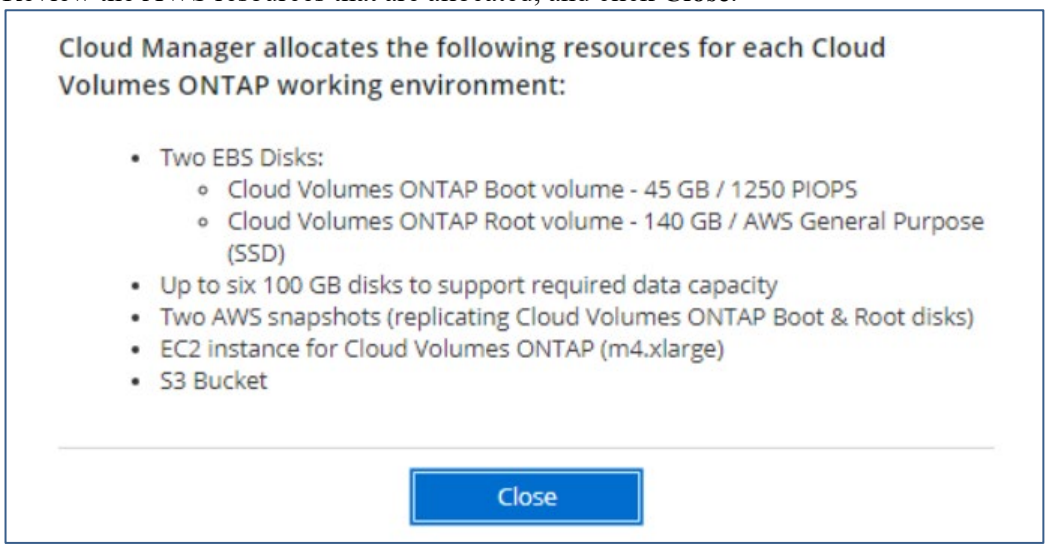
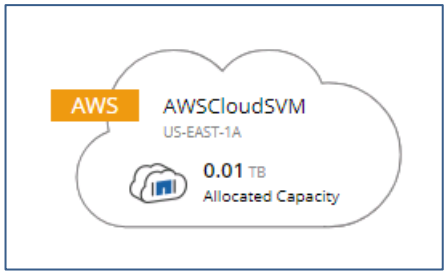
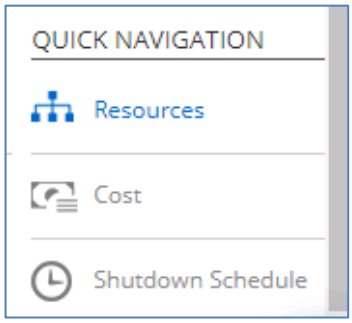
Step	Action
2-4	On the Details & Credentials page, enter the following values: • Working Environment Name: **AWSCloudSVM** • Password: **Netapp1!** • Confirm Password: **Netapp1!** 
2-5	Click **Continue**.
2-6	On the Location page, select the following values: • AWS region: **US East | N. Virginia** • VPC: **PrimaryVPC** • Subnet: **PrivateSubnet (10.221.0.0/20)** • Security Group: **Generated security group group** • SSH authentication method: **Password**
2-7	Click **Continue**.
2-8	On the Data Encryption page, click **None**. 
2-9	Click **Continue**.

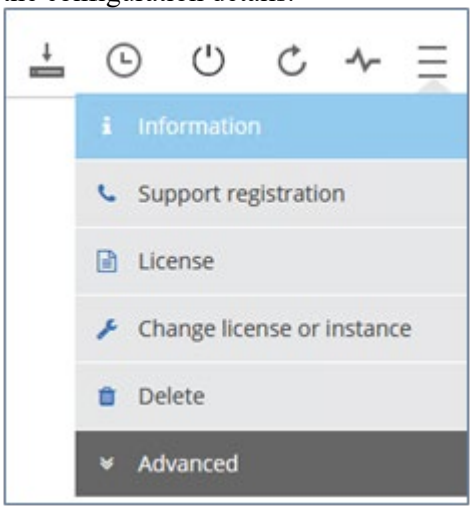
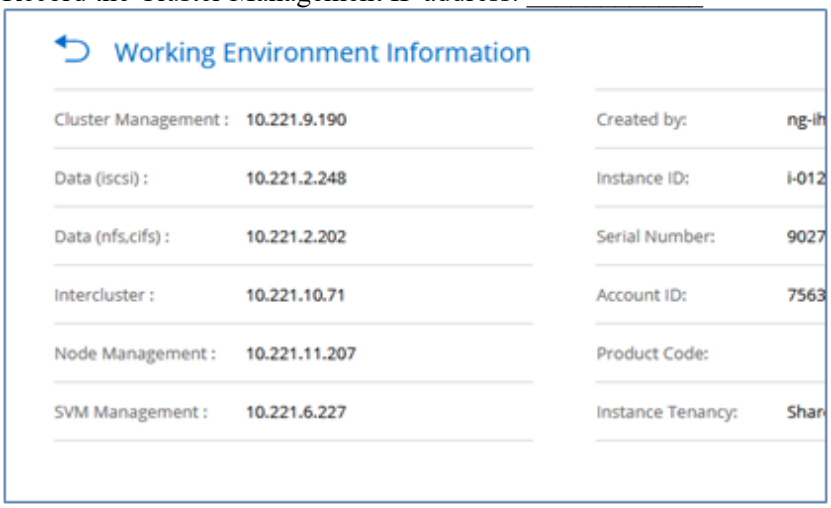
Step	Action
2-10	On the Cloud Volumes ONTAP BYOL License page, click **No**. 
2-11	On the Preconfigured Packages page, click **Create my own configuration**. 
2-12	On the IAM Role page, accept the recommendation **Let Cloud Manager create the role**. 
2-13	Click **Continue**.

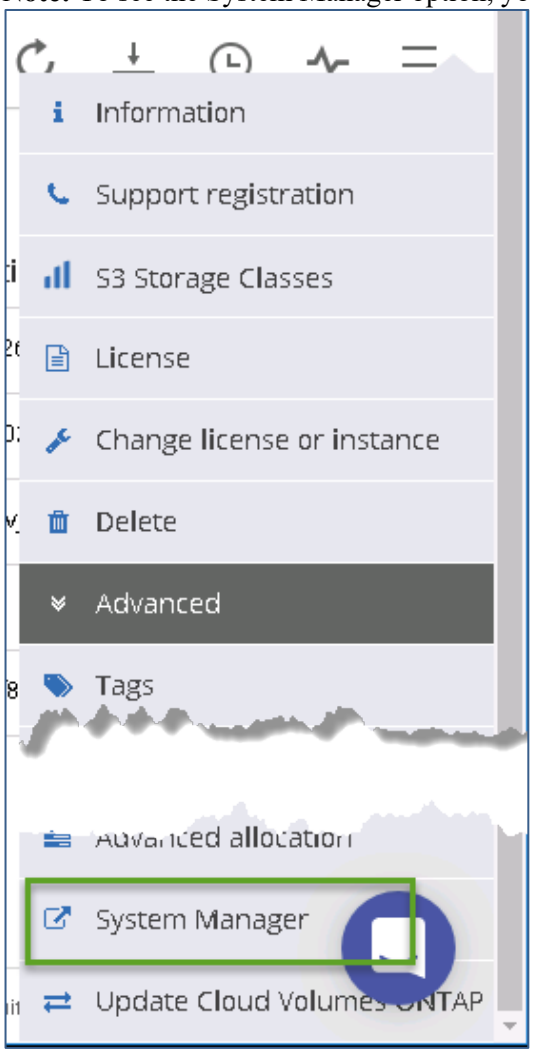
Step	Action
2-14	On the Licensing page, configure the following information: 1. Click **Change Version**, and select **ONTAP-9.5** from the list. 2. Click **Cloud Volumes ONTAP Standard**. 3. Select instance type **m4.2xlarge** 
2-15	Click **Continue**.
2-16	On the NetApp Support site credentials page, leave all the fields blank.
2-17	Click **Continue**.
2-18	On the Underlying Storage Resources page, select **General Purpose SSD** and AWS Disk Size as **100 GB**. 
2-19	Click **Continue**.

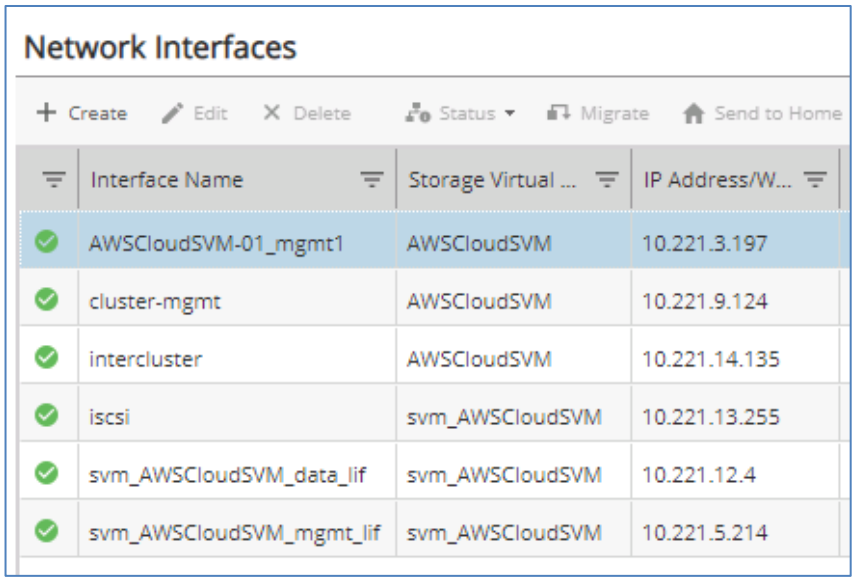
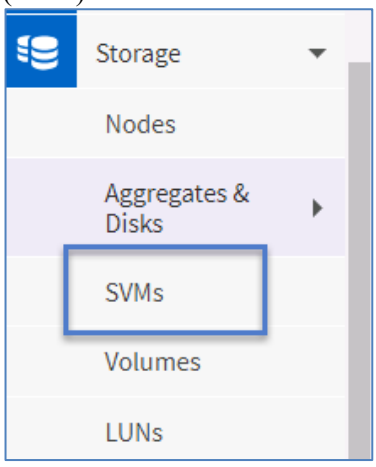
Step	Action
2-20	Complete the Write Speed & WORM page with the following: • For the Write Speed, select **Normal**. • For the WORM, select **Disable Worm**.
2-21	Click **Continue**.
2-22	On the Create Volume page, configure the following: • Volume name: **smb_vol1** • Volume size: **10** GB • Protocol: **CIFS Protocol** • Leave all other values as the defaults. 
2-23	Click **Continue**.
2-24	On the CIFS Setup page, enter the following values: • DNS Primary IP Address: **192.168.0.253** • Active Directory Domain to join: **demo.netapp.com** • Credentials authorized to join the domain: **administrator** and **Netapp1!** 

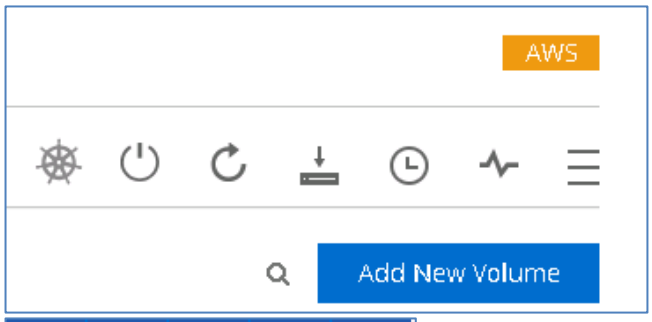
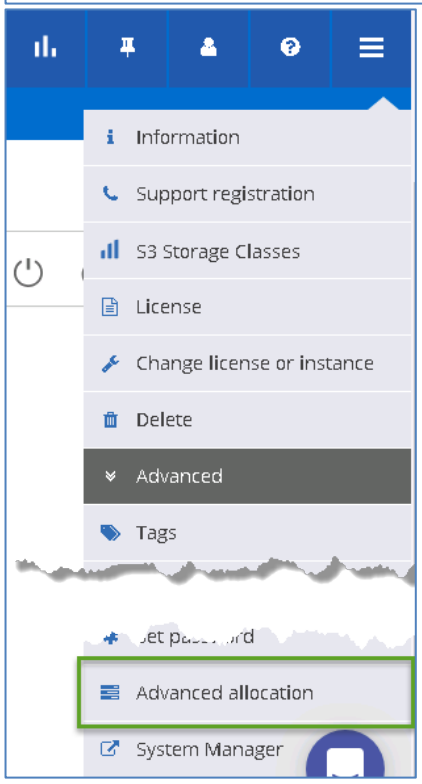
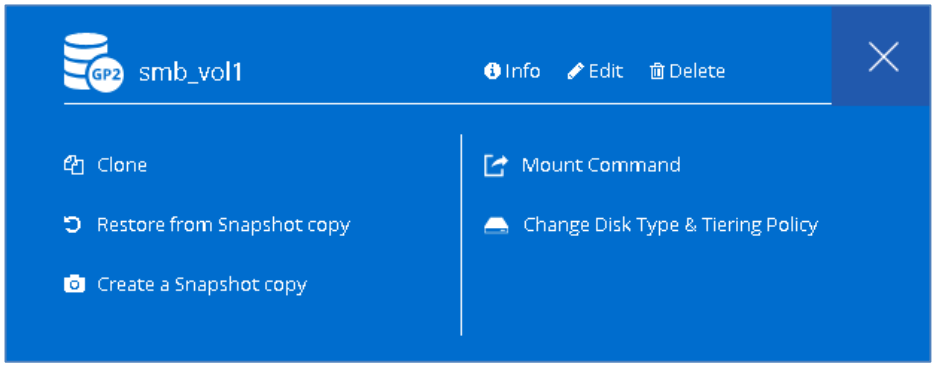
Step	Action
2-25	Click **Continue**.
2-26	On the Create Volume – Usage Profile, Disk Type & Tiering Policy page, select the **Volume Tiering Policy** menu and then select **None**. 
2-27	Click **Continue**.
2-28	On the Review & Approve page, review the information, and then complete the following actions: a. Select the checkbox that is labeled **I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp**. b. Select the checkbox that is labeled **I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements**. c. Next to the "I understand that Cloud Manager ..." text, click **More information**. 

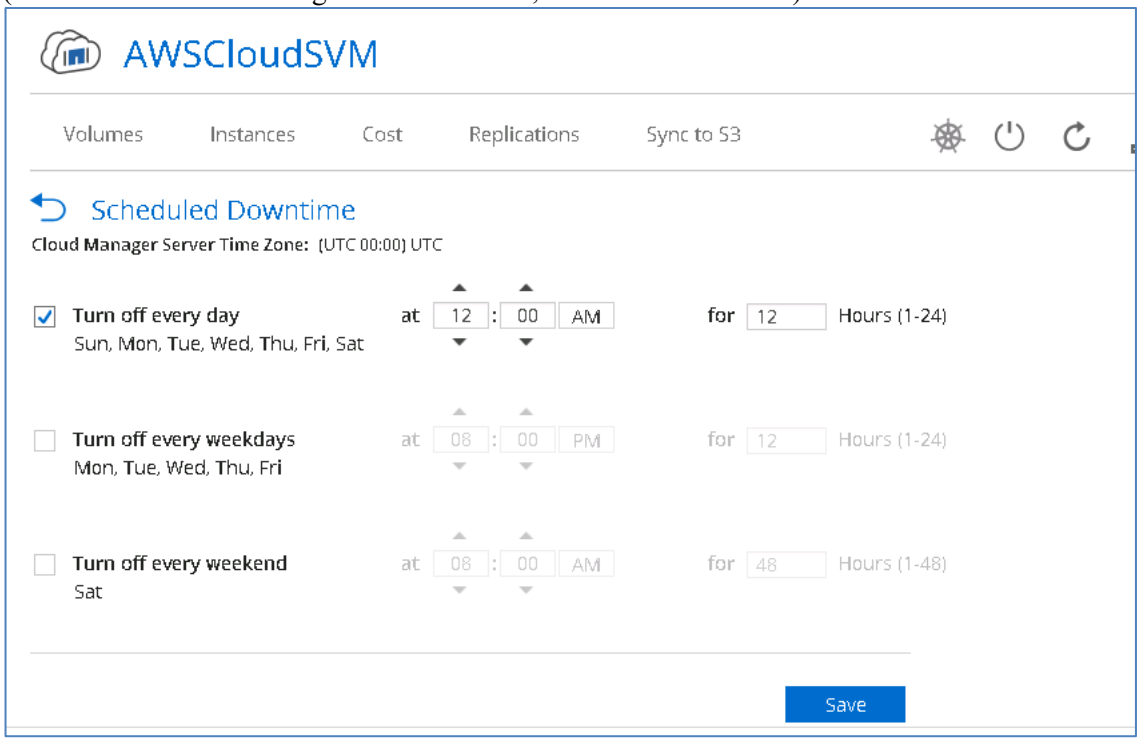
Step	Action
2-29	Review the AWS resources that are allocated, and click **Close**. 
2-30	Click **Go**.
2-31	You must wait while Cloud Volumes ONTAP initializes. Provisioning might take up to 25 minutes.
2-32	Click your new working environment. 
2-33	In the QUICK NAVIGATION section, select **Resources**. 

Step	Action
2-34	On the working environment page, click the menu icon, and then select **Information** to show the configuration details. 
2-35	Record the Cluster Management IP address: _____ 

Step	Action
2-36	Click the working environment menu icon, and then select **Advanced** > **System Manager**. **Note:** To see the System Manager option, you need to expand the Advanced menu selection. 
2-37	Click **Launch**.
2-38	Log in to OnCommand System Manager with the following Cloud Volumes ONTAP credentials: • User name: **admin** • Password: **Netapp1!**

Step	Action
2-39	View the network interfaces for Cloud Volumes ONTAP, and in the System Manager toolbar, select **Network** > **Network Interfaces**. 
2-40	In the System Manager toolbar, select **Storage** > **SVMs** and explore the storage virtual machine (SVM) that was created. 

Step	Action
2-41	Return to Cloud Manager to explore the following features: • Create an NFS volume. • Add disks to the Cloud Volumes ONTAP data aggregate. • Review the commands that are available on a volume.   
2-42	In the Working Environment toolbar, click the clock icon. 

Step	Action
2-43	Set the AWSCloudSVM cluster to power off every night at 7 p.m. EST. (You see that Cloud Manager time is in UTC, and EST is UTC – 5.) 

End of Exercise

Module 4: Implementing Disaster Recovery by Using NetApp Cloud Volumes ONTAP

Exercise 1: Configure and Manage Disaster Recovery in the Data Fabric

In this exercise, you use OnCommand Cloud Manager to set up and manage SnapMirror relationships. You also use Cloud Manager to perform a hybrid-cloud disaster recovery.

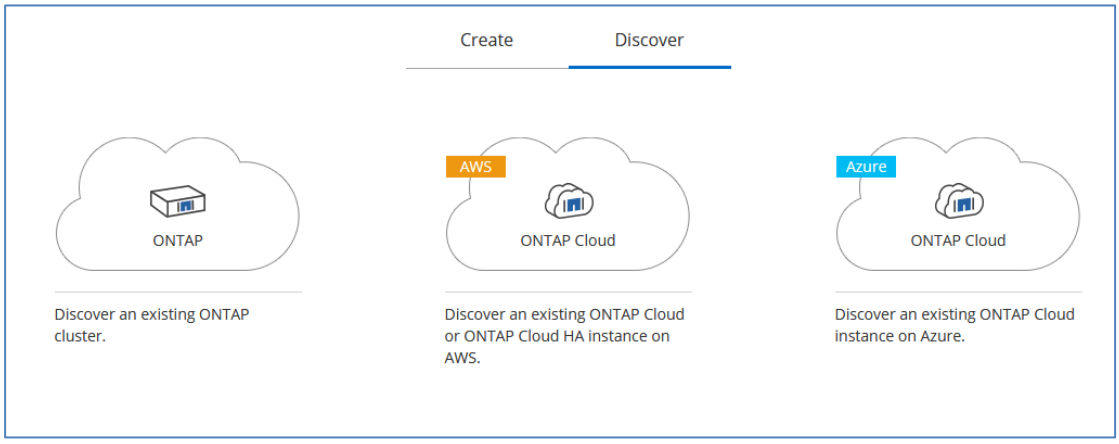
Objectives

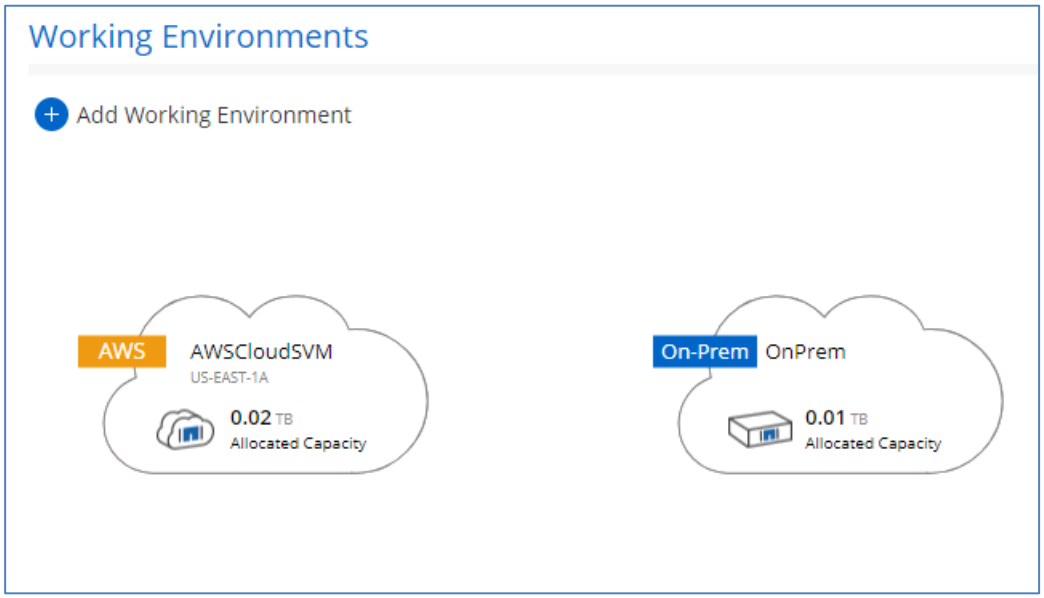
This exercise focuses on enabling you to do the following:

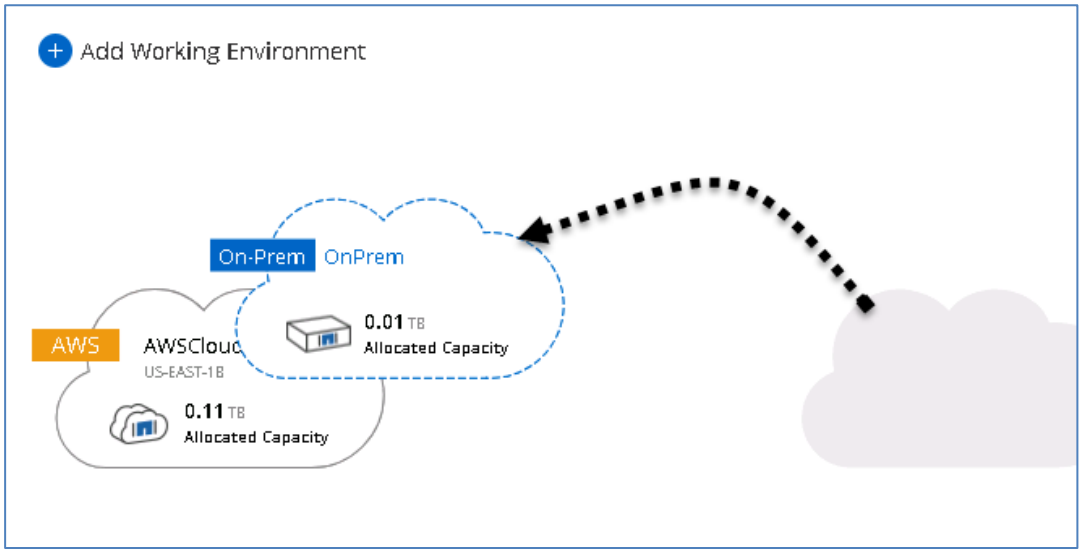
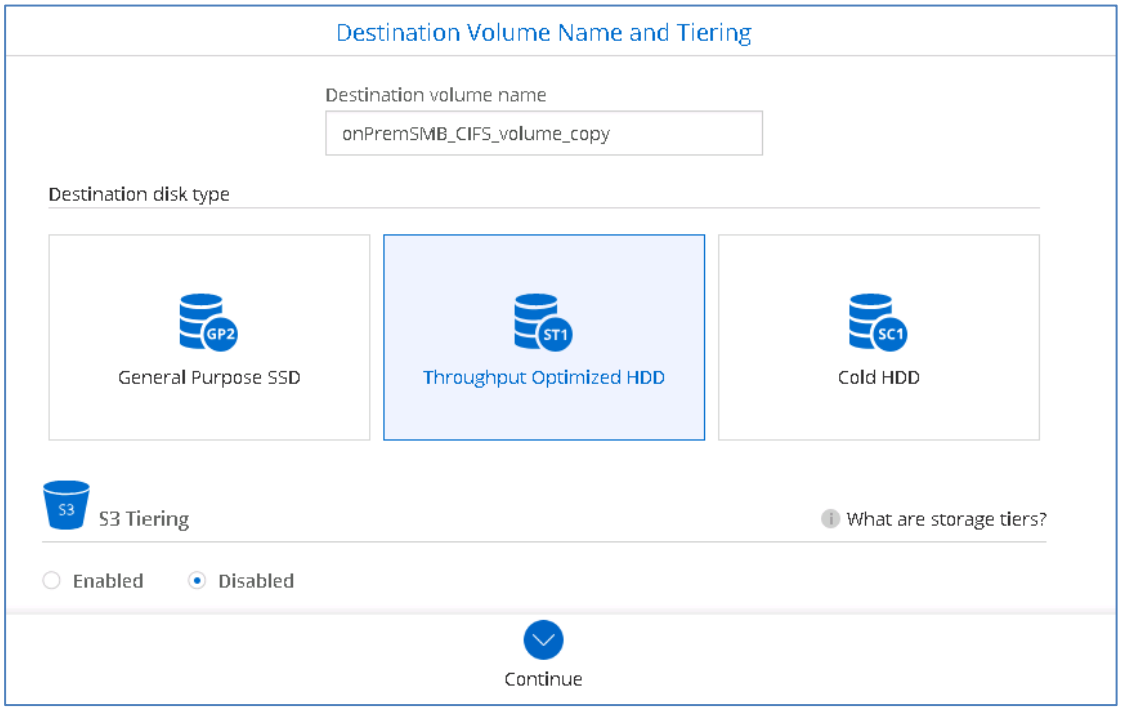
- Use Cloud Manager to implement hybrid-cloud SnapMirror relationships
- Perform a hybrid-cloud disaster recovery

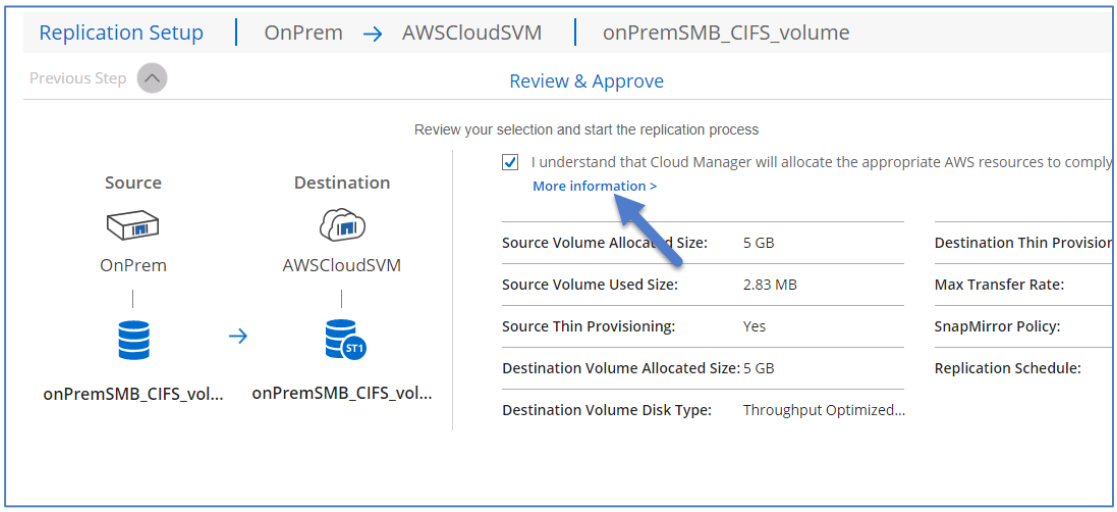
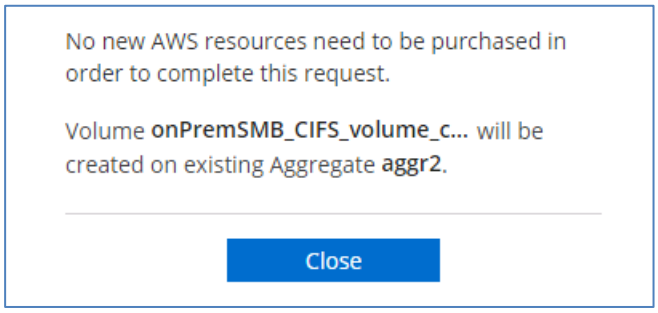
Task 1: Configure Replications Between On-Premises and Cloud

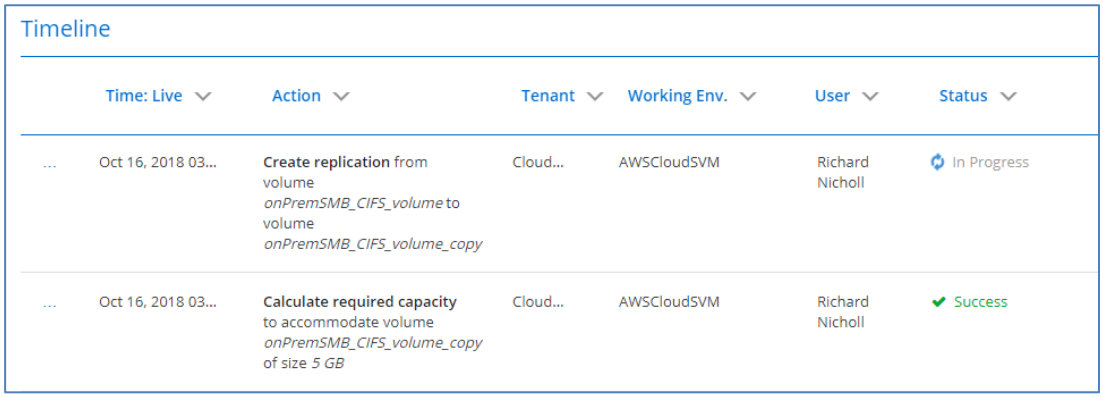
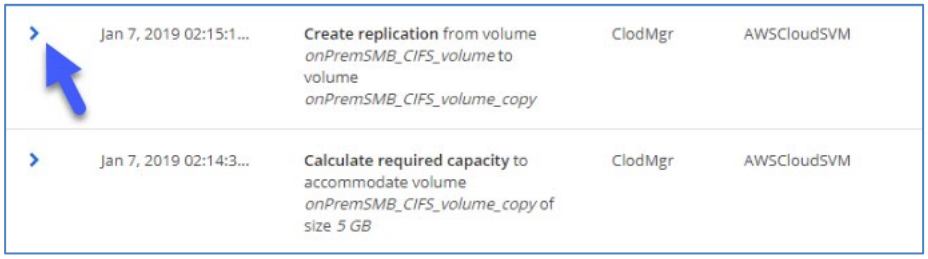
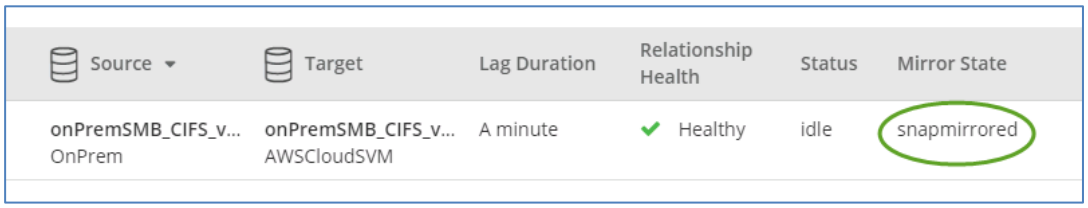
In this task, you use Cloud Manager to set up and manage SnapMirror relationships.

Step	Action
1-1	Copy files from the CourseFiles folder to the on-premises cluster: a. On the jump host, open the CourseFiles folder. b. Copy the file File_500M to the share onPremSMB (a shortcut is on the desktop).
1-2	Return to Cloud Manager.
1-3	If you need to log in, use the following information: • Email Address: <*email account that you used for Cloud Central*> eg. rt###@demo.netapp.com • Password: <*password that you used for Cloud Central*>
1-4	Click + **Add Working Environment**.
1-5	Click the **Discover** tab. 
1-6	Click **ONTAP (Discover an existing ONTAP cluster.)**

Step	Action
1-7	On the ONTAP Cluster Details page, enter the following information: • Cluster management IP address: **192.168.0.40** • User name: **admin** • Password: **Netapp1!** • Work Environment Type: **On-Premises**
1-8	If the lab environment is a NetApp Private Storage (NPS) deployment, you select NPS – connected to AWS.
1-9	Click **Continue**.
1-10	Click **Go**.
1-11	Verify that you now have two working environments. 
1-12	In the OnPrem cluster, use System Manager (or the CLI) to verify that no cluster peer relationships exist. CLI command: `cluster peer show`
1-13	The class OnPrem cluster does have an intercluster LIF. You need an intercluster LIF to exist on the OnPrem cluster, or you receive an error message in the next step. CLI command to verify the existence of intercluster LIF: `net int show -role intercluster`

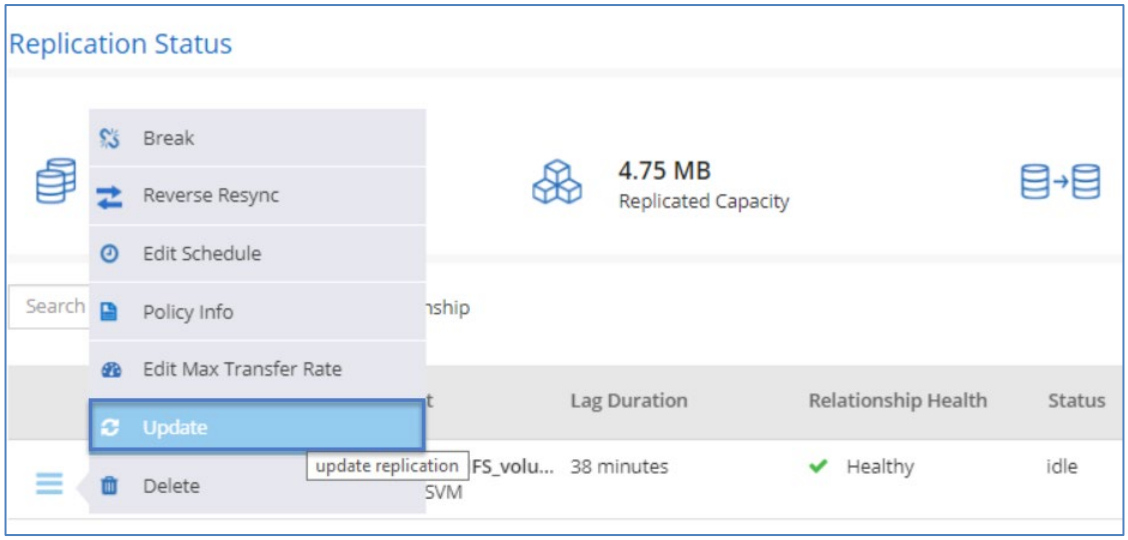
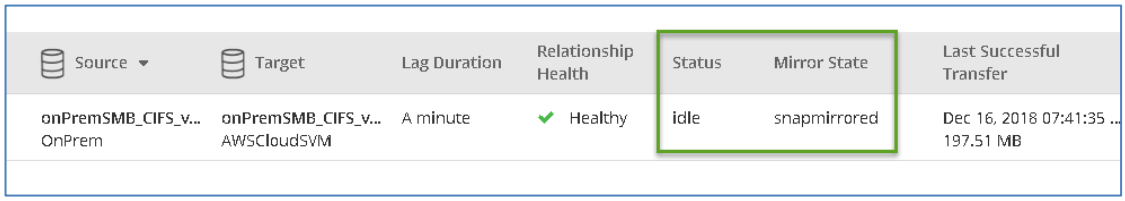
Step	Action
1-14	Return to Cloud Manager, and then drag the **OnPrem** cloud to the AWSCloudSVM cloud. 
1-15	On the Source Volume Selection page, select **onPremSMB_CIFS_volume**, and then click **Continue**.
1-16	On the Destination Volume and Tiering page, do the following: • Leave the default Destination volume name. • For the Destination Disk type, select **Throughput Optimized HDD**. • For the S3 tiering, select **Disabled**. 
1-17	Click **Continue**.
1-18	On the Max Transfer Rate page, leave the defaults and click **Continue**.

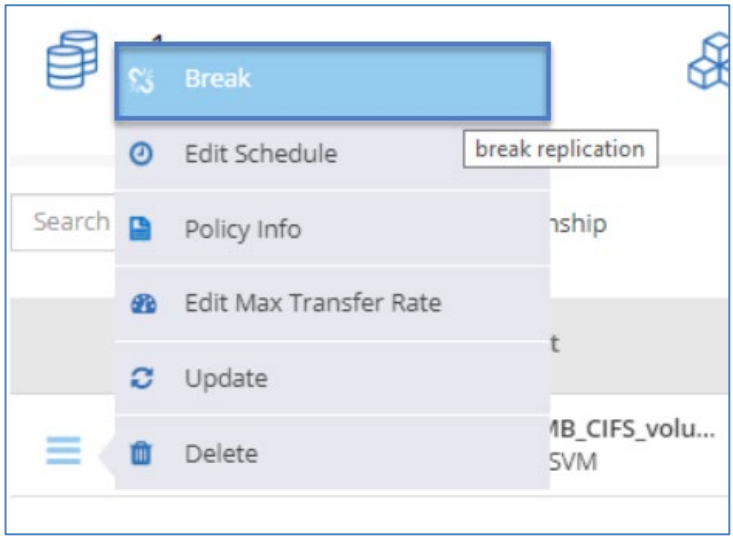
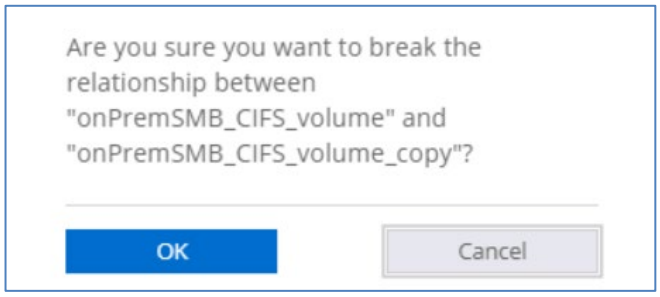
Step	Action
1-19	On the Replication Policy page, click **Mirror**.
1-20	On the Schedule page, click **hourly**.
1-21	On the Review page, review the information, and then do the following: a. Select the checkbox that is labeled **I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements**. b. Click **More information**. 
1-22	Review the AWS resources that are allocated for this request. In this case, no new AWS resources are needed because the existing aggregate on Cloud Volumes ONTAP is used. 
1-23	Click **Close**.
1-24	Click **Go**.

Step	Action
1-25	Click **Timeline** to view the replication progress. 
1-26	To view low-level details of a task, click on any of the columns within a row to expand. 
1-27	Click the **Replication Status** tab, and then verify that replication is finished. 
1-28	In the OnPrem cluster, use System Manager (or the CLI) to verify that a cluster peer relationship exists.

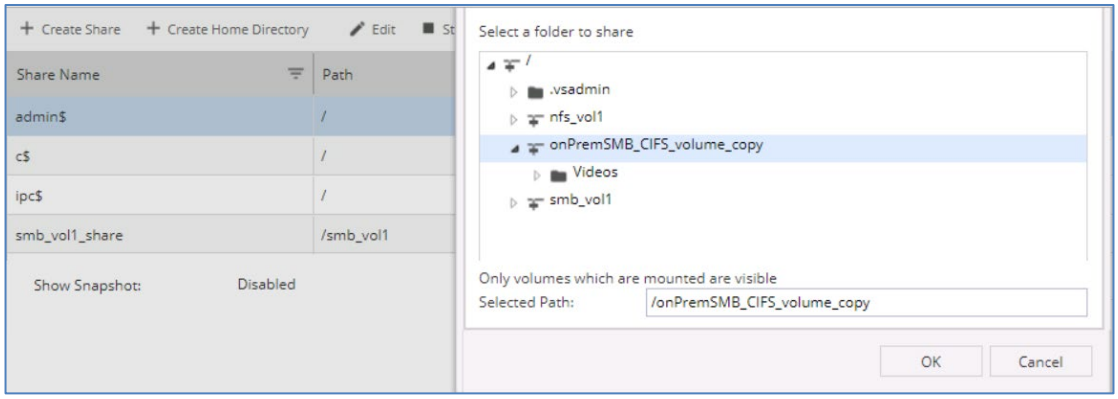
Task 2: Simulate Disaster Recovery

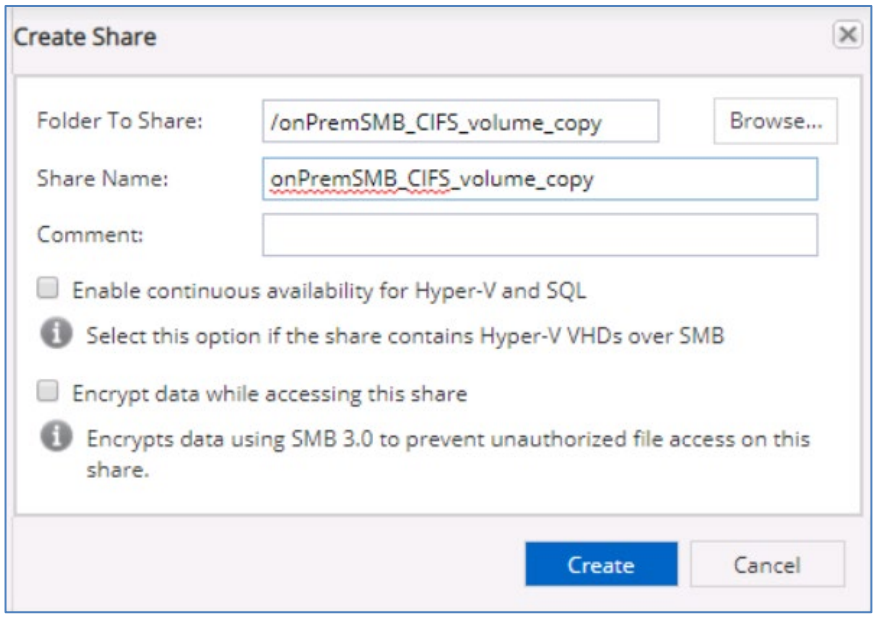
In this task, you verify that you can use the jump host or an Amazon Elastic Compute Cloud (Amazon EC2) virtual machine (VM) to access SnapMirror data on the Cloud Volumes ONTAP instance.

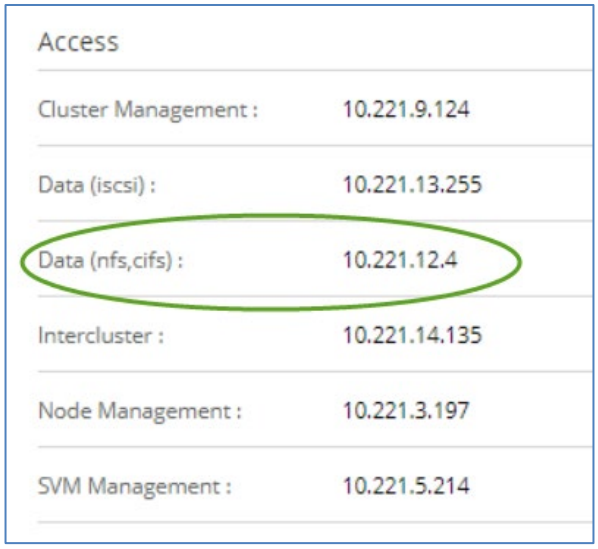
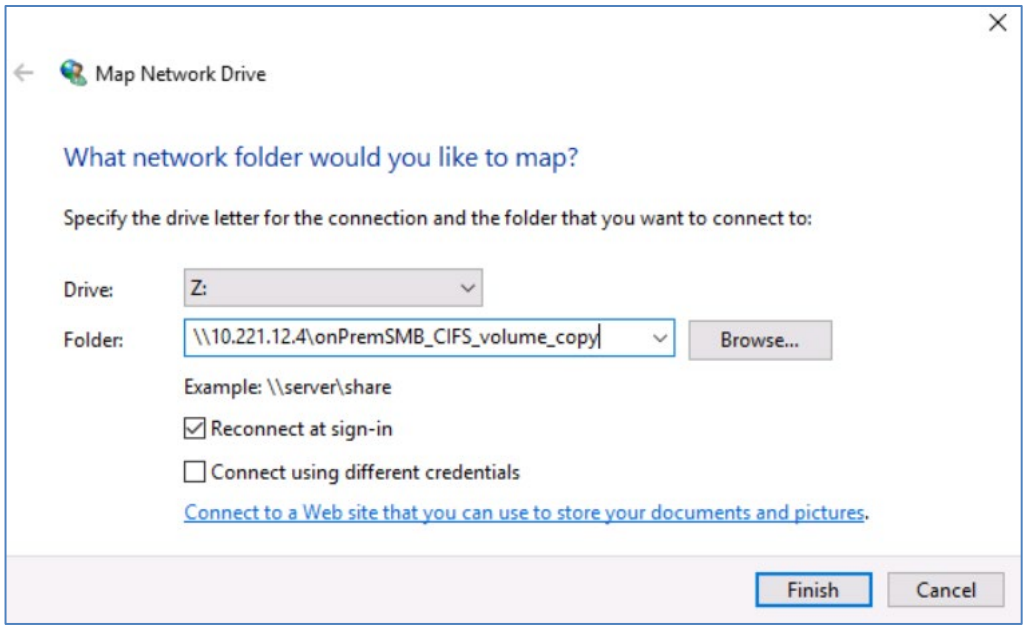
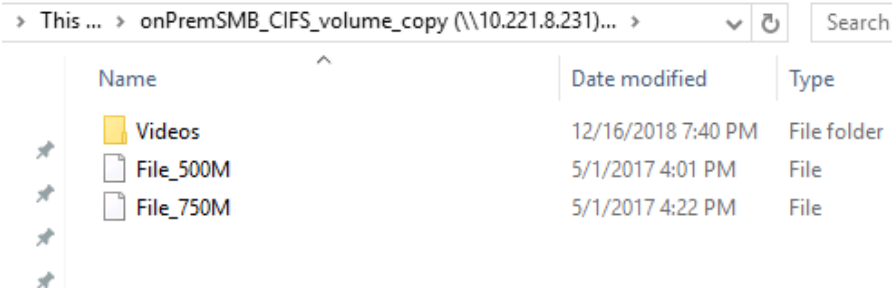
Step	Action
2-1	Copy files from the CourseFiles folder to the on-premises cluster: a. On the jump host, open the CourseFiles folder. b. Copy the file File_750M and the Videos folder to the share onPremSMB (a shortcut is on the desktop).
2-2	Use Cloud Manager to perform a manual update of the SnapMirror relationship. 
2-3	Wait for the Status to become Idle and the Mirror State to become snapmirrored. 
2-4	In this scenario, you imagine that something catastrophic has occurred in the OnPrem data center, and you need to access the data from the Windows Server instance in the cloud.

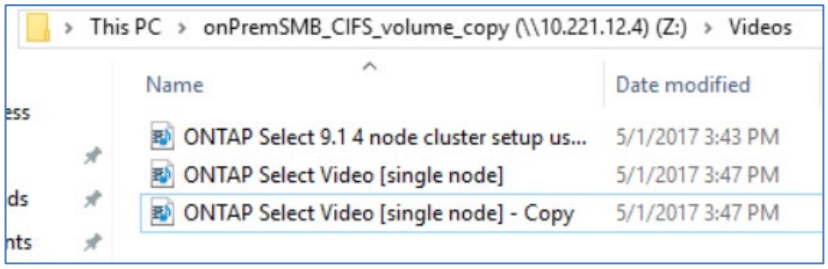
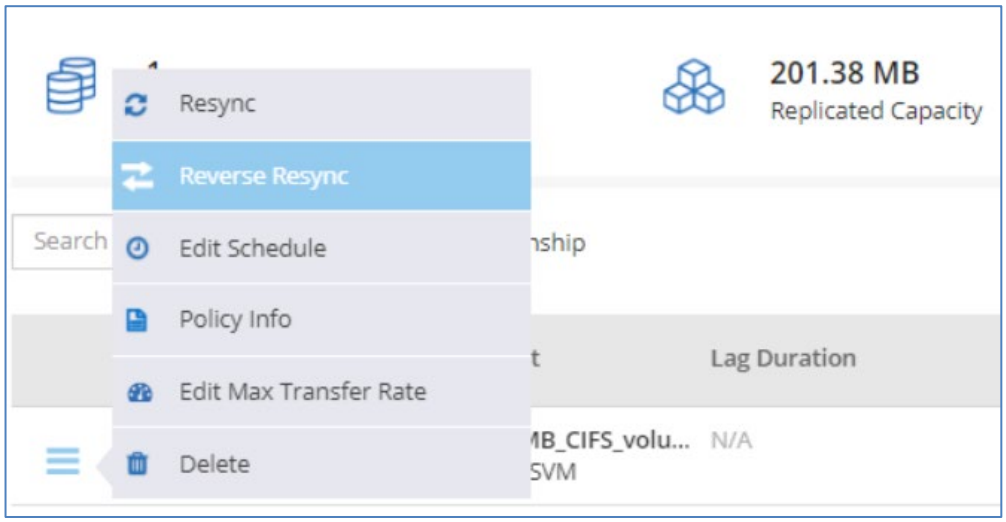
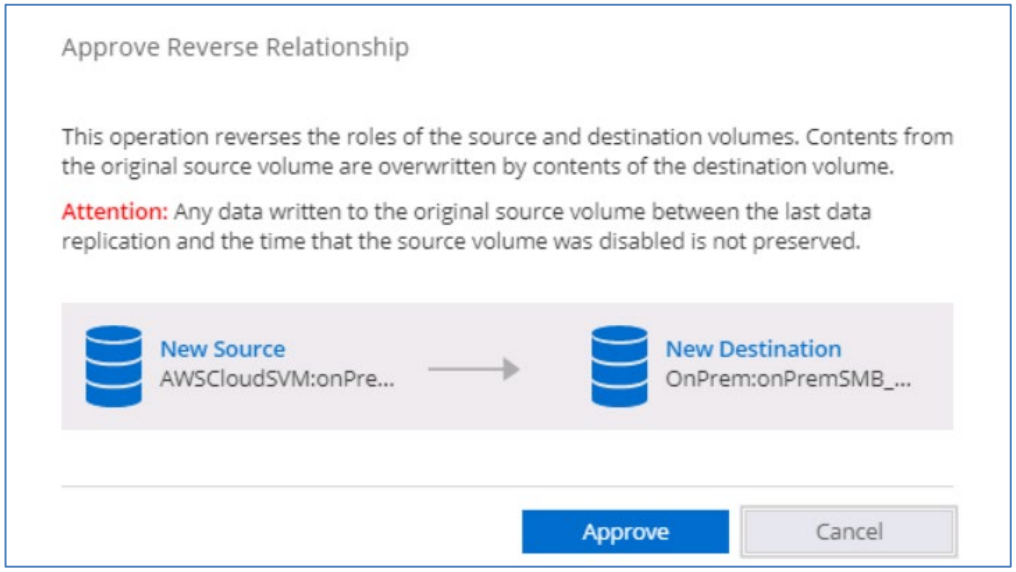
Step	Action
2-5	To start, break the SnapMirror relationship. 
2-6	Click **OK**. 
2-7	Log in to your Public_W2K16 Windows Server by using the public or private IP address of the server.
2-8	The login information and password are saved in the CourseFiles folder, in the Public_W2K16_Login.txt file.

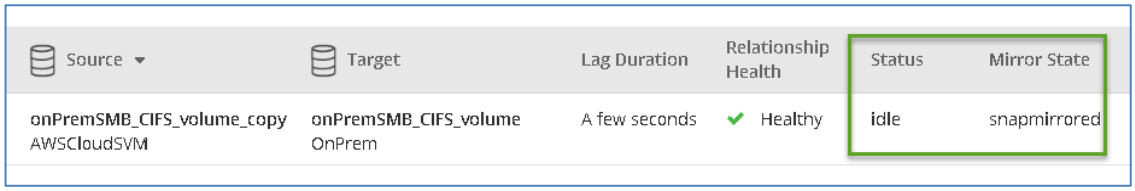
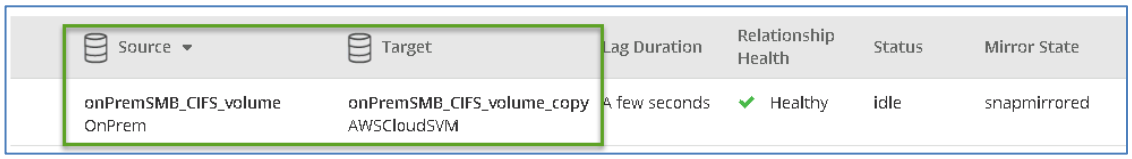
Step	Action
2-9	Using System Manager for **svm_AWSCloudSVM**, create a share for the copy so that you can access the data.





Step	Action
2-10	On the Public_W2K16 host, map a network drive to the onPremSMB share (the onPremSMB_CIFS_volume_copy on the AWS storage virtual machine [SVM]).  
2-11	Verify that you can see the data and write data to the folders. 

Step	Action
2-12	Copy a video file. 
2-13	Now, you imagine that the data center has been recovered, and you want to transfer all new data back to the OnPrem cluster.
2-14	Use Cloud Manager to reverse the SnapMirror relationship by selecting **Reverse Resync**. 
2-15	Click **Approve**. 

Step	Action
2-16	Wait for the Status to become Idle and the Mirror State to become snapmirrored. 
2-17	Verify that the new data (the copy of the video file) that you wrote to the SMB share copy is visible on the onPremSMB share on your jump host.
2-18	Re-create the original SnapMirror relationship direction. (Hint: You do another Reverse Resync).
2-19	Verify that onPremSMB_CIFS_volume is again the Source of the SnapMirror relationship. 

End of Exercise

Module 5: Azure Virtual Network and Connectivity

Exercise 1: Configuring Azure Virtual Network to On-Premises VPN Connectivity

In this exercise, you create a Microsoft Azure Virtual Network (VNet) and subnets that can host virtual machines (VMs). You also set up an VNet gateway. You use this gateway to configure a VPN Internet Protocol security (IPsec) connection between Azure and the on-premises data center. The data center connection is made with a pfSense virtual router.

Objectives

This exercise focuses on enabling you to do the following:

- Use Windows PowerShell to configure Azure resources
- Create and configure VNet resources
- Connect the VNet to a customer gateway through a VNet gateway

Task 1: Create VNet Resources

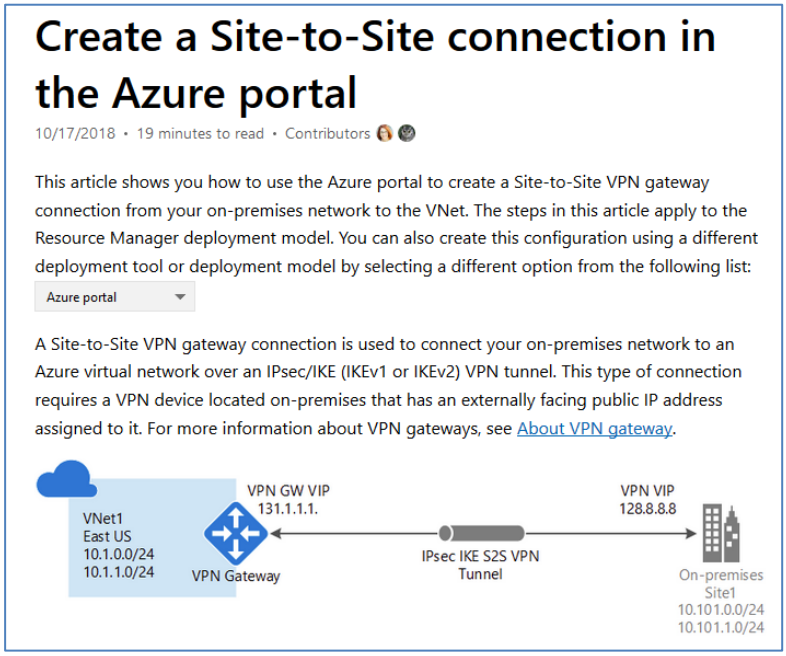
In this task, you create a VNet. You also create two subnets: one private subnet and one gateway subnet. The gateway subnet is a small network that Azure requires for use as a gateway zone for the VPN connection. You also create a local network gateway to connect to the customer gateway (the on-premises data center).

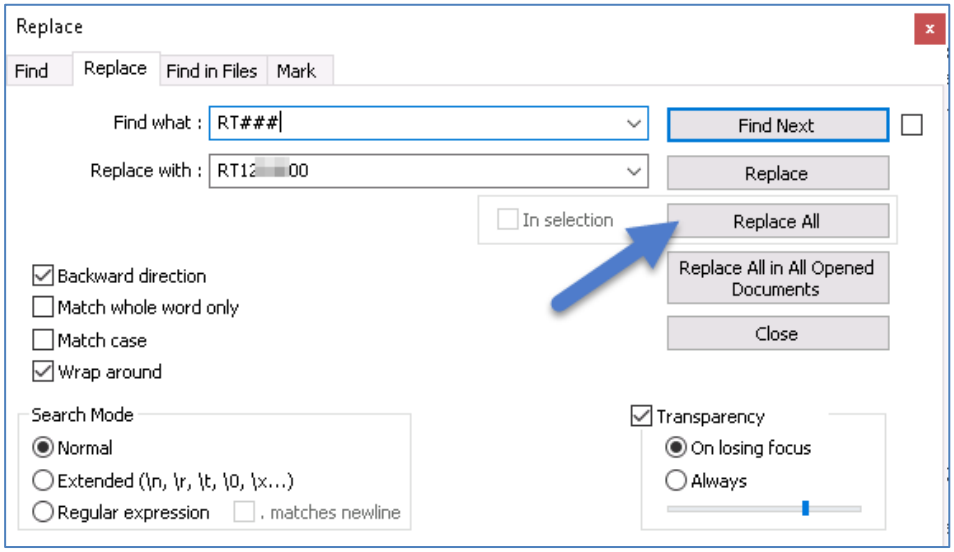
Step	Action
1-1	On your jump host, open a Windows PowerShell window.

1-2	Log in to the Azure Resource Management account:
	a. Enter the **`Login-AzureRmAccount`** command.
	• For email, enter the Azure user name (email) from azurelogin.txt.
	• If you are asked for the account type, select **Personal**.
	• For password, enter the password that you created when you unlocked your Azure account.
	Sample output:
	`Environment : AzureCloud`
	`Account : student@ngihcdurhamihcnetappu.onmicrosoft.com`
	`TenantId : 3927913f-473b-42a7-b302-d346f21f012e`
	`SubscriptionId : a23dc3ad-e613-43bd-8784-85ba05c0e94b`
	`SubscriptionName : Pay-As-You-Go`
	`CurrentStorageAccount :`

Step	Action

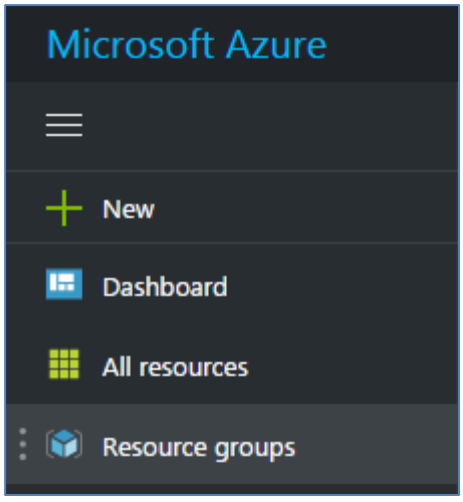
1-3	Get your Resource Group Name:
	`PS C:\Users\Administrator.DEMO> **Get-AzureRmResourceGroup**`
	Example Output:
	`ResourceGroupName : RT1224200`
	`Location : eastus`
	`ProvisioningState : Succeeded`
	`Tags :`
	`ResourceId : /subscriptions/fe09285f-3668-4ac2-9222cc13edf9c959/resourceGroups/RT1224200`

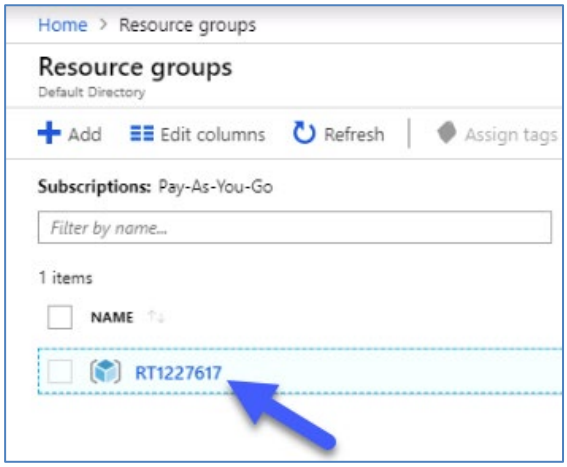
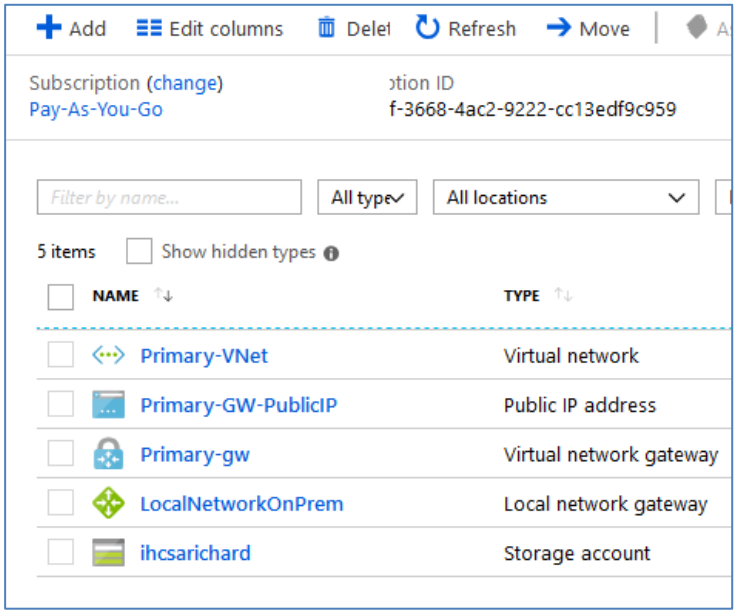
1-4	In the rest of this exercise you use Windows PowerShell commands to create a VNet and VPN connectivity. If you want to see how to configure VPN connectivity by using the Azure portal interface instead of Windows PowerShell, review the following URL: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal 
1-5	Using Notepad++, in the CourseFiles folder, open the file **Azure_PS_Cmds.txt**.
1-6	In Notepad++, select **Search** > **Replace.**

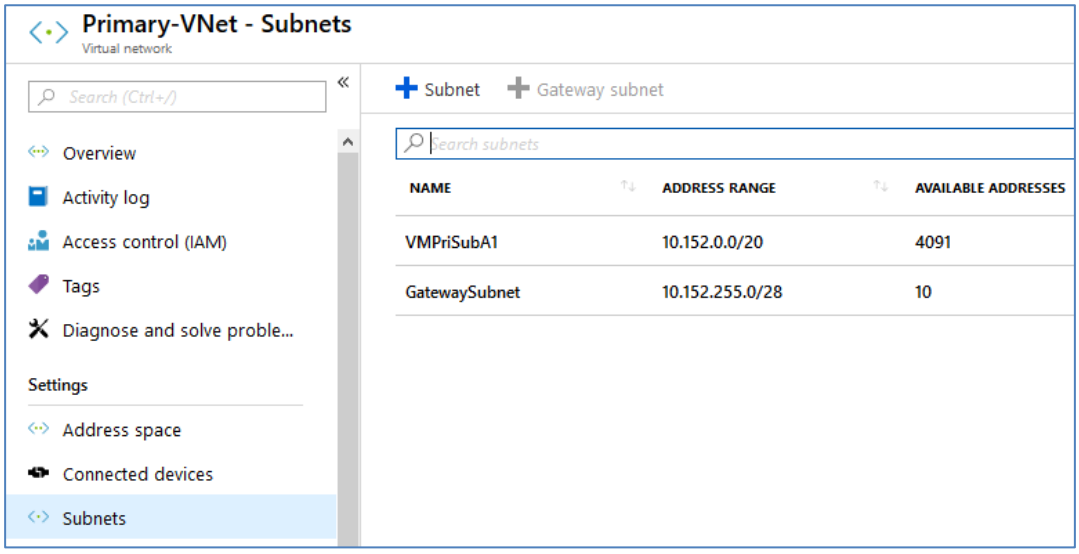
Step	Action
1-7	In the Replace window, do the following: • Find what: **RT###** • Replace with: *<Your-RG-Name>* • Click **Replace All**. 
1-8	Do another search to find and replace: • Find what: **yourIP** • Replace with: the local network gateway IP address that your instructor gave you
1-9	From section **A. Create VNets and Subnets**, copy and paste the commands into the Windows PowerShell.
1-10	Verify that the VNet creation succeeded. Note: The last command in section A should show an output like below. 

Step	Action
1-11	From section **B. Create Local Network Gateway**, copy and paste the commands into the Windows PowerShell.

1-12	Verify that the local network gateway creation succeeded.
	`Name : LocalNetworkOnPrem`
	`ResourceGroupName : DEV178`
	`Location : eastus`
	`Id : /subscriptions/fe09285f-3668-4ac`
	`Gateways/LocalNetworkOnPrem`
	`Etag : W/"e1e1e243-4ad6-4f90-ac10-87bda`
	`ResourceGuid : 141ce889-159b-4a28-8983-401cd7f7`
	`ProvisioningState : Succeeded`
	`Tags :`
	`GatewayIpAddress : 216.240.31.145`
	`LocalNetworkAddressSpace : {`
	`"AddressPrefixes": [`
	`"192.168.0.0/24"`
	`]`

1-13	Open a web browser to http://portal.azure.com.
1-14	Enter your assigned user name. Note: you can find the username in the azurelogin.txt file on the desktop.
1-15	Enter your password.
1-16	In the Microsoft Azure panel, click **Resource groups** to view the resources that you have created so far. 

Step	Action
1-17	Click **RT###**. 
1-18	Click **Primary-VNet**. 

Step	Action
1-19	In the Primary-VNet dashboard, click **Subnets**, and then view the subnets in the VNet. 
1-20	Return to the RT### resource group, click the local network gateway **LocalNetworkOnPrem**, and then view the configuration. Note the IP address is here is the IP address of the on-premises network. Sample output: 

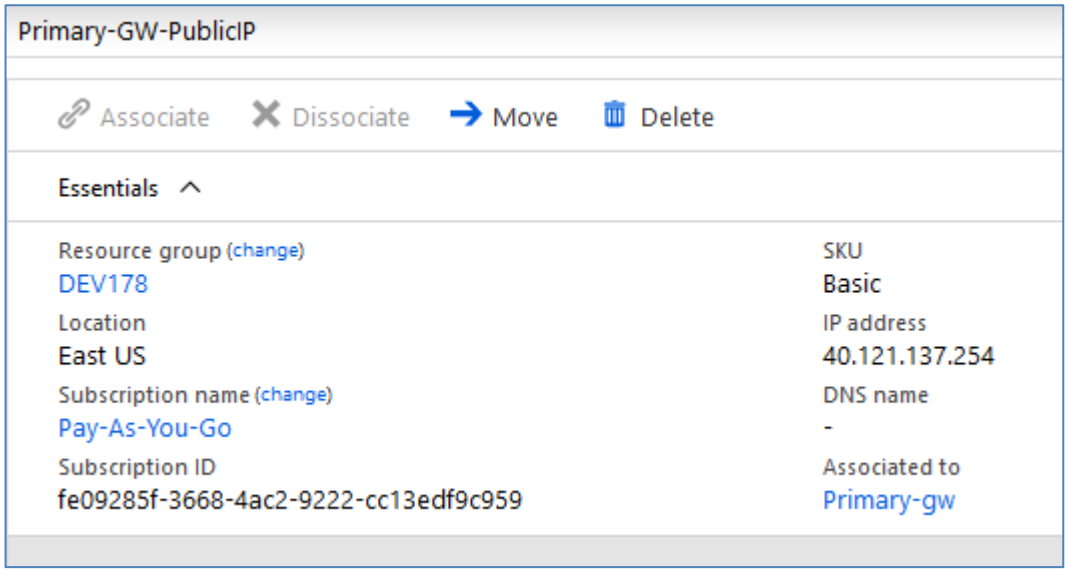
Task 2: Configure a VPN Connection

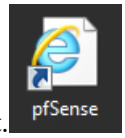
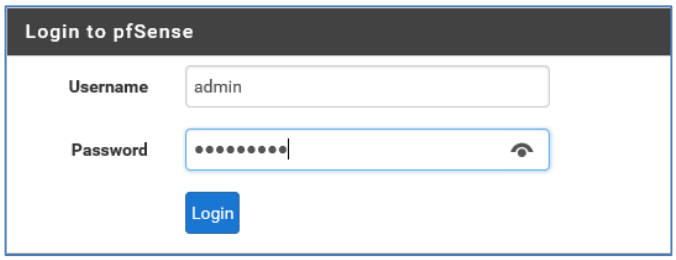
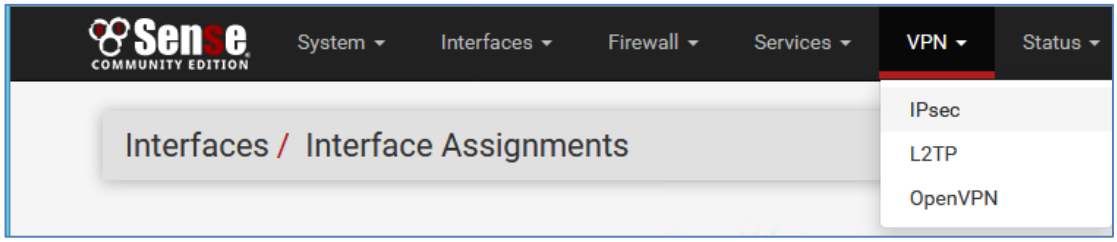
In this task, you set up a connection between Azure and the on-premises data center by using a VPN IPsec connection. You create and configure a VNet gateway, and then you create the VPN connection on the Azure side. Finally, you use pfSense in the on-premises data center to configure and initiate the VPN connection.

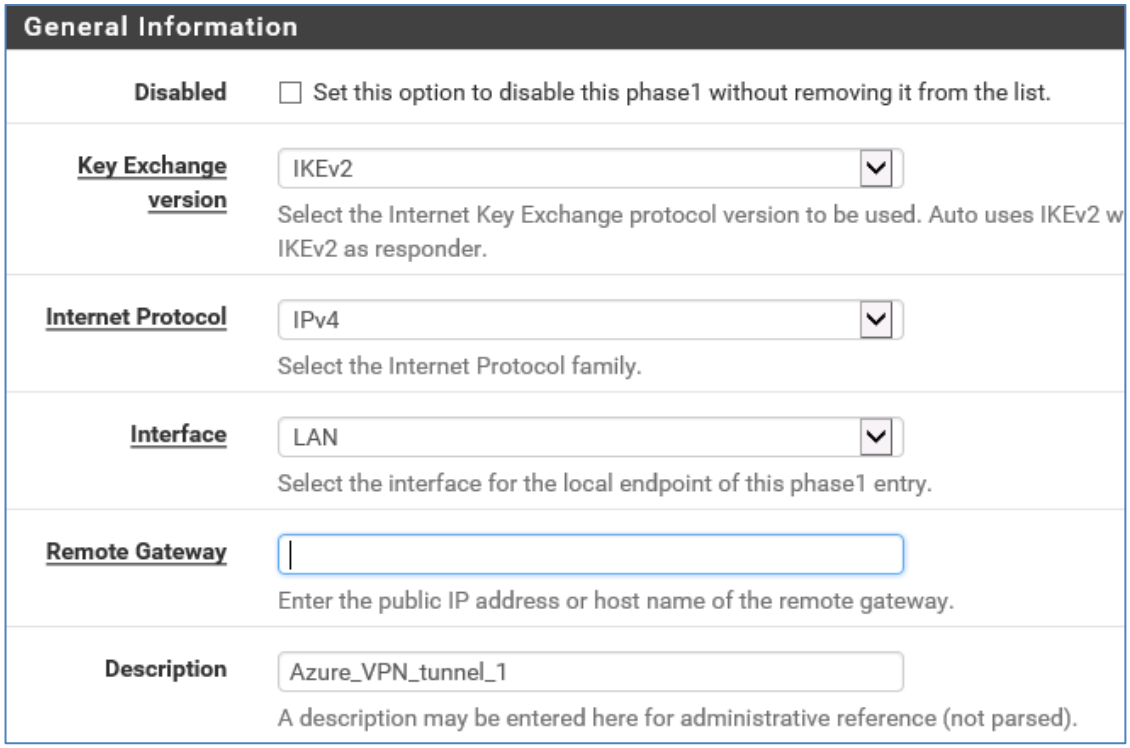
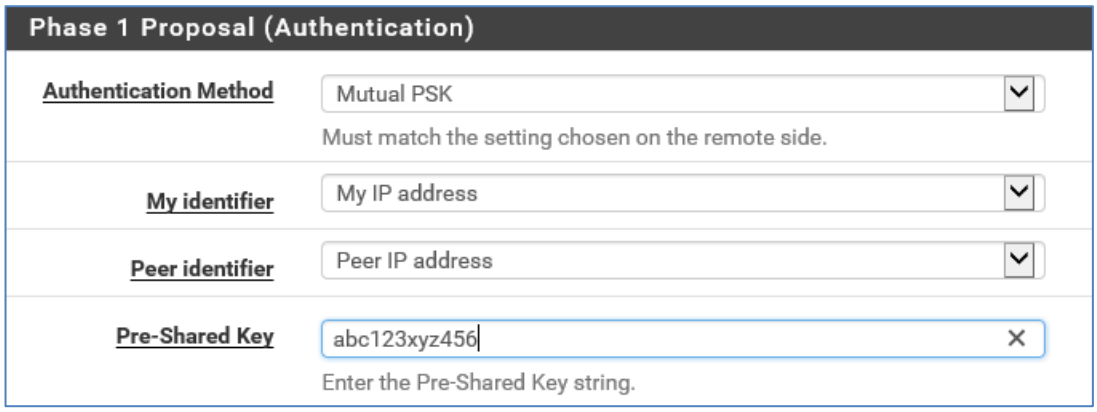
Step	Action

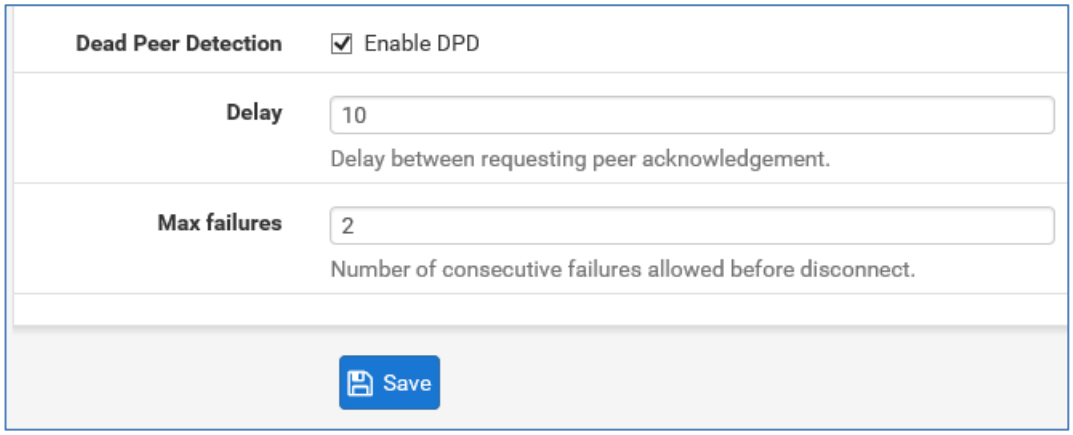
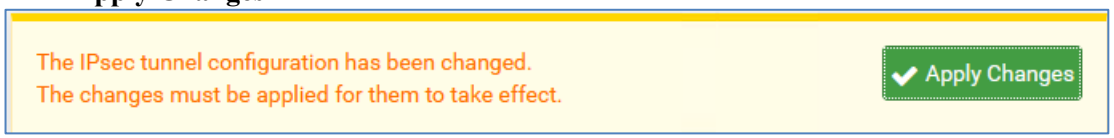
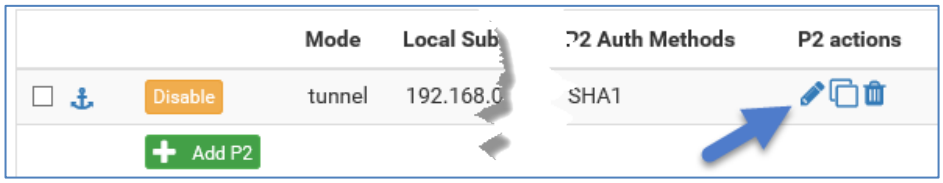
2-1	From section **C. Create VNet Gateway (VGW)**, copy and paste the commands into the Windows PowerShell.
	
	Note: The gateway-creation process might take up to 45 minutes. After the process is complete, you might need to press Enter in the Windows PowerShell window to see the results.
	
	Sample output:
	
	`Name : Primary-gw`
	`ResourceGroupName : DEV178`
	`Location : eastus`
	`Id : /subscriptions/fe09285f-3668-4ac2-9222-cc13ec`
	`Gateways/Primary-gw`
	`Etag : W/"02ac54a8-82c9-47b8-b4b7-f9461db54b64"`
	`ResourceGuid : 2e543d80-32b5-4287-bdd6-0a9d7b392b77`
	`ProvisioningState : Succeeded`
	`Tags :`
	`IpConfigurations : [`
	`{`
	`"PrivateIpAllocationMethod": "Dynamic",`
	`"Subnet": {`
	
	If

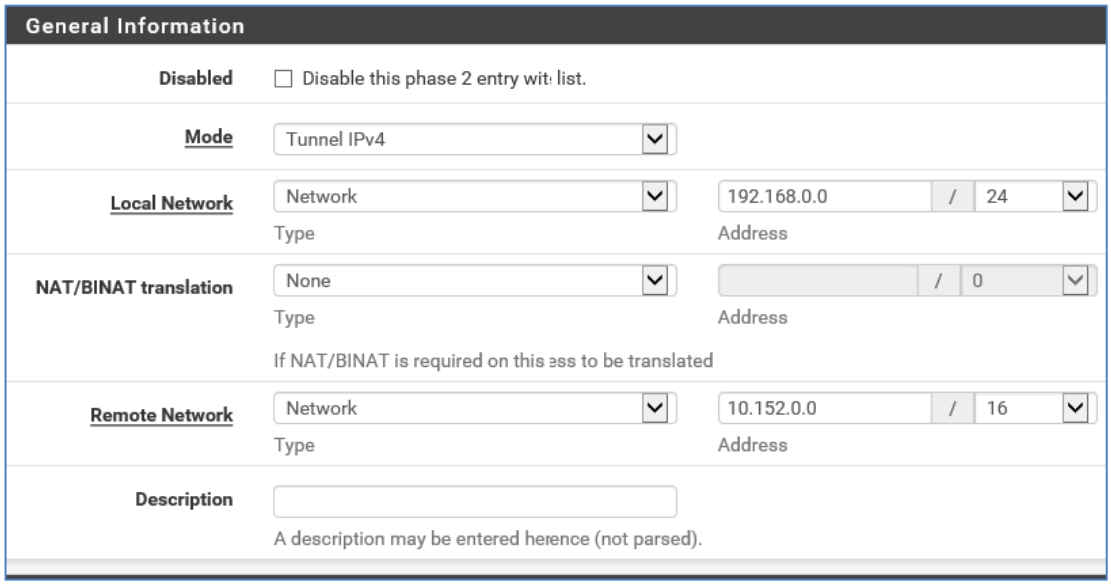
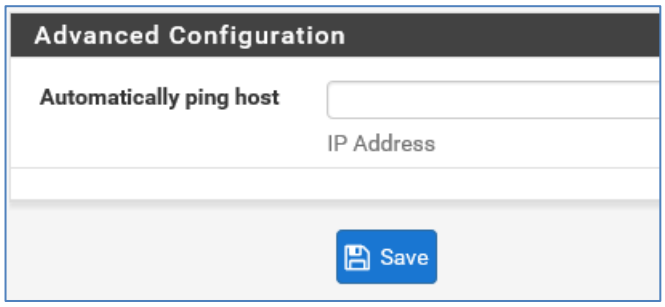
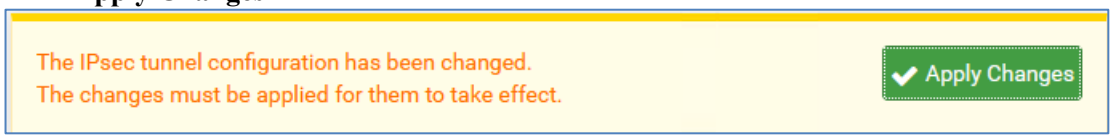
2-2	Review the commands that you issued: • You used the **`New-AzureRmPublicIpAddress`** command to request a public IP. • You then associated that IP address with the GatewaySubnet that you created when you created the Primary-VNet. • Finally, you requested a VNet gateway connection by using this information (public IP and GatewaySubnet) and by setting the gateway type to VPN.

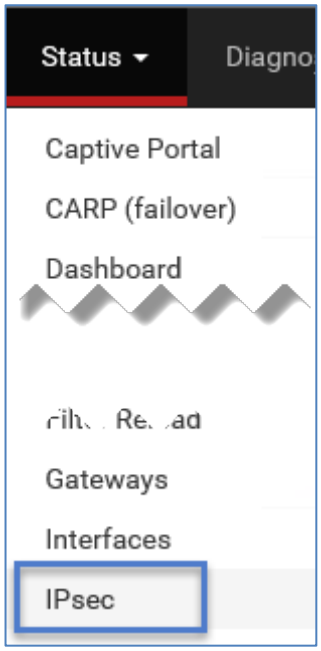
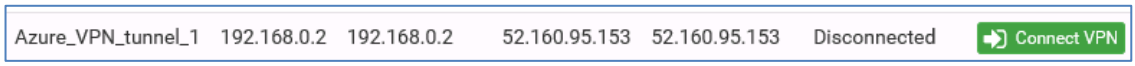
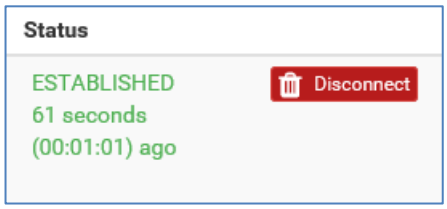
Step	Action
2-3	Return to the Azure portal RT### resource group, and then look at the Primary-GW-PublicIP. 
2-4	Record the public IP address, or save it in the Azure_connection_info.txt file in the CourseFiles folder: _____
2-5	From section **D. Create VPN Connection**, copy and paste the commands into the Windows PowerShell.
2-6	Verify that the VPN Connection is created. (The ConnectionStatus is “Unknown” or “Connecting” until the pfSense on-premises configuration is complete.) Name : VNet2OnPrem ResourceGroupName : DEV178 Location : eastus Id : /subscriptions/fe09285f-3668-4ac2-9222-c Net2OnPrem Etag : W/"757c266a-2ff1-4813-992b-3e8b6d5890dc" ResourceGuid : 27f1300f-49b3-470c-ad9d-b3c67c0454bf ProvisioningState : Succeeded Tags : AuthorizationKey : VirtualNetworkGateway1 : "/subscriptions/fe09285f-3668-4ac2-9222- rkGateways/Primary-gw" VirtualNetworkGateway2 : LocalNetworkGateway2 : "/subscriptions/fe09285f-3668-4ac2-9222- Gateways/LocalNetworkOnPrem" Peer : RoutingWeight : 10 SharedKey : abc123xyz456 ConnectionStatus : Unknown

Step	Action
2-7	For Shared Key, the value must match the value that you will use for your local on-premises VPN device ("abc123xyx456" in this exercise) during configuration. The value of the shared key itself is not important. The important information is that both the on-premises and Azure sides of the connection use the same value.
2-8	On your Windows Server jump host, double-click the **pfSense** shortcut. 
2-9	If a security warning appears, click **Continue to this website (not recommended)**.
2-10	Enter the following credentials: • User name: **admin** • Password: **Netapp1!** 
2-11	Select **VPN** > **IPsec**. 
2-12	In the Azure VPN Tunnel 1 entry, click the Edit icon. 

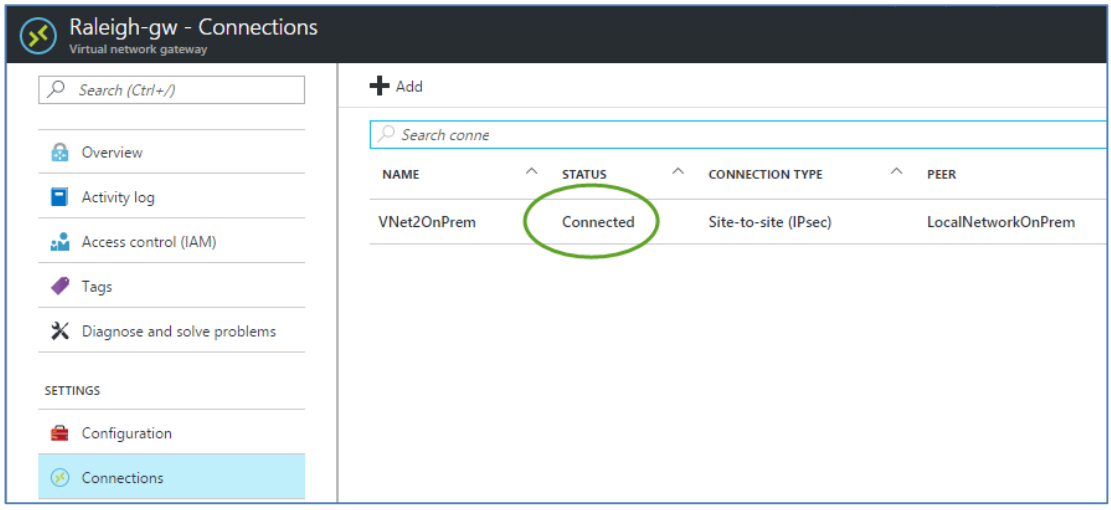
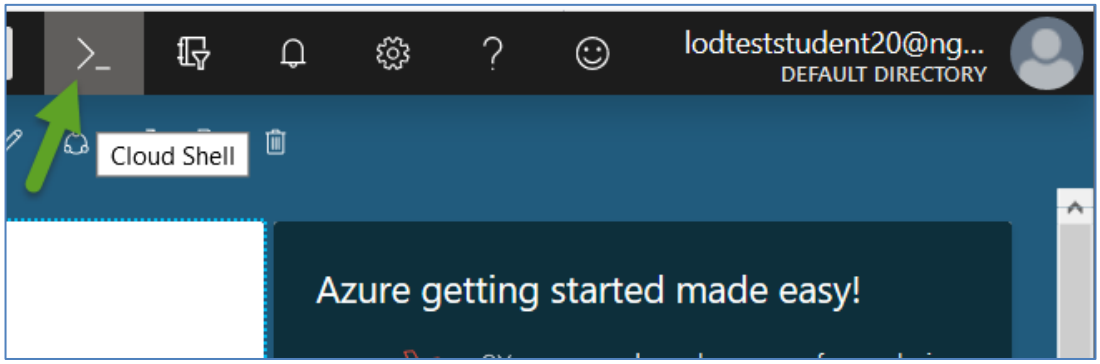
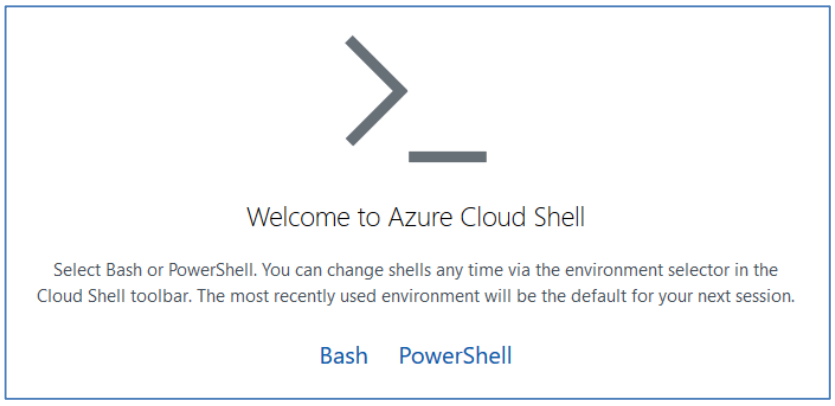
Step	Action
2-13	In the General Information section, in the Remote Gateway field, overwrite the value with the IP address that you recorded in Step 2-4. 
2-14	In the Phase 1 Proposal (Authentication) section, in the Pre-Shared Key field, overwrite the value with the value **abc123xyz456.** 

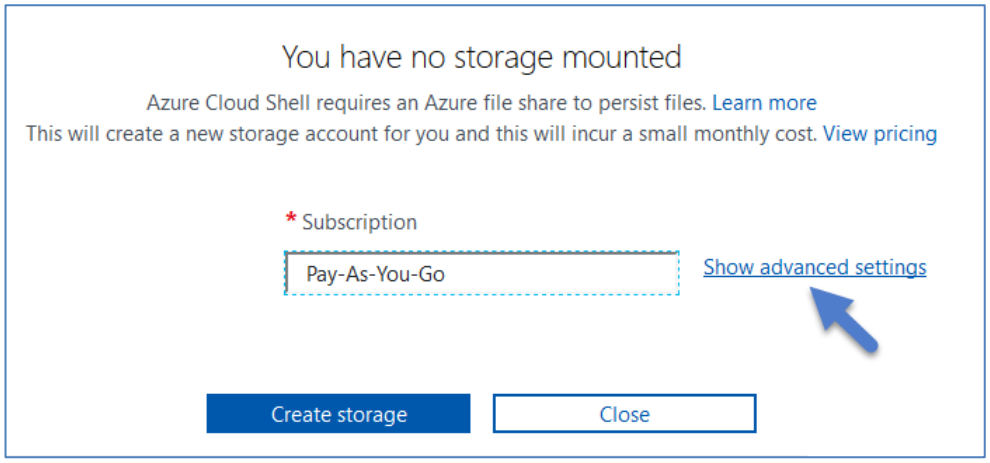
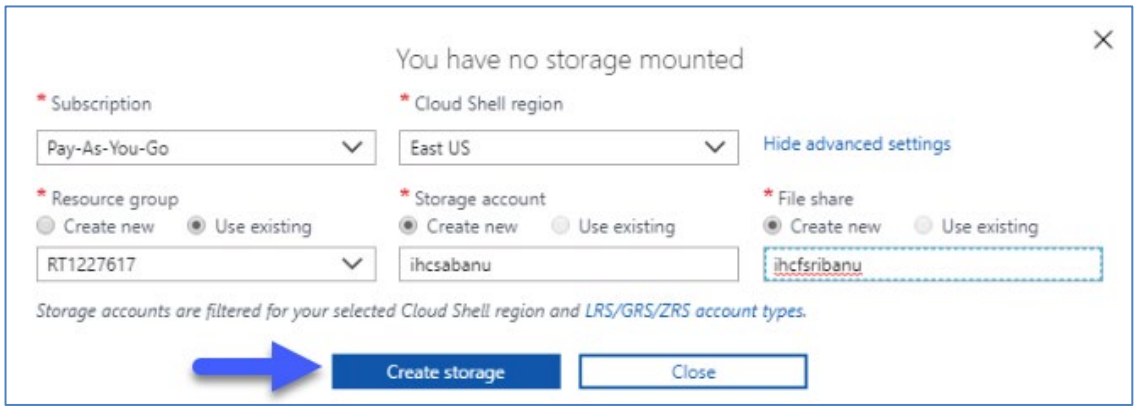
Step	Action
2-15	Accept all the other default values, scroll to bottom of the page, and then click **Save**. 
2-16	Click **Apply Changes**. 
2-17	For Azure VPN Tunnel 1, click **Show Phase 2 Entries (1)**. 
2-18	In the Phase2 entry, click the Edit icon. 

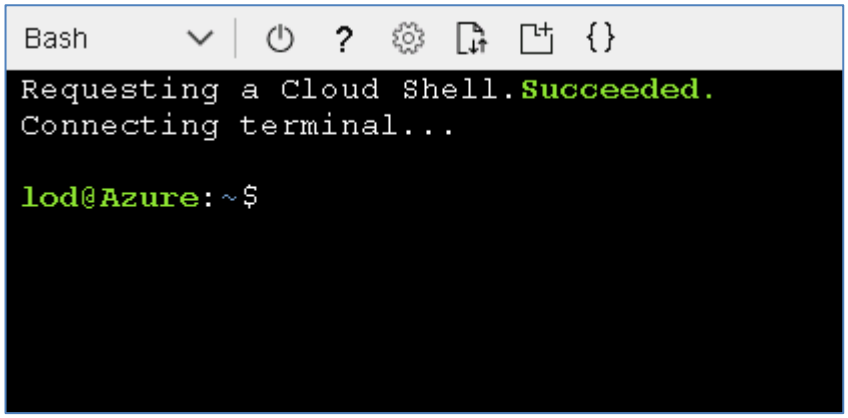
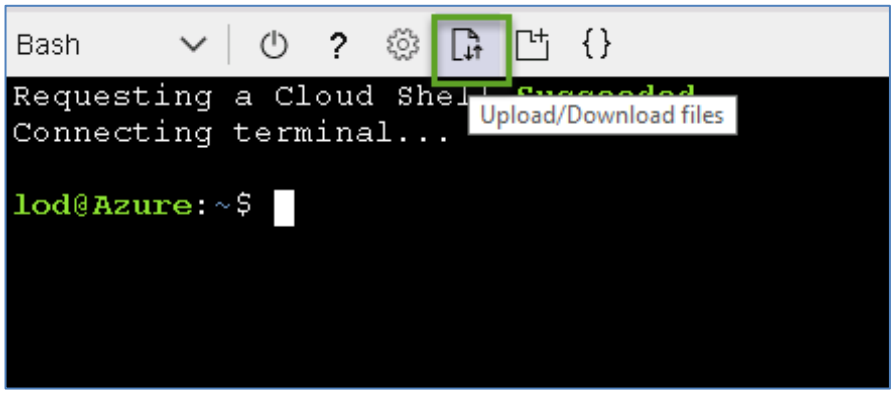
Step	Action
2-19	In the General Information section, enter the specified values in place of the defaults in the following fields: • Local Network: **192.168.0.0/24** • Remote Network: **10.152.0.0/16** 
2-20	Accept all other default values, scroll to bottom of the page, and then click **Save**. 
2-21	Click **Apply Changes**. 

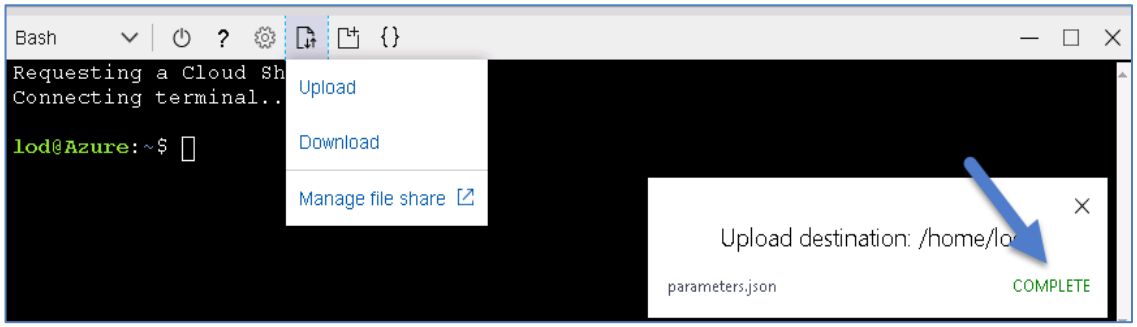
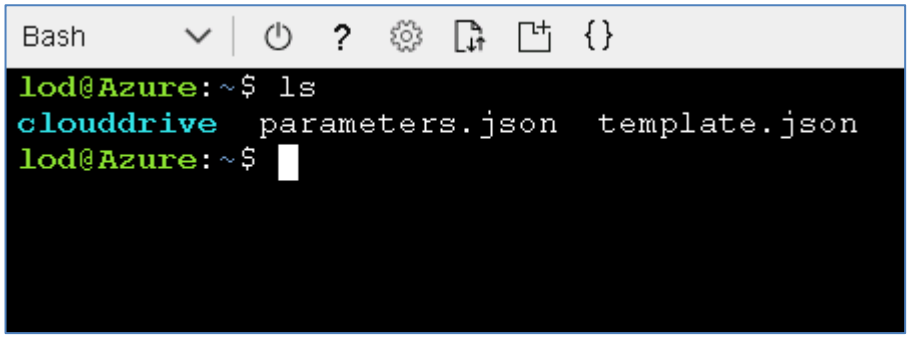
Step	Action
2-22	From the pfSense menu bar, select **Status** > **IPsec**. 
2-23	For Azure VPN Tunnel 1, click **Connect VPN**. 
2-24	Verify that the session is Established. 

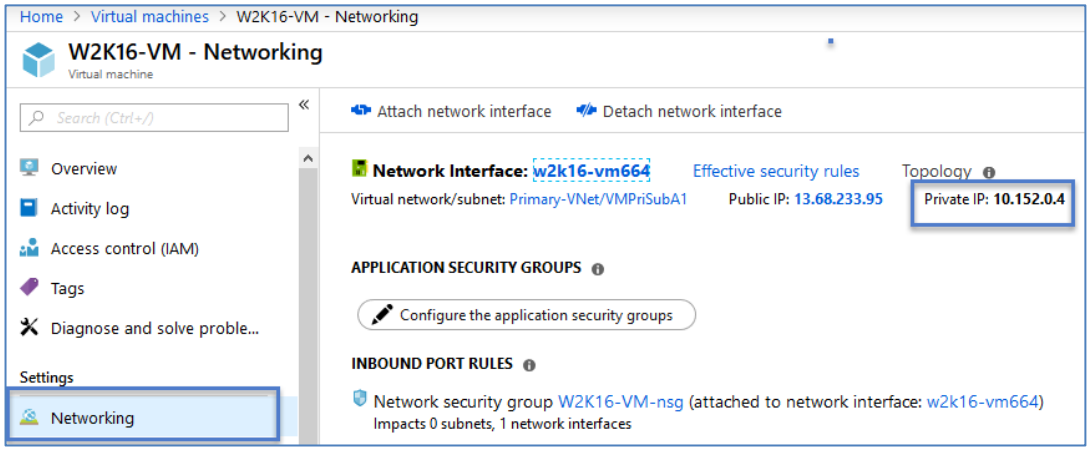
Task 3: Verify Connectivity

Step	Action
3-1	Return to the Azure Portal **Primay-gw** resource, click **Connections**, and then verify that the Site-to-site (IPsec) connection type shows a status of Connected. **Note:** You might need to wait several minutes to see the Connected state. 
3-2	In the Azure portal top menu, click the Azure Cloud Shell icon. 
3-3	Click **Bash.** 

Step	Action
3-4	Click **Show advanced settings**. 
3-5	In the You have no storage mounted page, do the following: a) Select the Cloud Shell region **East US**. b) For the Resource group, select **Use existing** and then select your available resource group. c) For the storage account, select **Create new** and then enter **ihcsa**<*your name*>. d) For the file share, select **Create new** and then enter **ihcfs**<*your name*>. 
3-6	Click **Create storage**.

Step	Action
3-7	Wait for the cloud shell to initialize (it should take only a few minutes). 
3-8	In the Azure Cloud Shell toolbar, click the upload/download icon and select **Upload**. 
3-9	From the CourseFiles folder, upload **template.json** and **parameters.json**. (Note you cannot multi-select, you must upload the items one at a time.)

Step	Action
3-10	Verify that the files are uploaded.  

Step	Action
3-11	Launch a Windows Server VM by using the Azure CLI: (For <*Your-ResourceGroup*>, you can start typing RT and then press Tab to complete it.) a. **`az group deployment create --resource-group <Your-ResourceGroup> --template-file ./template.json --parameters ./parameters.json`** Please provide string value for 'VNetName' (? for help): **RT**### (Example concatenated output) `{ "id": null, "namespace": "Microsoft.Compute", "registrationState": null, "resourceTypes": [{ "aliases": null, "apiVersions": null, "locations": ["eastus"], "properties": null, "resourceType": "virtualMachines" }] }], "provisioningState": "Succeeded", "template": null, "templateLink": null, "timestamp": "2018-12-06T15:39:41.507766+00:00" } "resourceGroup": "RT1782456" }`
3-12	Select **Virtual Machines** > **W2K16-VM** > **Networking**, and then record the Private IP Address: _____ 

Step	Action
3-13	 The following step verifies VPN connectivity.
3-14	On the on-premises Windows Server jump host (your lab kit), use the Remote Desktop Connection icon to connect to the private IP address of the Azure Windows Server virtual machine that you just launched. The user name is “\winadmin” and the password is “Netapp123.”

End of Exercise

Module 6: NetApp Cloud Volumes ONTAP Data Tiering

Exercise 1: Tier Backup Data to Amazon Simple Storage Service

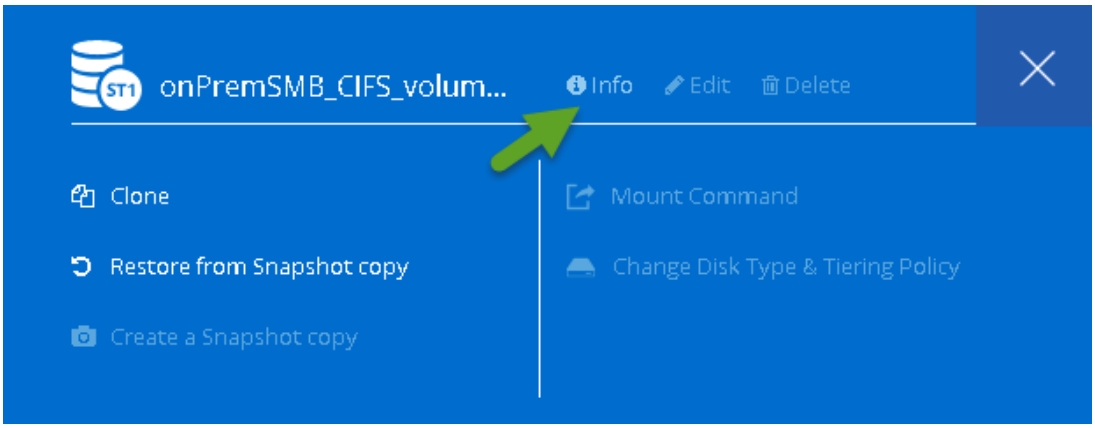
In this exercise, you tier secondary data from Cloud Volumes ONTAP to Amazon Simple Storage Service (Amazon S3).

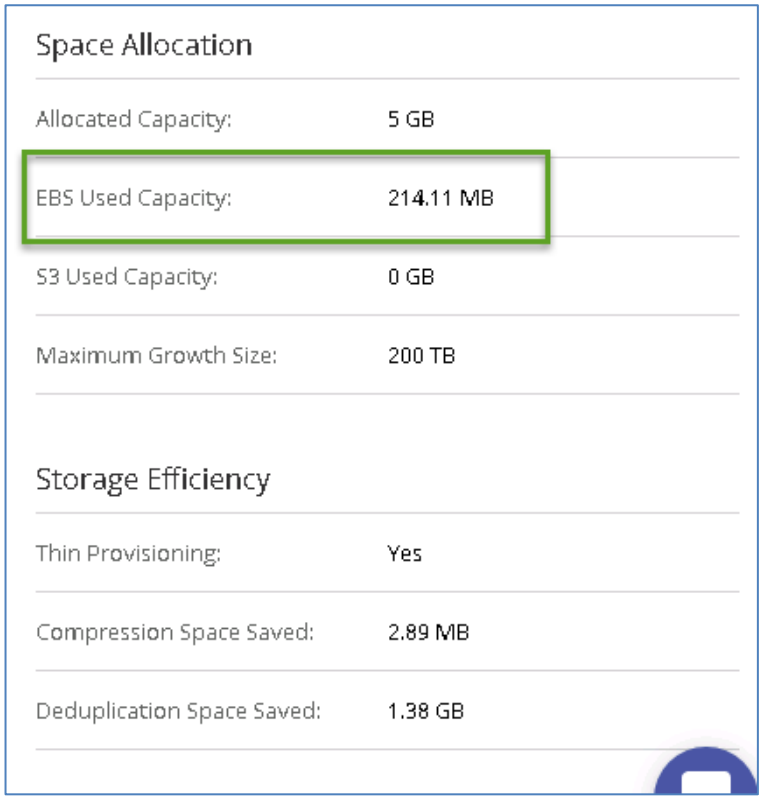
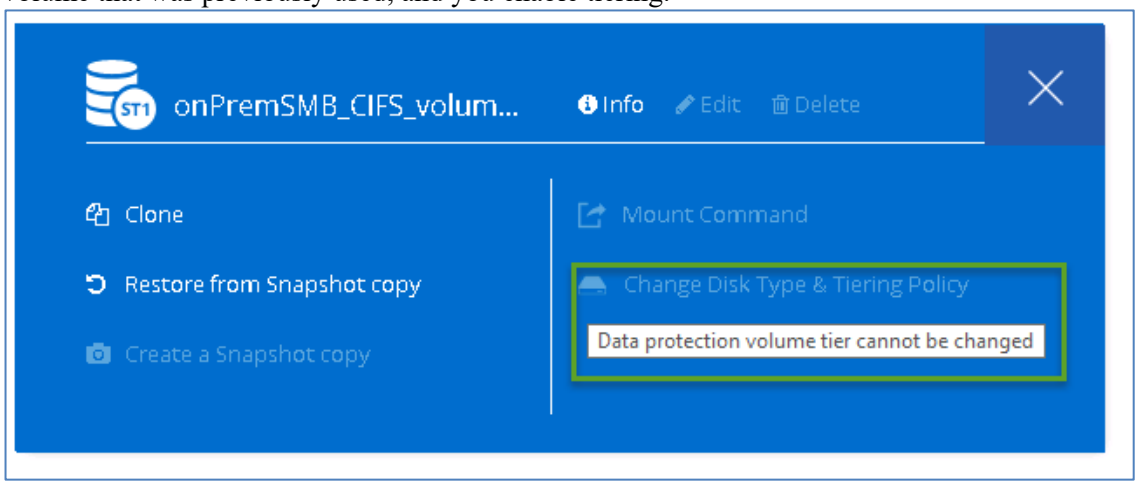
Objectives

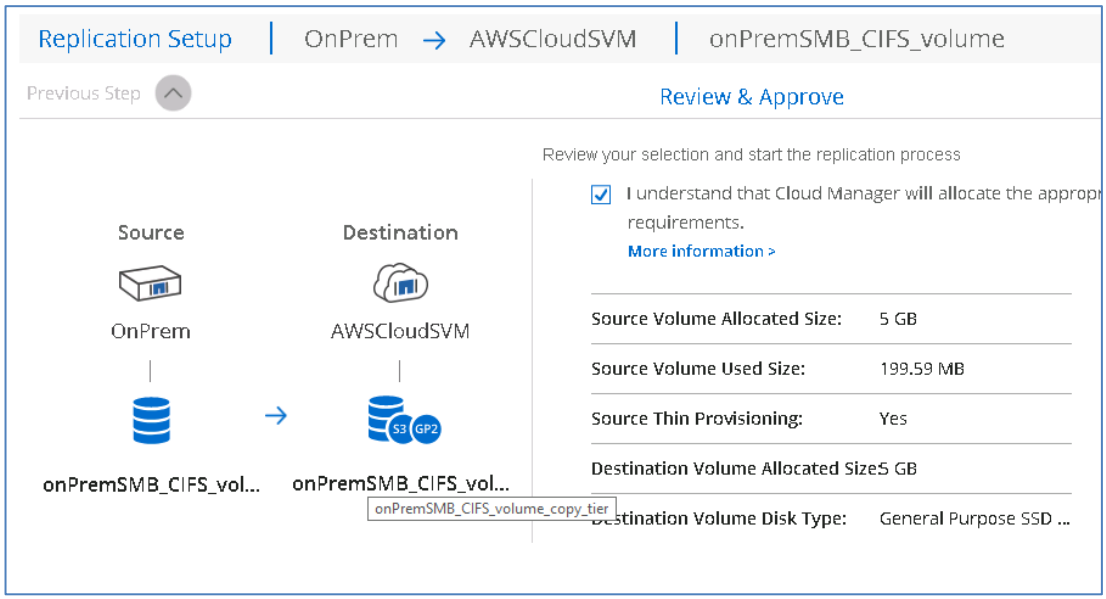
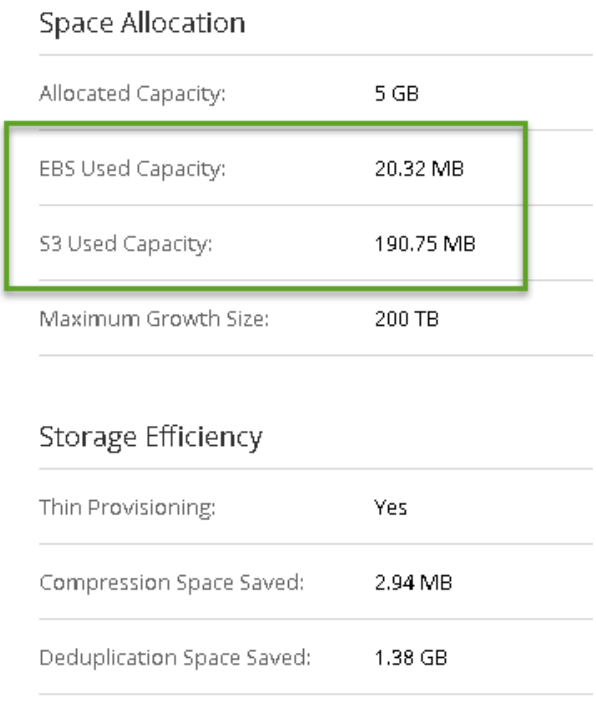
This exercise focuses on enabling you to do the following:

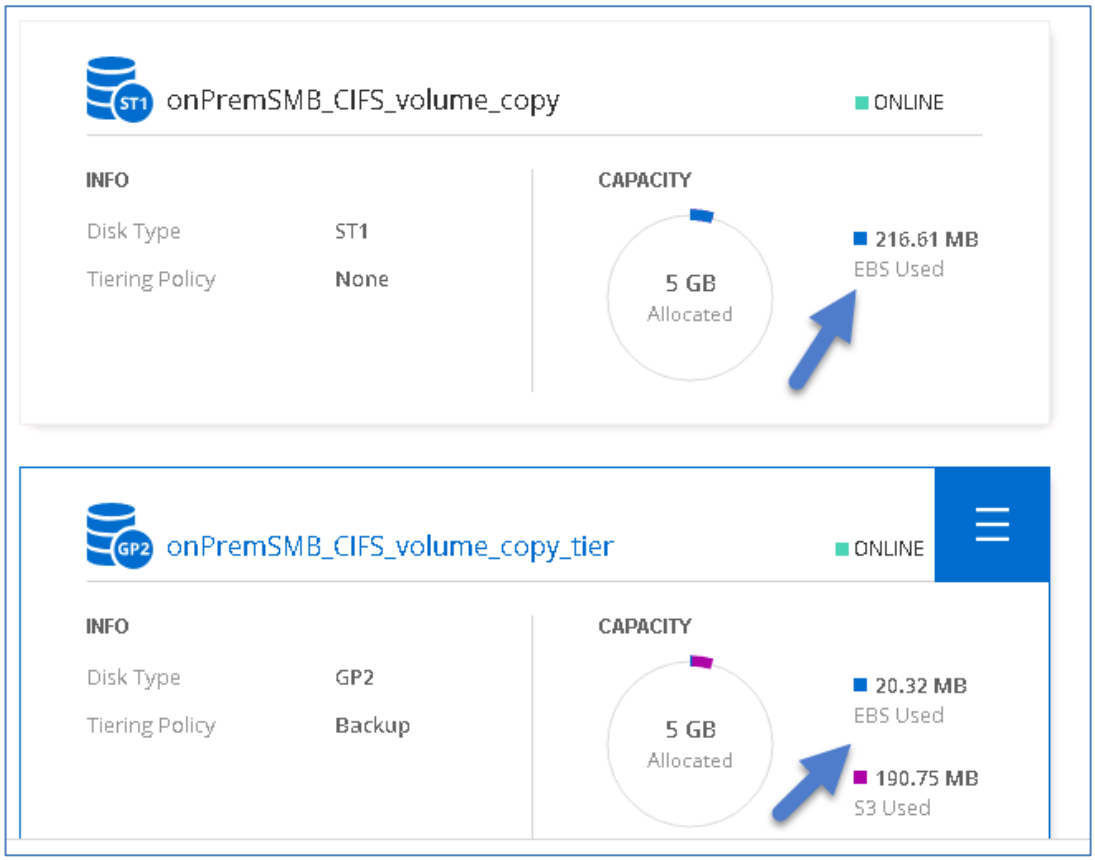
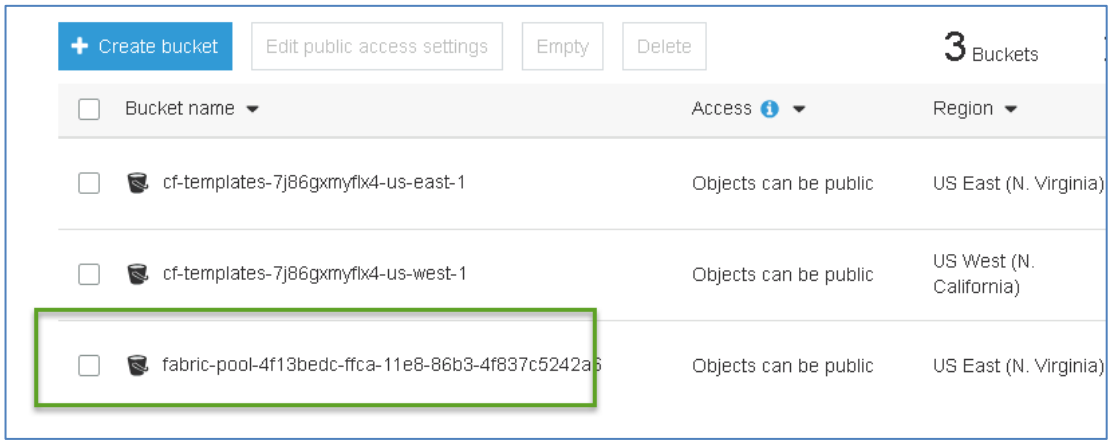
- Use OnCommand Cloud Manager to configure data tiering
- Verify that data is tiered to Amazon Simple Storage Service (Amazon S3 or S3).

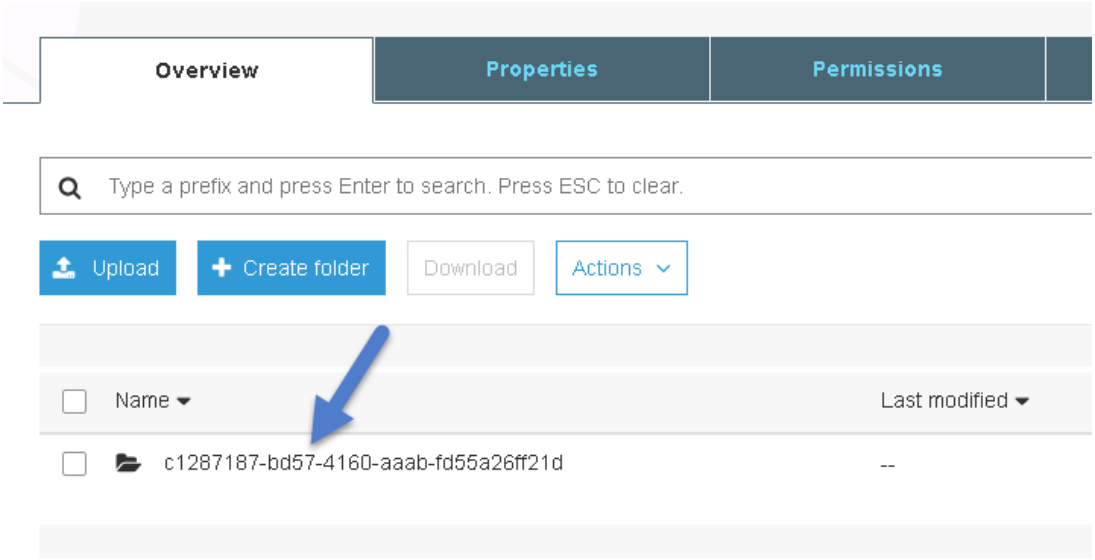
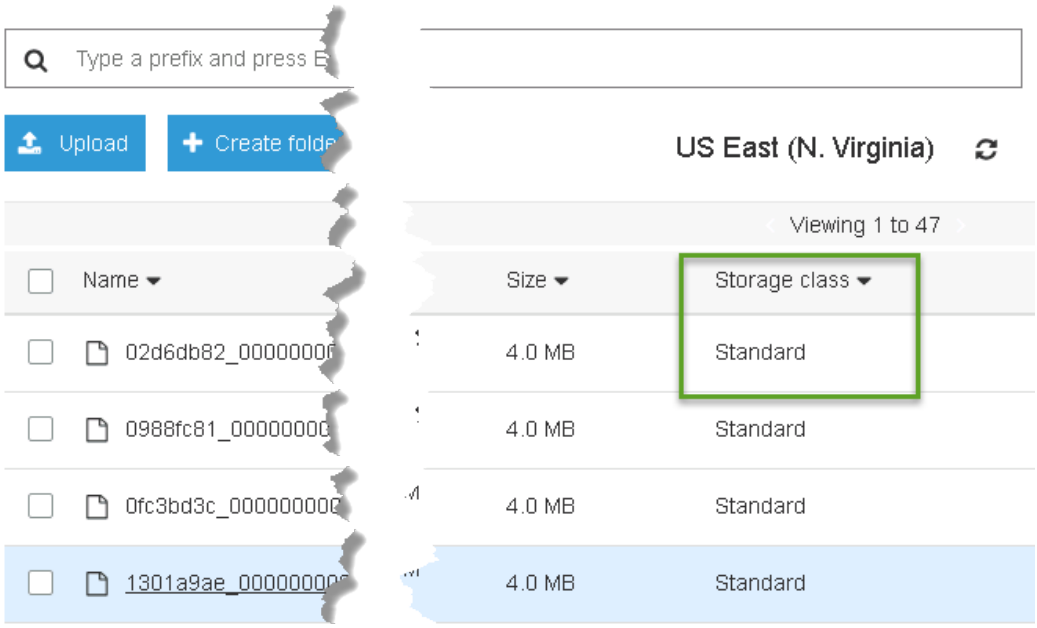
Task 1: Compare Space Allocation Between Tiering and Not Tiering

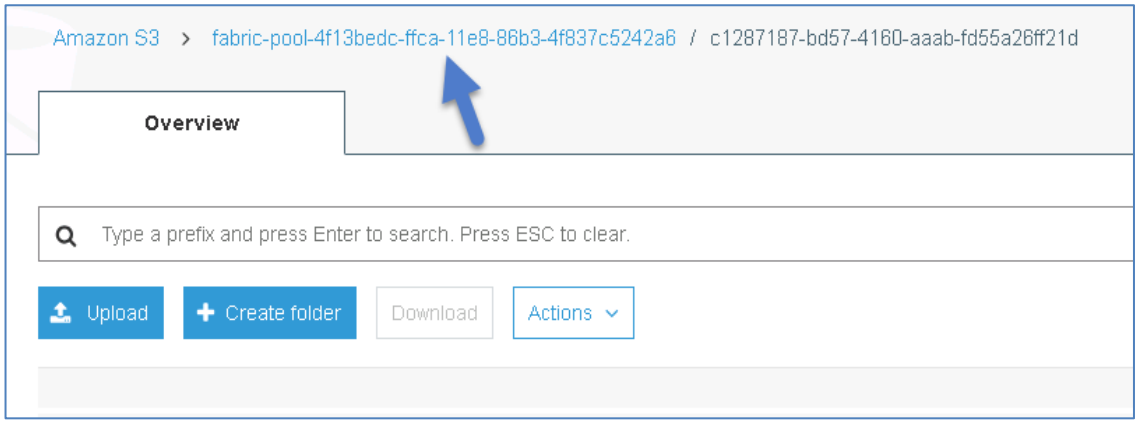
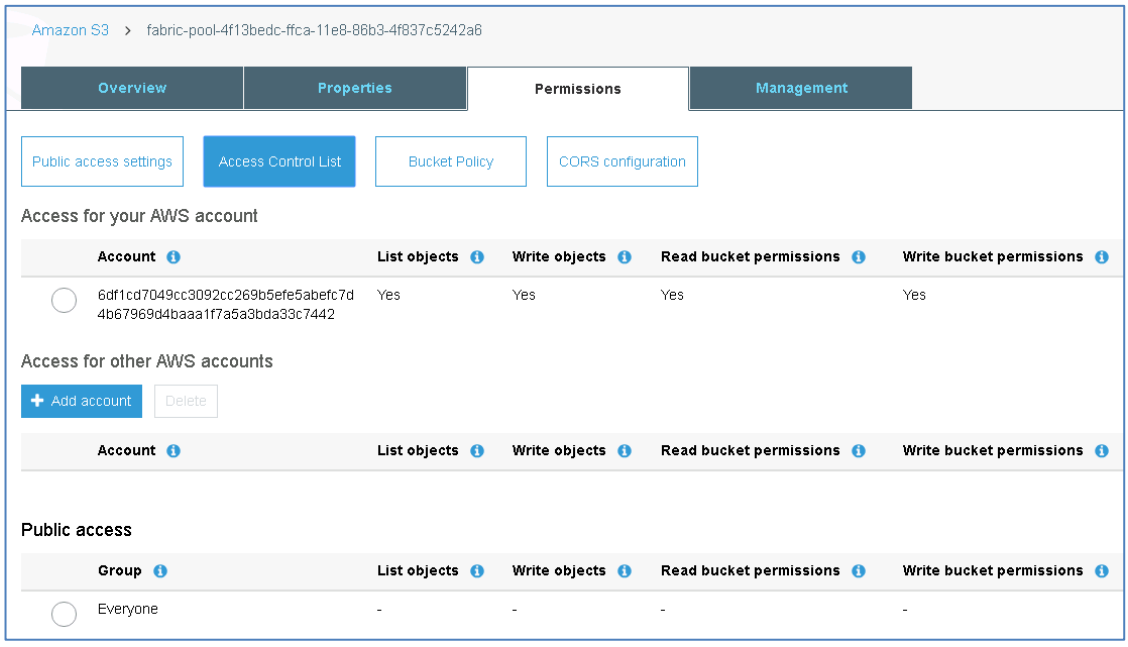
Step	Action
1-1	Return to Cloud Manager.
1-2	Enter the AWSCloudSVM working environment.
1-3	On the onPremSMB_CIFS_volume_copy, select **Menu** > **Info**. 

Step	Action
1-4	Note how much Amazon Elastic Block Store (Amazon EBS) data is used 
1-5	Ideally, for a data protection volume, “Backup” tiering policy should be turned on when the SnapMirror relationship is first set up. After the relationship is set up, you cannot set up or change the tiering policy on a DP volume. You can see this when you hover over the Change Disk Type & Tiering Policy. So, for this tiering exercise, you create a new destination DP volume and set up a SnapMirror relationship with the source volume that was previously used, and you enable tiering. 

Step	Action
1-6	Using Cloud Manager, create another relationship with onPremSMB_CIFS_volume as the source, name the destination **onPremSMB_CIFS_volume_copy_tier**, and set S3 tiering to Enabled. Note: Follow the same data replication procedure as before, but remember to enable S3 tiering for this new relationship. 
1-7	Wait for the Status to become idle and the MirrorState to become snapmirrored.
1-8	On the Volumes page, select **onPremSMB_CIFS_volume_copy_tier**, and then select **Menu** > **info**.
1-9	View the EBS Used Capacity and the S3 Used Capacity. 

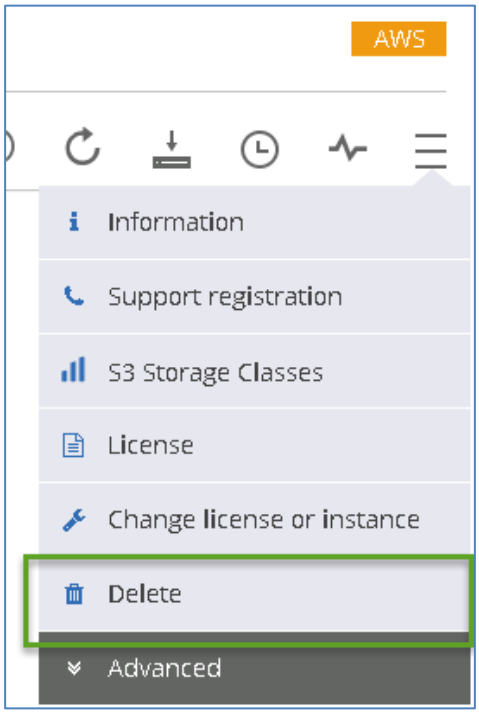
Step	Action
1-10	With the “Backup” tiering policy, the data from the source volume is sent to S3 immediately with just the metadata remaining in the destination data protection volume.
1-11	You can also view the capacity directly from the Volumes page. 
1-12	Return to the Amazon Web Services (AWS) Console.
1-13	Select **Services** > **S3**.
1-14	Verify that you see a fabric-pool bucket. 
1-15	Click the fabric-pool bucket name.

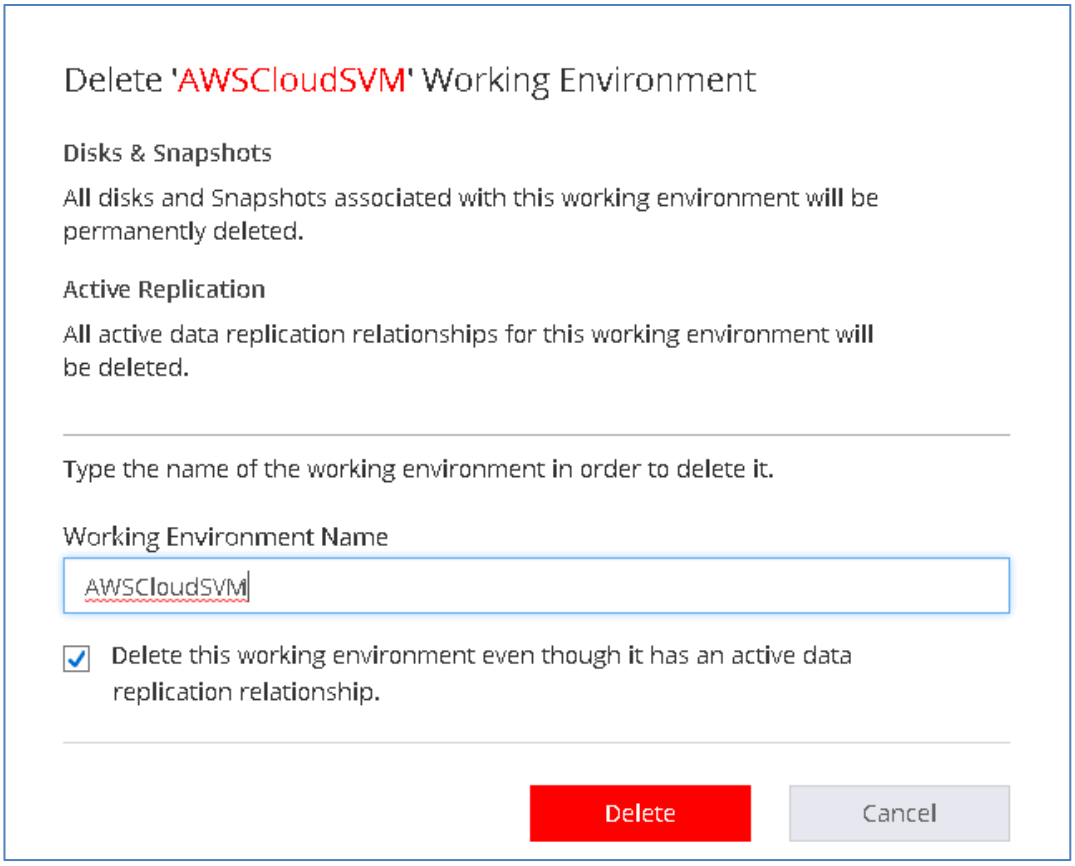
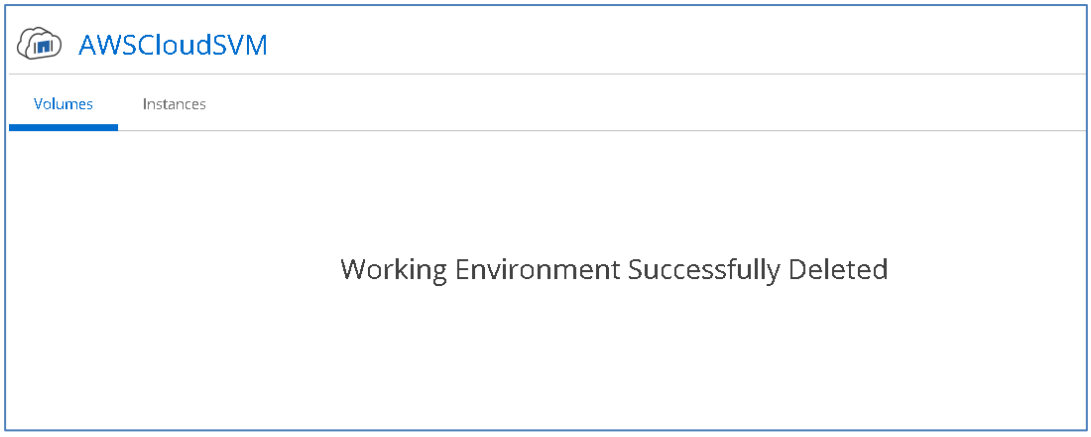
Step	Action
1-16	Click the folder. 
1-17	Verify that all the objects are currently in the Standard storage class. 

Step	Action
1-18	At the top of the page, click the fabric-pool name in the path. 
1-19	Click the **Permissions** tab.
1-20	Click **Access Control List**.
1-21	Verify that only your AWS account has access to this bucket. It is not publicly available. 

Task 2: Delete the Cloud Volumes ONTAP Instance

In this task, you clean up your Cloud Volumes ONTAP instance by using Cloud Manager.

Step	Action
2-1	Return to Cloud Manager.
2-2	Enter the AWSCloudSVM working environment.
2-3	Select **Menu** > **Delete**. 

Step	Action
2-4	Enter the working environment name **AWSCloudSVM** and select the checkbox that is labeled **Delete this working environment even though it has an active data replication relationship**. 
2-5	Click **Delete**.
2-6	Verify that the Working Environment is deleted. 

End of Exercise

Module 7: NetApp Cloud Volumes ONTAP High Availability

Exercise 1: Implement Cloud Volumes ONTAP High Availability

In this exercise, you use OnCommand Cloud Manager to deploy a Cloud Volumes ONTAP high-availability (HA) instance.

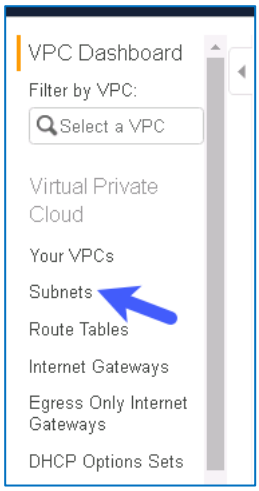
Objectives

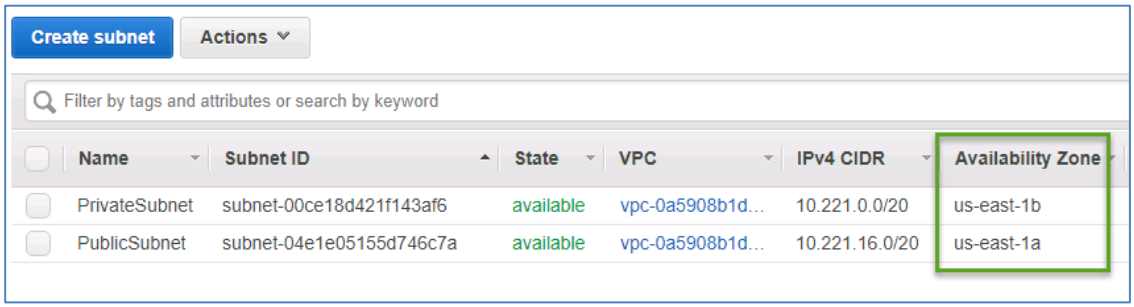
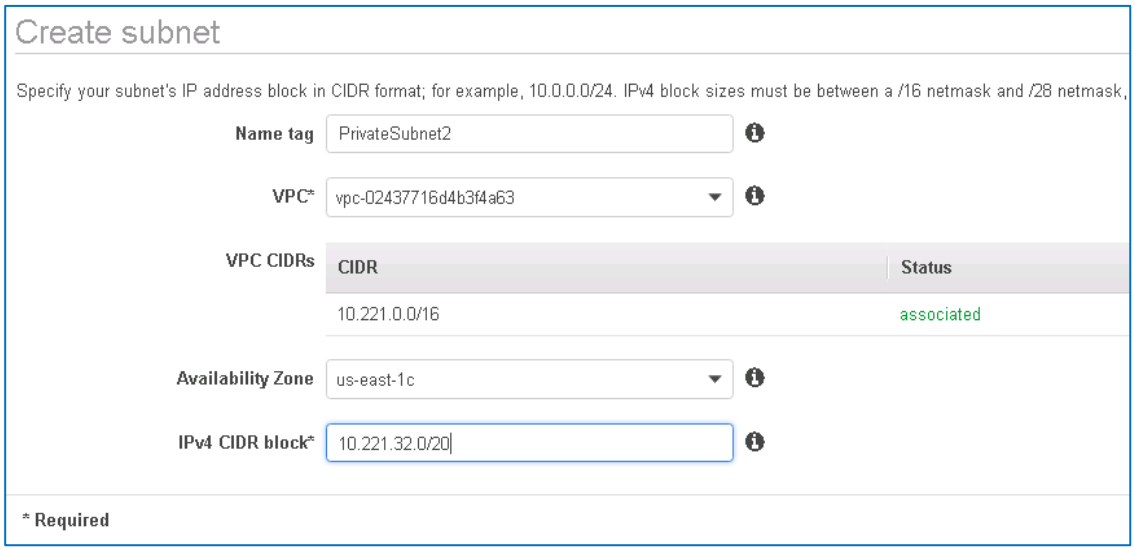
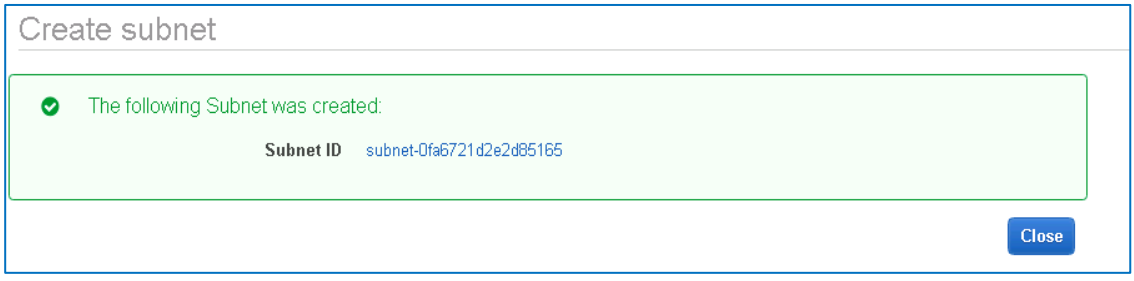
This exercise focuses on enabling you to do the following:

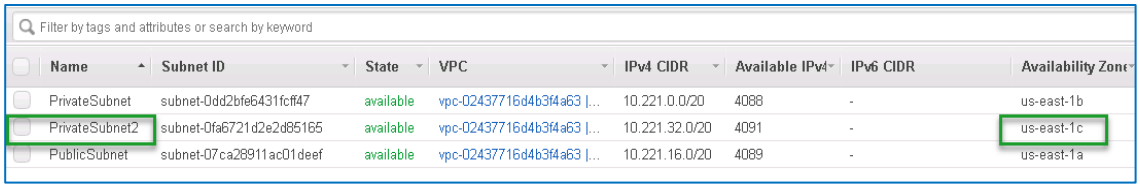
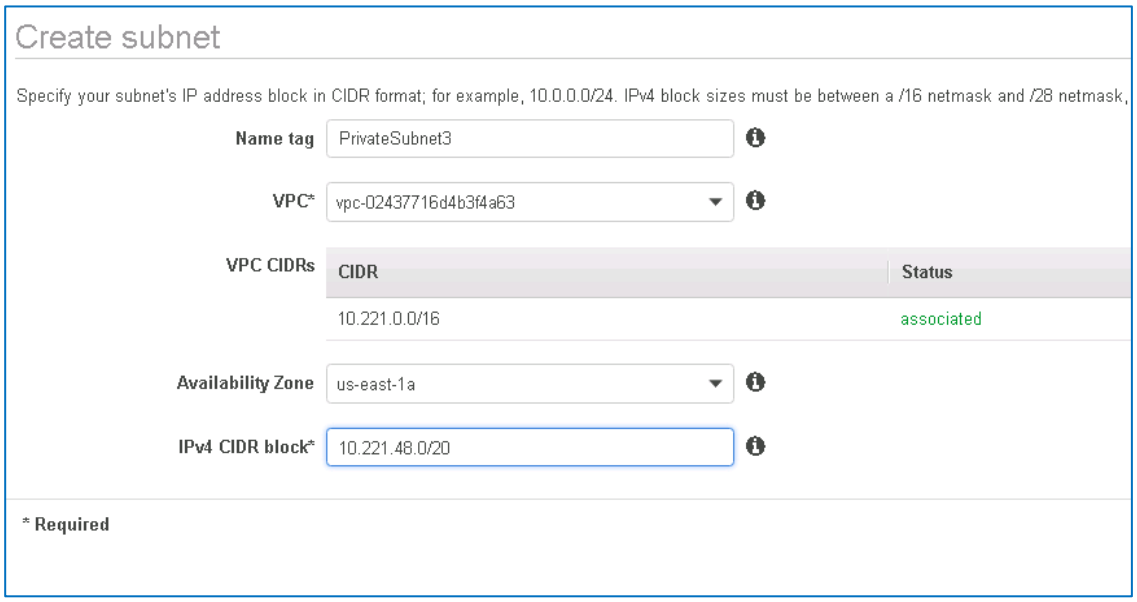
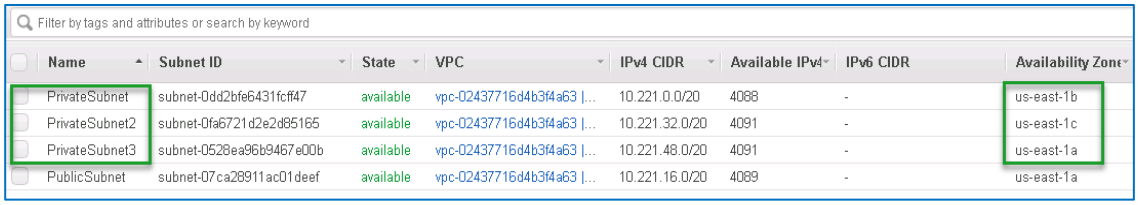
- Deploy Cloud Volumes ONTAP in HA mode by using Cloud Manager
- Use floating IPs and deploy the Cloud Volumes ONTAP high availability in multiple Availability Zones (AZs)
- Perform a failover and failback and verify that client access to data continues with the same data LIF

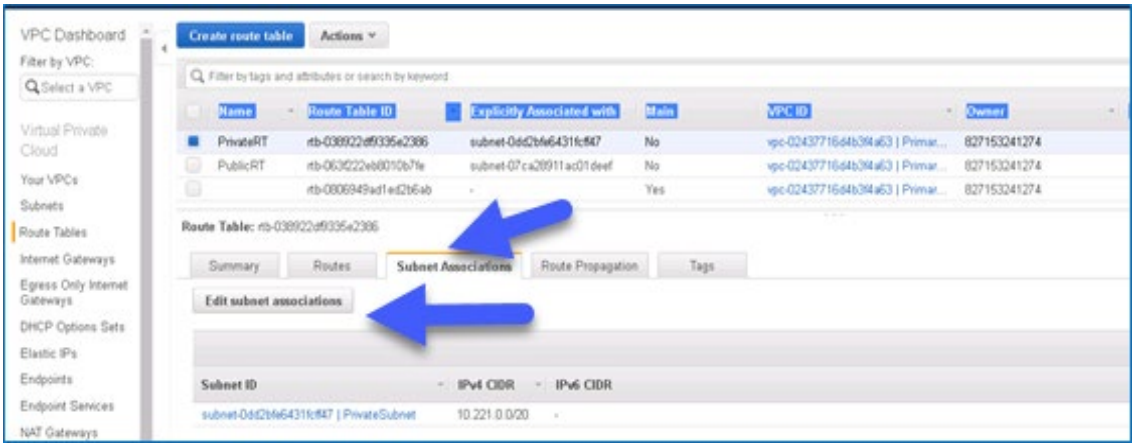
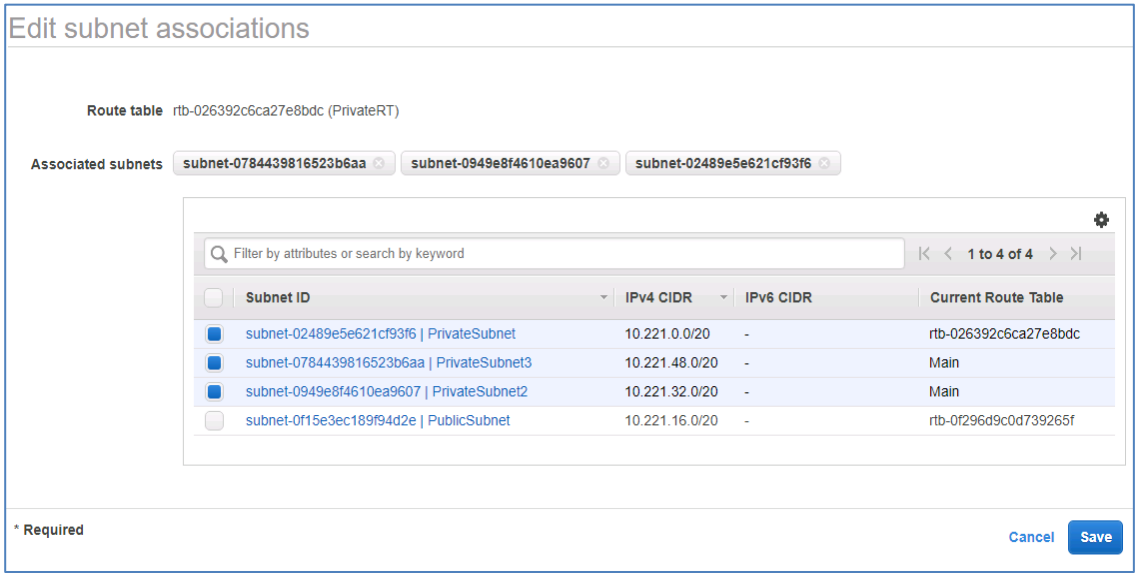
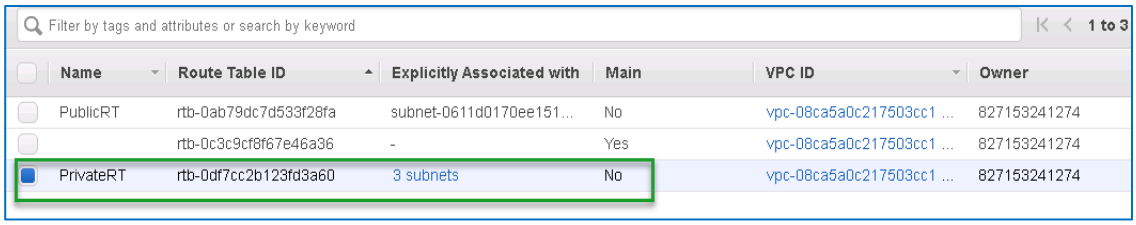
Task 1: Create Additional Subnets to Deploy HA Nodes of Cloud Volumes ONTAP

In this task, you create two additional private subnets in the Primary Virtual Private Cloud (VPC). One private subnet is in the same AZ as the public subnet, and the other private subnet is in a new AZ. At the end of this task, you have two newly created subnets and a previously created private subnet. The total is three private subnets in three different AZs to deploy Cloud Volumes ONTAP high availability.

Step	Action
1-1	In the Amazon Web Services (AWS) Console, select **Services** > **VPC**.
1-2	In the VPC Dashboard, click **Subnets**. 

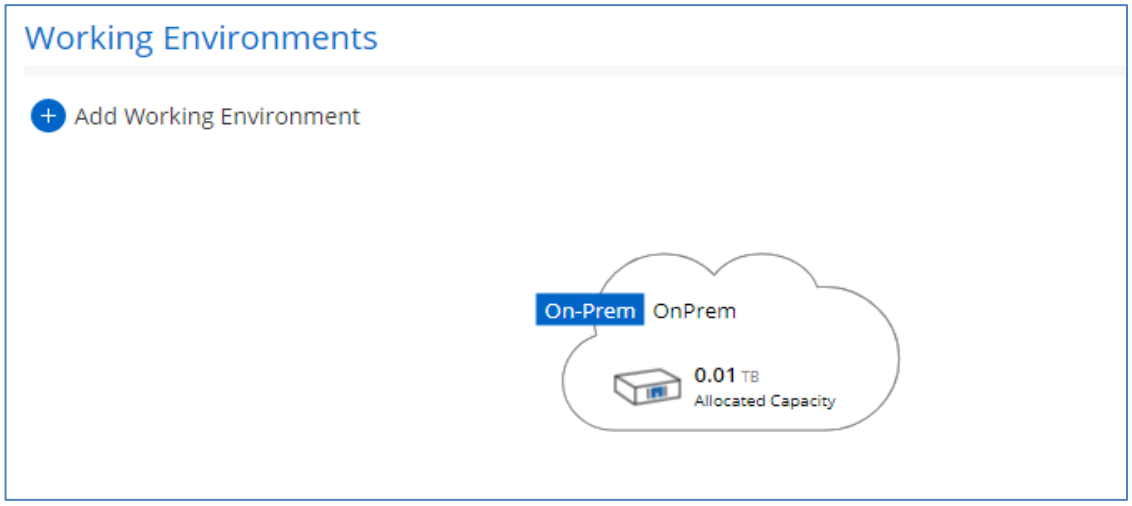
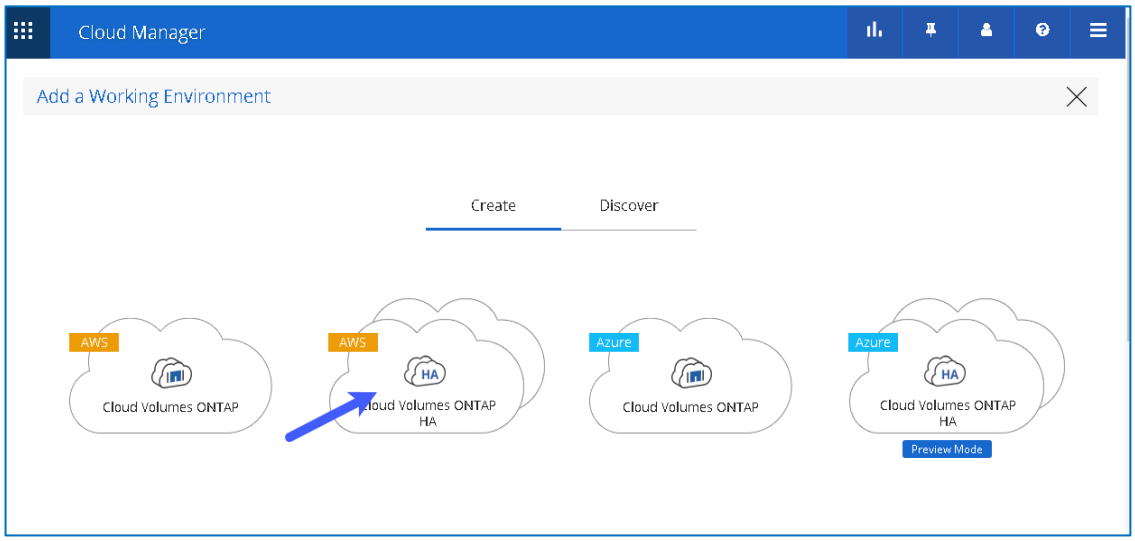
Step	Action
1-3	Record the Availability Zones being used by your subnets, PrivateSubnet and PublicSubnet. PrivateSubnet: _____ PublicSubnet: _____ 
1-4	Click **Create Subnet** and configure the following information: ▪ Name tag: **PrivateSubnet2** ▪ VPC: **PrimaryVPC** ▪ Availability Zone: Choose an **AZ** that is unique from the other subnets in your Primary VPC. ▪ IPv4 CIDR block: **10.221.32.0/20** 
1-5	Click **Create**.
1-6	When you see the following, click **Close**. 

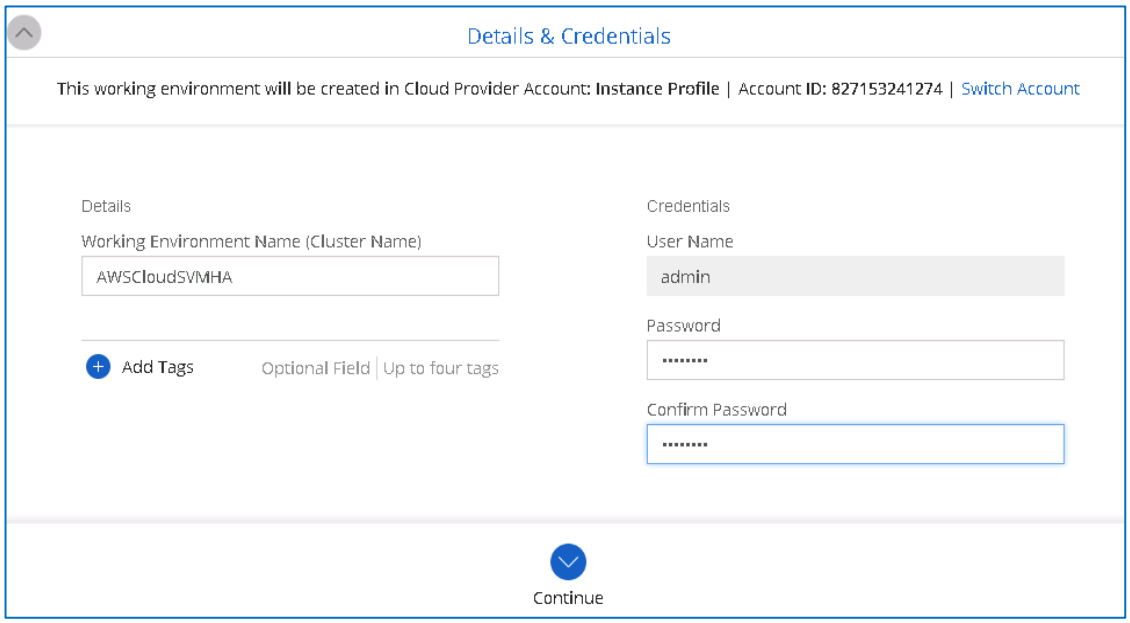
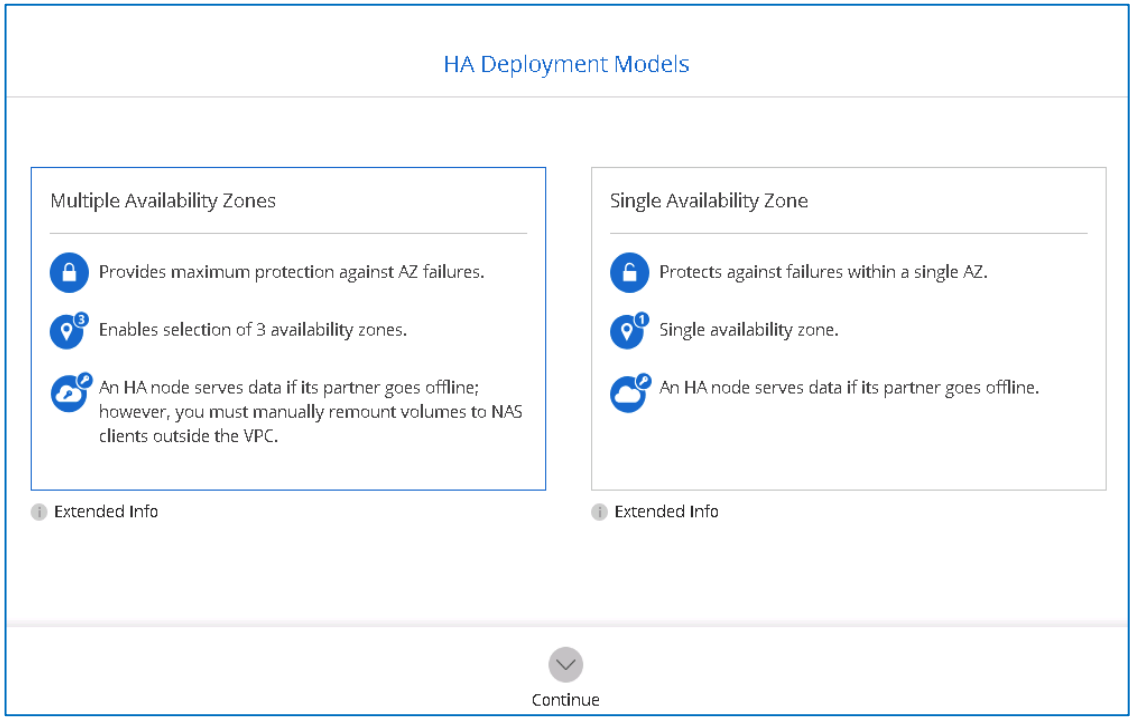
Step	Action
1-7	Verify that the private subnet was created in an AZ that is unique from the AZs of the other subnets in your Primary VPC. 
1-8	Create another subnet, and configure the following information: ▪ Name tag: **PrivateSubnet3** ▪ VPC: **PrimaryVPC** ▪ Availability Zone: Choose the same AZ as your PublicSubnet. ▪ IPv4 CIDR block: **10.221.48.0/20** 
1-9	Verify that you have three private subnets in three different AZs. 
1-10	In the VPC Dashboard, click **Route Tables**, and then select the **PrivateRT.**

Step	Action
1-11	Select the **Subnet Association** tab, and then click **Edit subnet associations**. 
1-12	Select PrivateSubnet2 and PrivateSubnet3, and click **Save**. 
1-13	The PrivateSubnet2 and PrivateSubnet3 were using the Main Route Table, and you now explicitly associate them with the PrivateRT.
1-14	Verify that the PrivateRT is explicitly associated with three subnets. 

Task 2: Deploy Cloud Volumes ONTAP High Availability

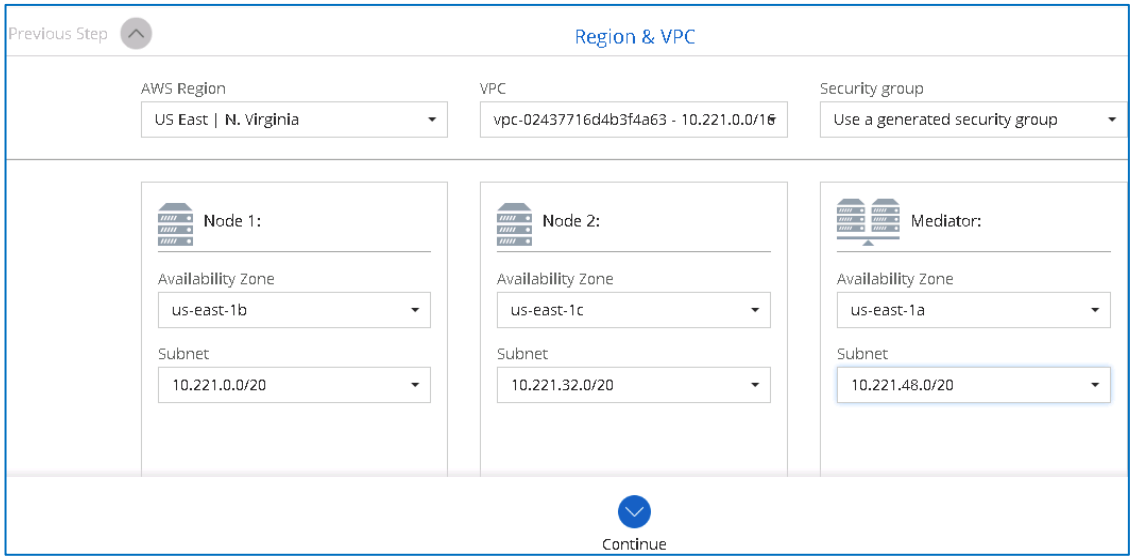
In this task, you use Cloud Manager to deploy Cloud Volumes ONTAP high availability in multiple AZs.

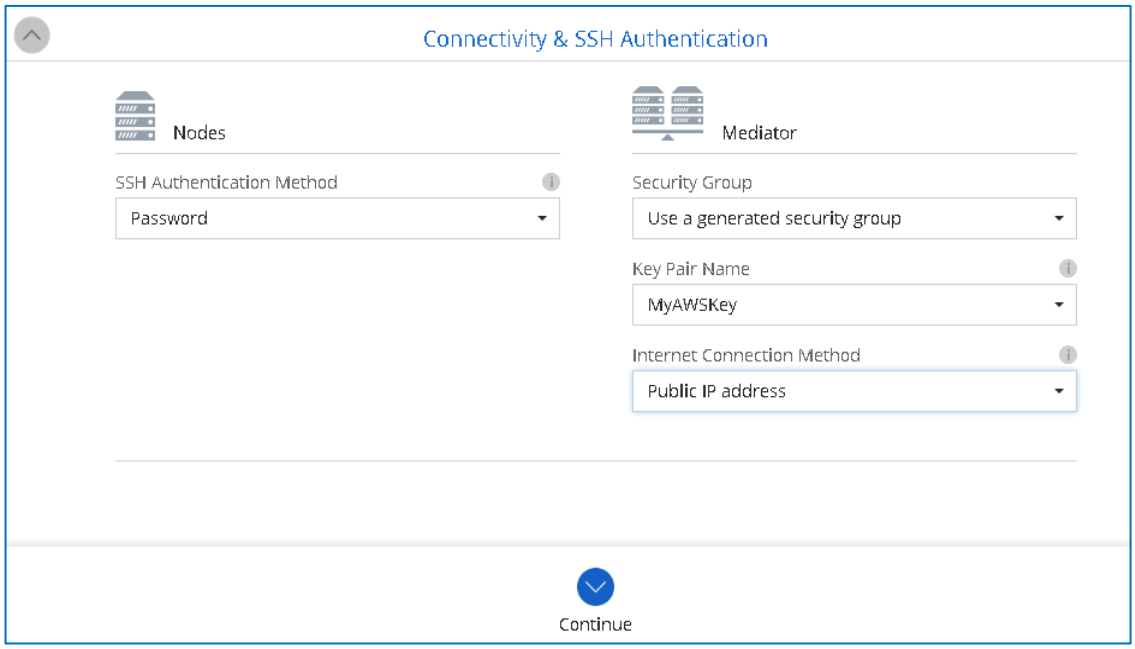
Step	Action
2-1	Return to the Cloud Manager interface on your browser.
2-2	Click **Add Working Environment**. 
2-3	In the Add a Working Environment page, click **Create**, and select **Cloud Volumes ONTAP HA.** 

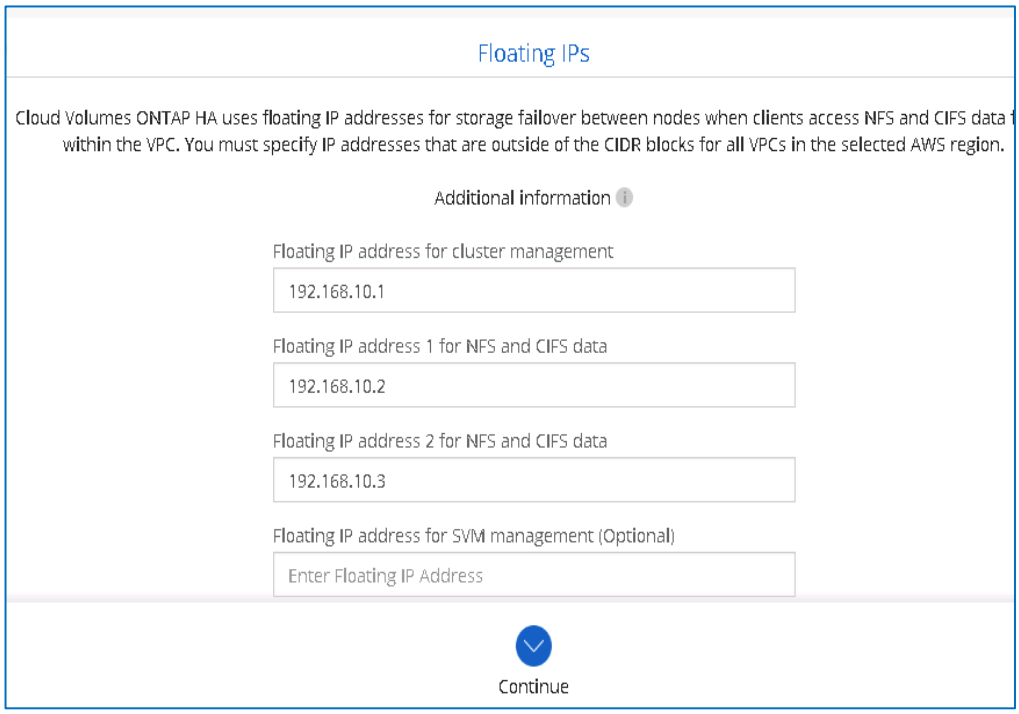
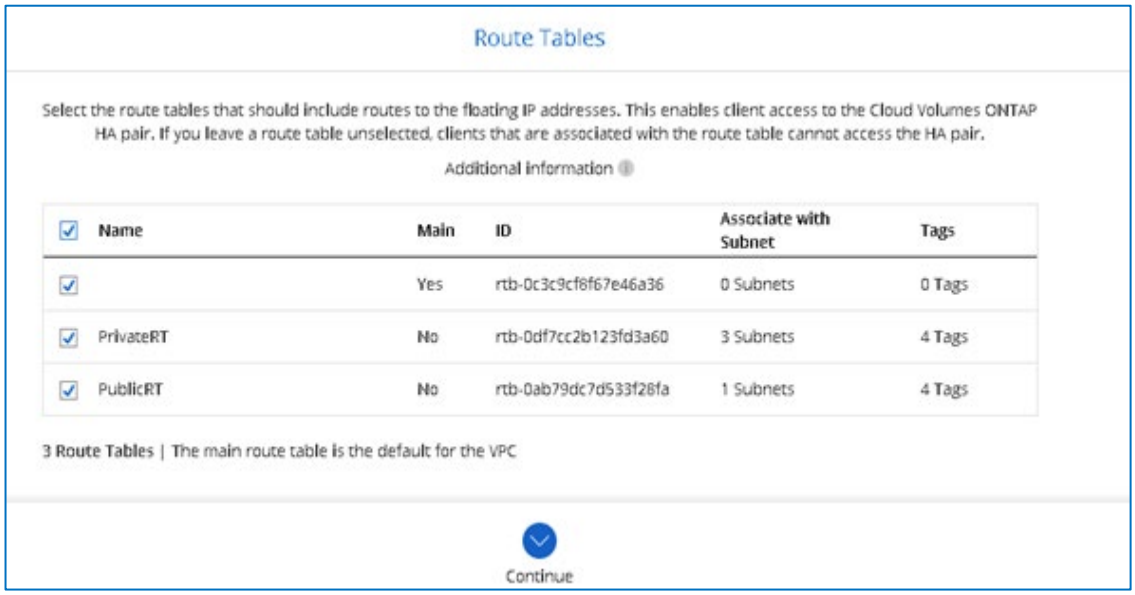
Step	Action
2-4	On the Details & Credentials page, enter the following, and then click **Continue**. ▪ Working Environment Name: **AWSCloudSVMHA** ▪ Password: **Netapp1!** ▪ Confirm Password: **Netapp1!** 
2-5	In the HA Deployment Models Page, click **Multiple Availability Zones**,and then click **Continue**. 

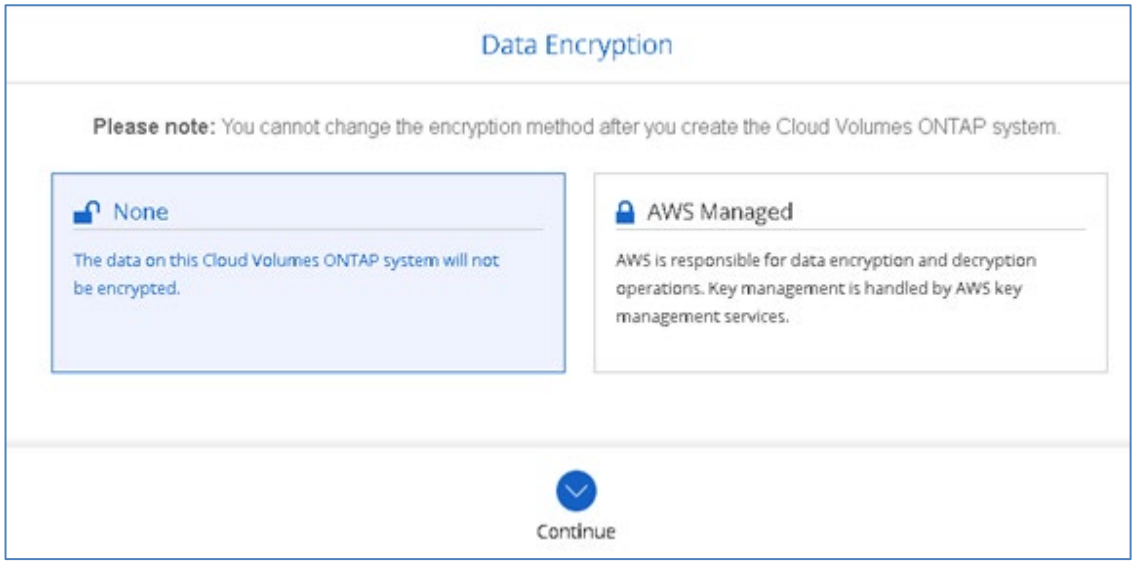
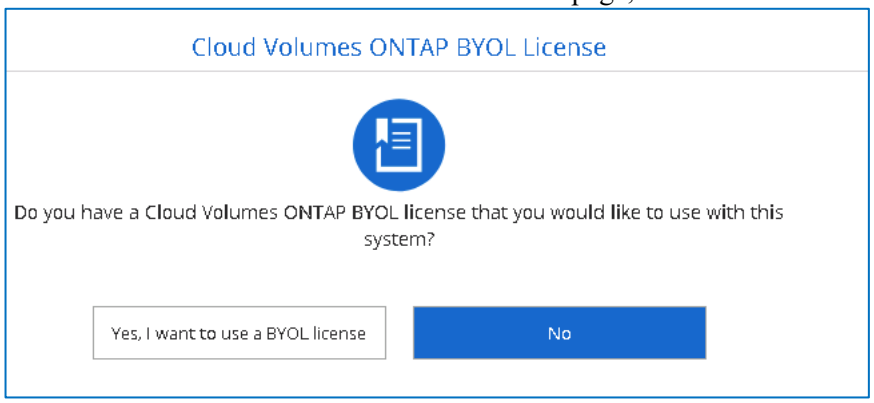
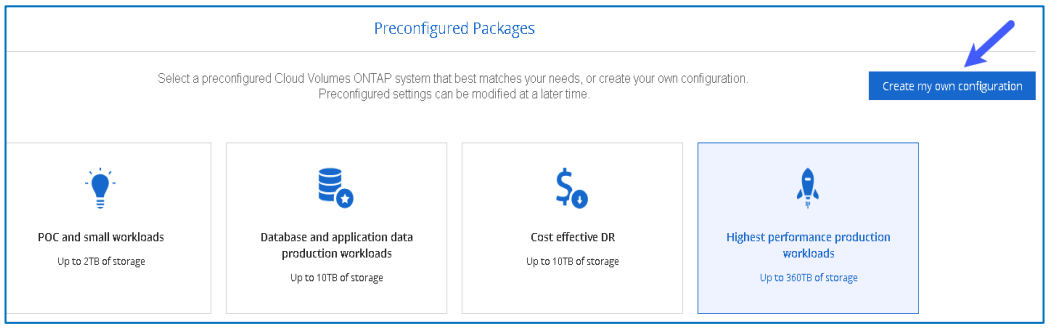
Step	Action

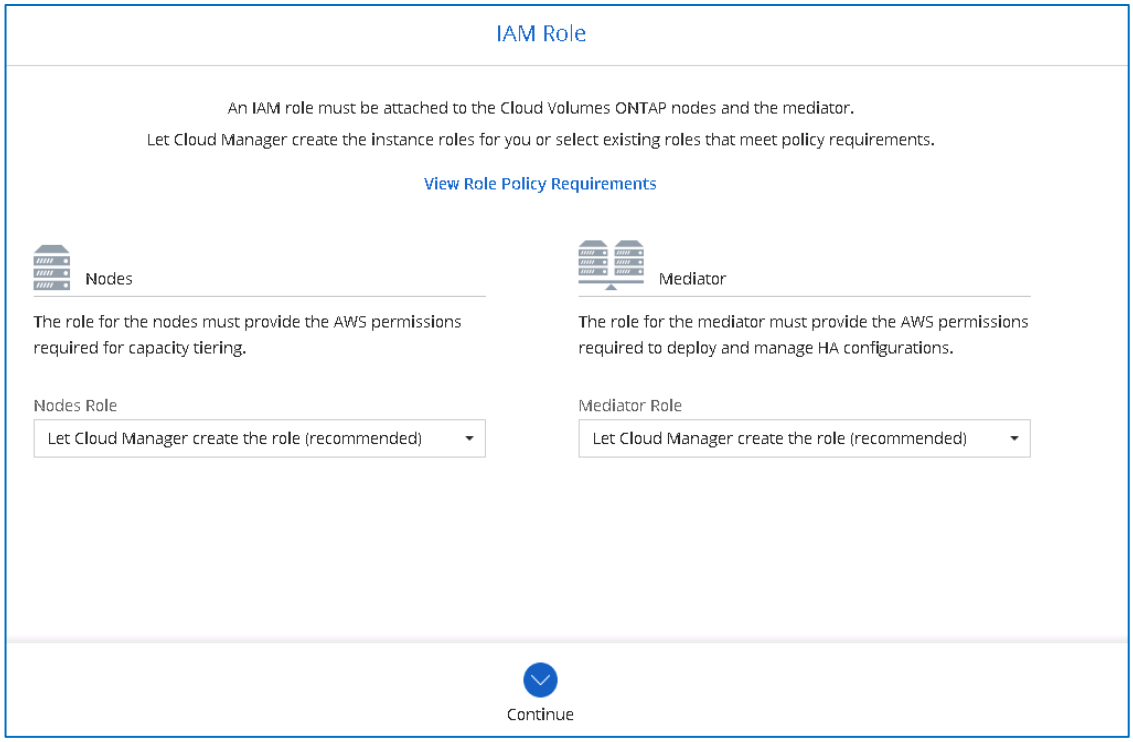
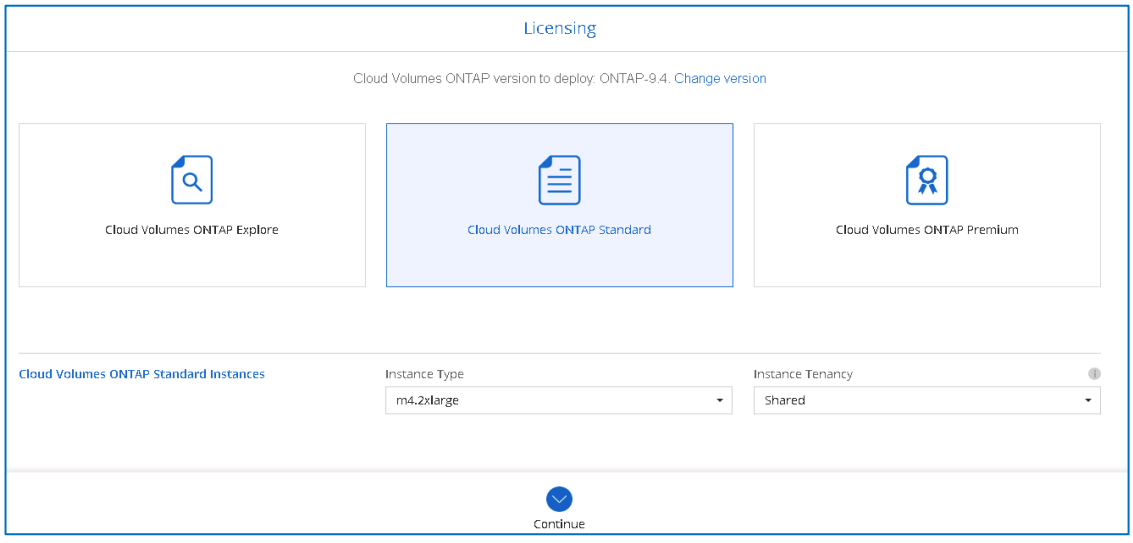
2-6	On the Region and VPC page, enter the following values and then click **Continue**.
	• AWS Region: **US East | N.Virginia**
	• VPC: **PrimaryVPC**
	• Security group: **Use a generated security group**
	• Place Node 1, Node 2, and Mediator in the subnets below. Your exact AZs may be different from those AZs in this example, but they should all be unique.
	  ○ Node 1:
	  ▪ Availability zone: **us-east-1b**
	  ▪ Subnet: **PrivateSubnet**
	  ○ Node 2:
	  ▪ Availability zone: **us-east-1c**
	  ▪ Subnet: **PrivateSubnet2**
	  ○ Mediator:
	  ▪ Availability zone: **us-east-1a**
	  ▪ Subnet: **PrivateSubnet3**

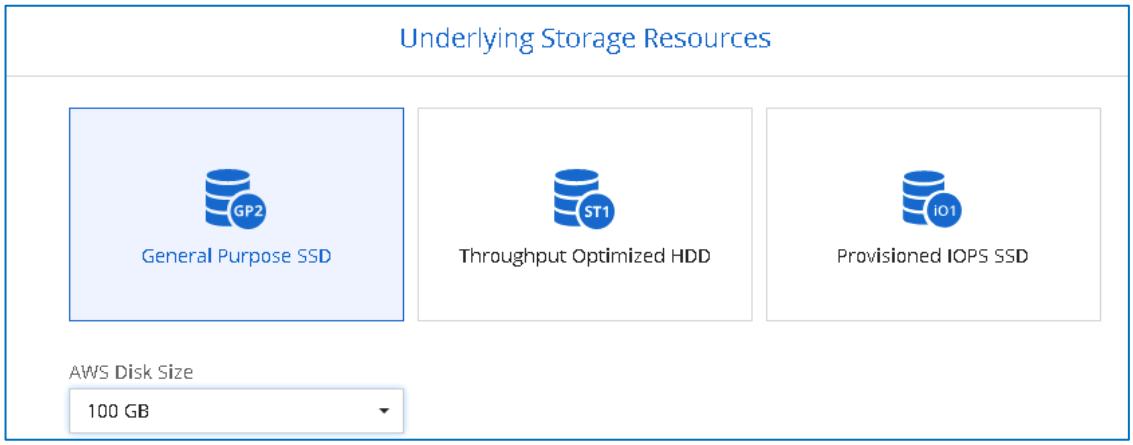
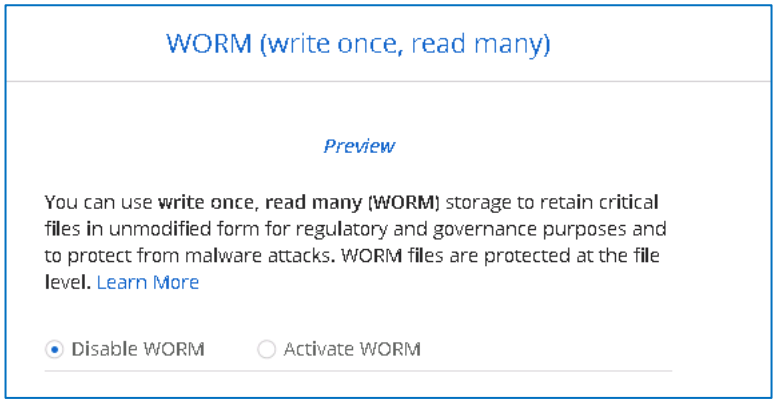


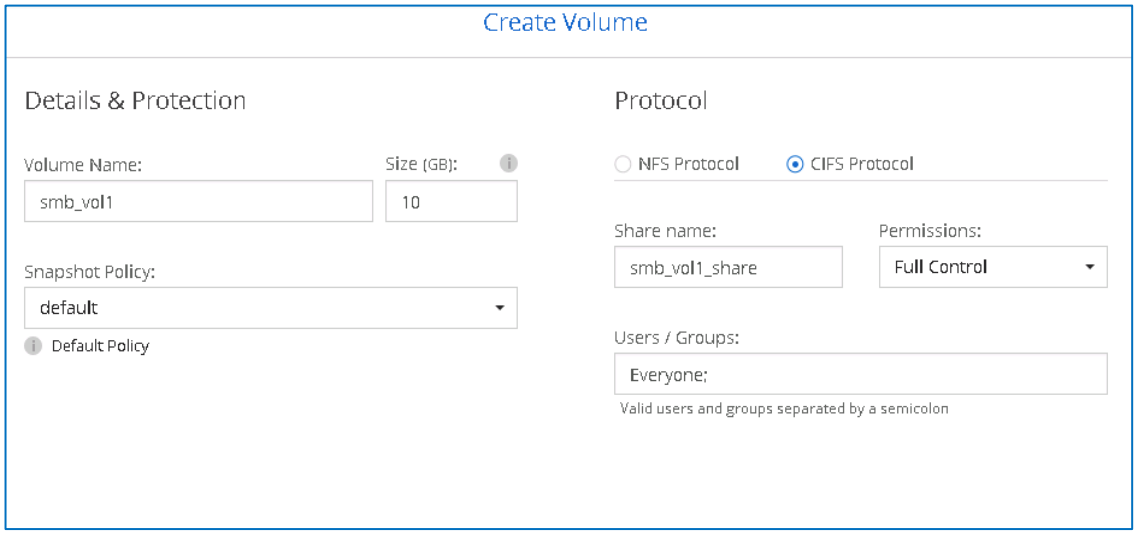
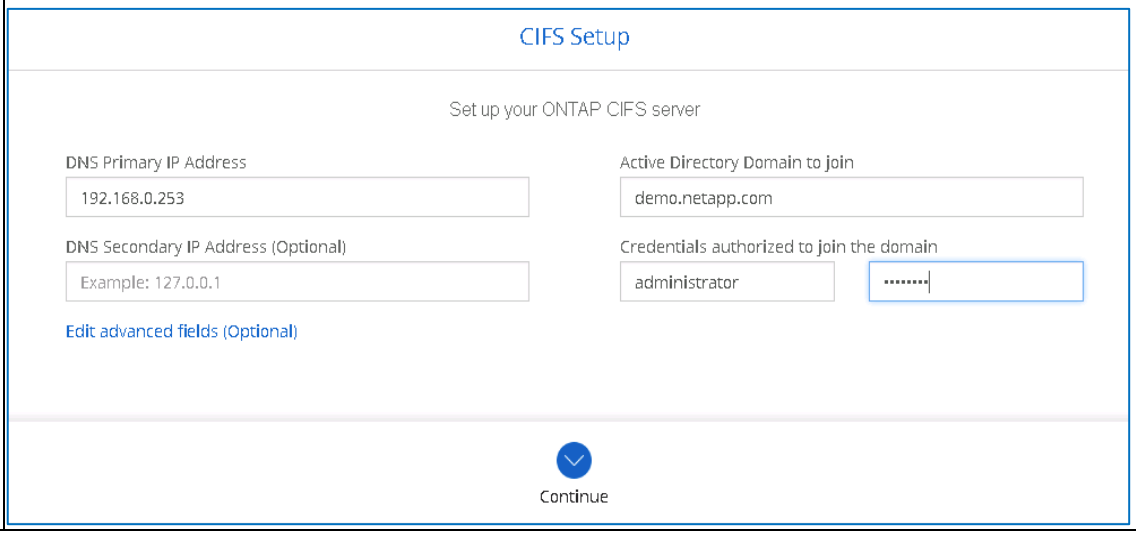
Step	Action
2-7	On the Connectivity & SSH Authentication page, use the following values, and then click **Continue**: ▪ SSH Authentication Method: **Password** ▪ Security Group: **Use a generated security group** ▪ Key Pair Name: **MyAWSKey** ▪ Internet Connection Method: **Public IP address** 

Step	Action
2-8	On the Floating IPs page, provide the following floating IPs, and then click **Continue**: ▪ Floating IP for cluster management: **192.168.10.1** ▪ Floating IP address 1 for NFS and CIFS data: **192.168.10.2** ▪ Floating IP address 2 for NFS and CIFS data: **192.168.10.3** 
2-9	On the Route Tables page, select the checkboxes for all three route tables, and then click **Continue**. 

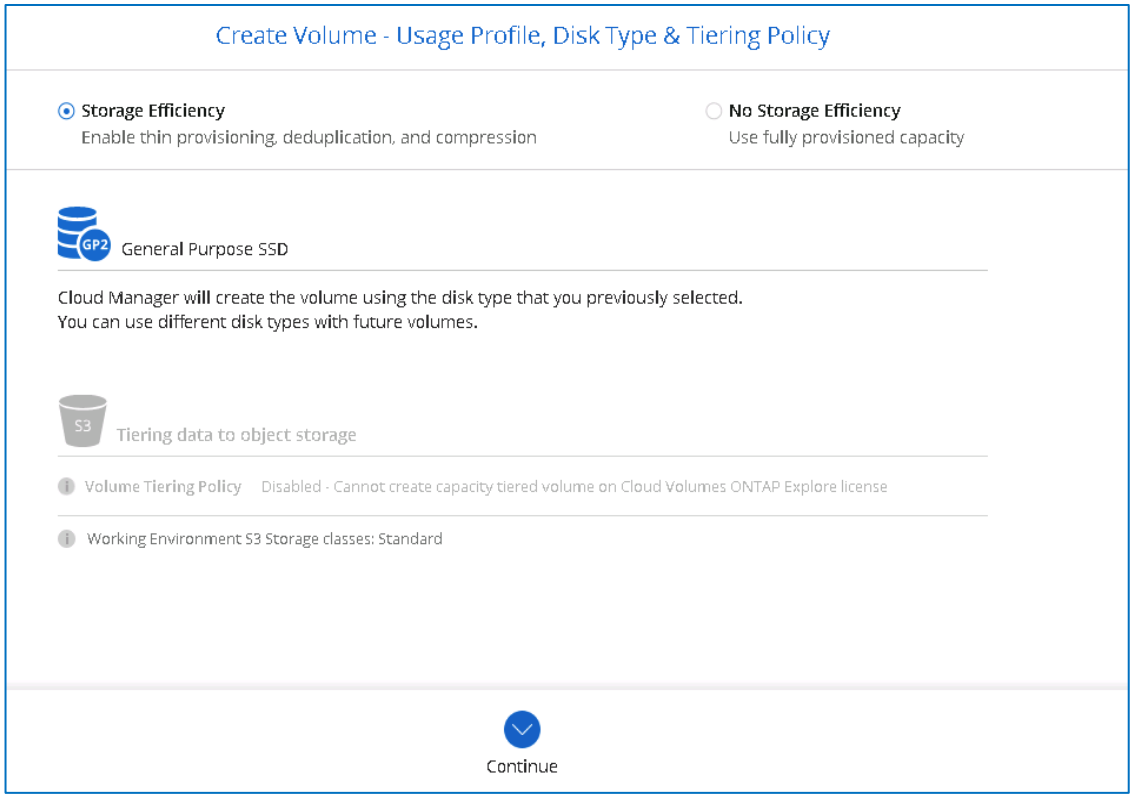
Step	Action
2-10	In the Data Encryption Page, select **None**, and then click **Continue.** 
2-11	On the Cloud Volumes ONTAP BYOL License page, click **No**. 
2-12	On the Preconfigured Packages page, click **Create my own configuration**. 

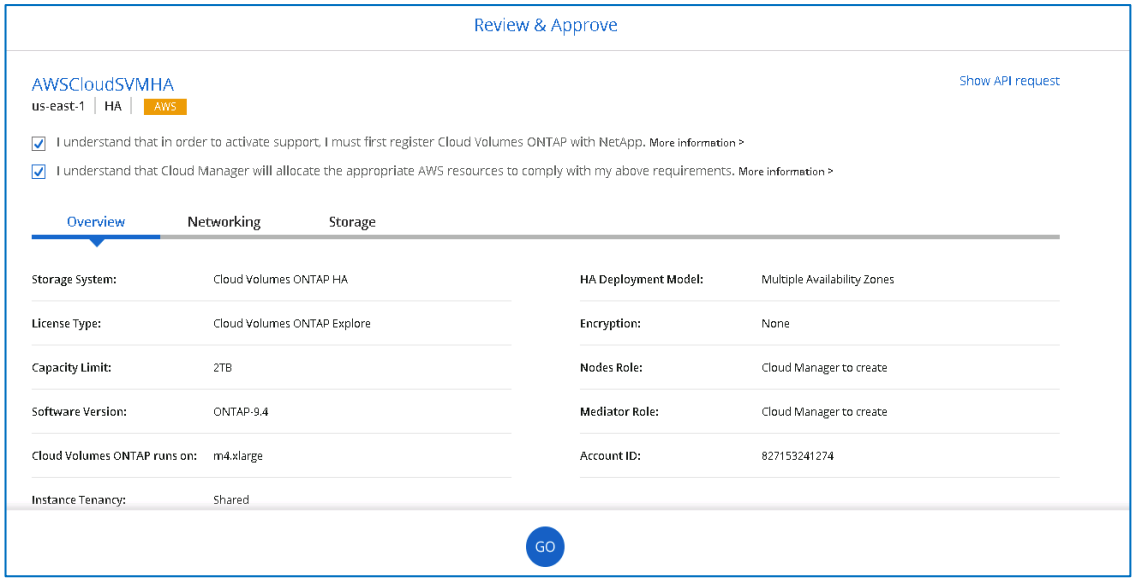
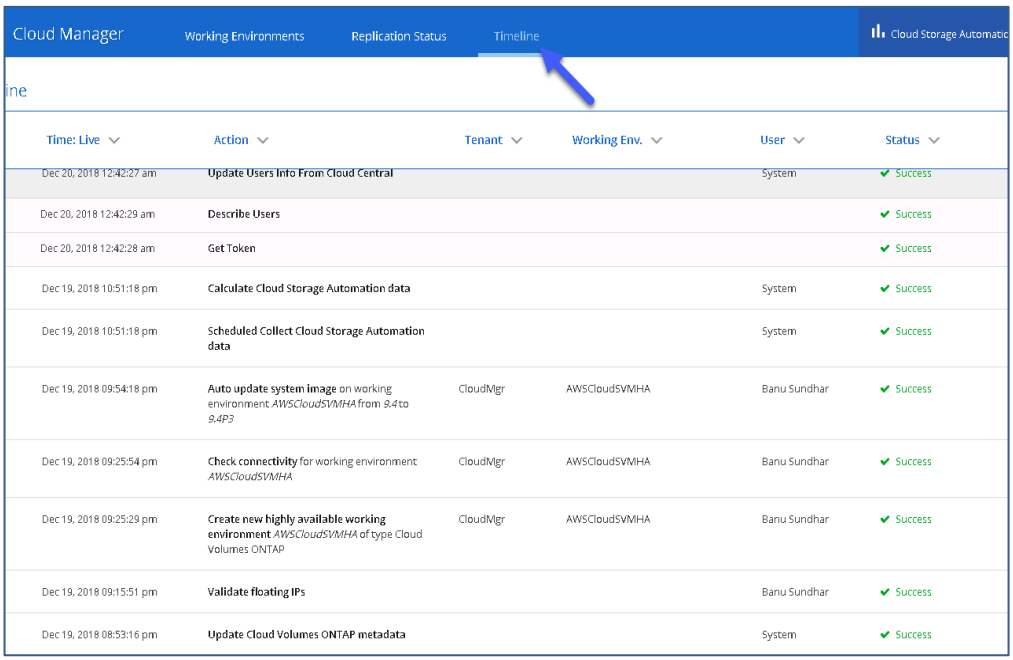
Step	Action
2-13	On the IAM Role page, leave the default recommendation, Let Cloud Manager create the role, and then click **Continue.** 
2-14	On the Licensing page, configure the following information and then click **Continue**. 1. Click **Change Version** and select **ONTAP-9.5** from the list. 2. Click **Cloud Volumes ONTAP Standard**. 3. Select instance type **m4.2xlarge**. 
2-15	On the NetApp Support site credentials page, leave all the fields blank, and then click **Continue**.

Step	Action
2-16	On the Underlying Storage Resources page, select the following, and then click **Continue**. ▪ Select **General Purpose SSD.** ▪ AWS Disk Size: Select **100 GB** from the list. 
2-17	On the WORM page, select **Disable WORM**, and then click **Continue**. 

Step	Action
2-18	On the Create Volume page, configure the following, and then click **Continue**. • Volume Name: **smb_vol1** • Size: **10** • Protocol: **CIFS Protocol** • Leave all other values as the defaults. 
2-19	On the CIFS Setup page, enter the following values, and then click **Continue**. • DNS Primary IP Address: **192.168.0.253** • Active Directory Domain to join: **demo.netapp.com** • Credentials authorized to join the domain: **administrator** and **Netapp1!** 

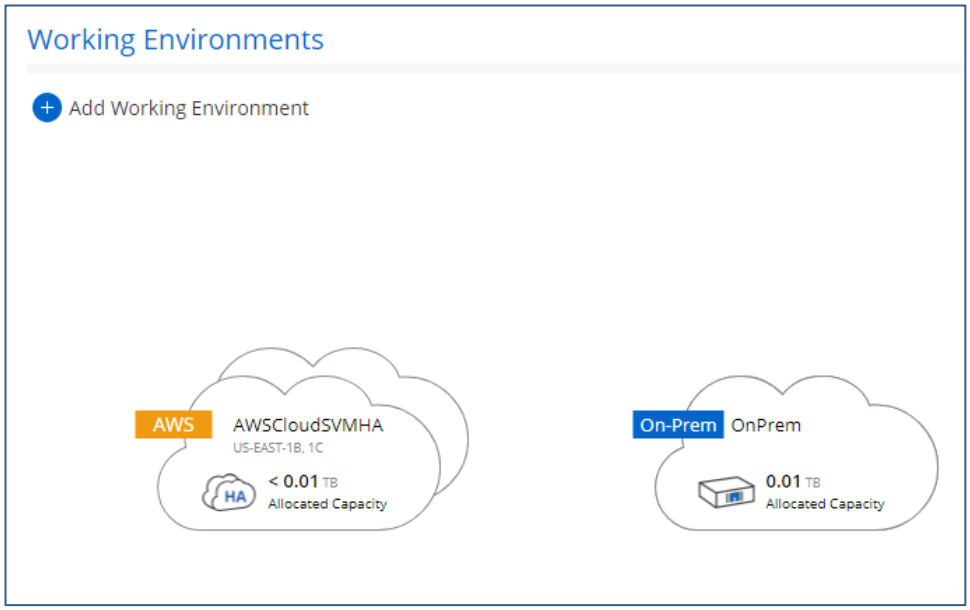
Step	Action
2-20	On the Create Volume – Usage Profile, Disk Type & Tiering Policy page, select **Storage Efficiency**, and then click **Continue**.



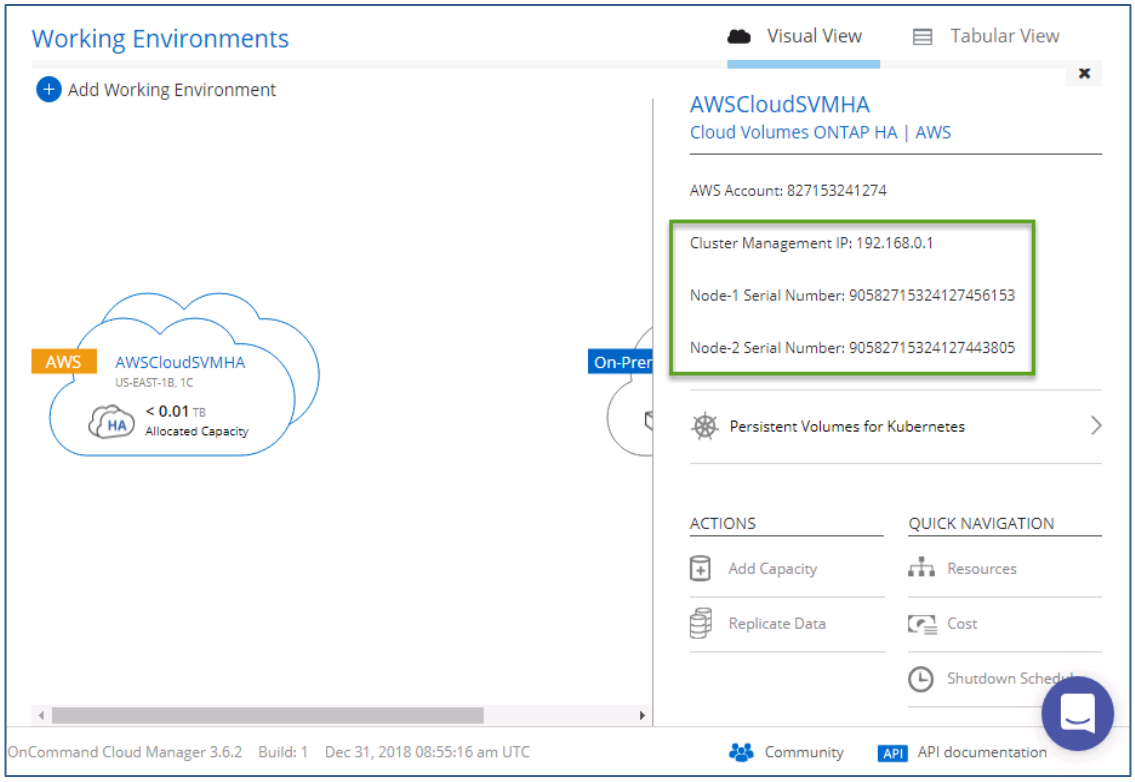
Step	Action
2-21	On the Review & Approve page, review the information, and then complete the following actions: 1. Select the two checkboxes • **I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp**. • **I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements**. 2. Next to both "I understand ..." checkboxes, click **More information** to learn more. 
2-22	Click **Go.**
2-23	It takes about 30 minutes to deploy the Cloud Volumes ONTAP HA pair. You can click Timeline to view the progress. 

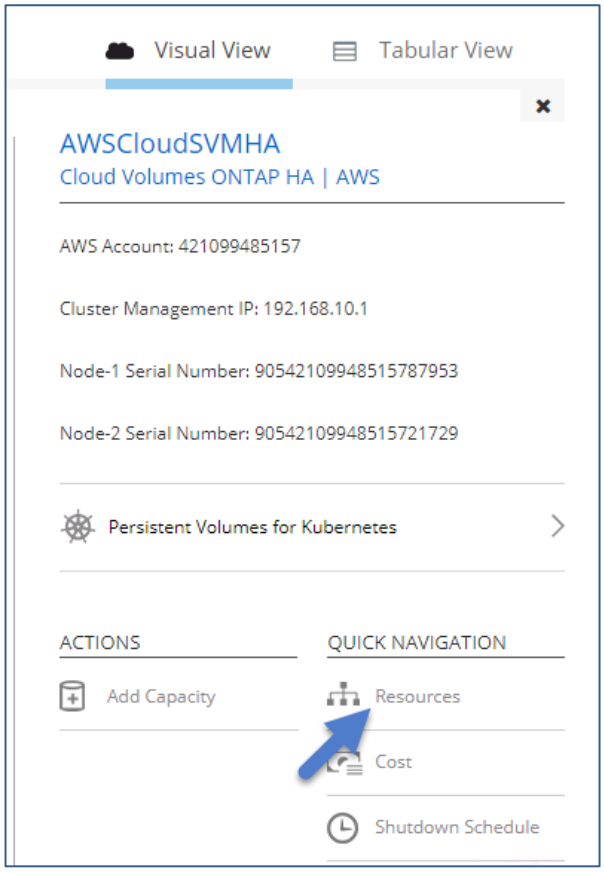
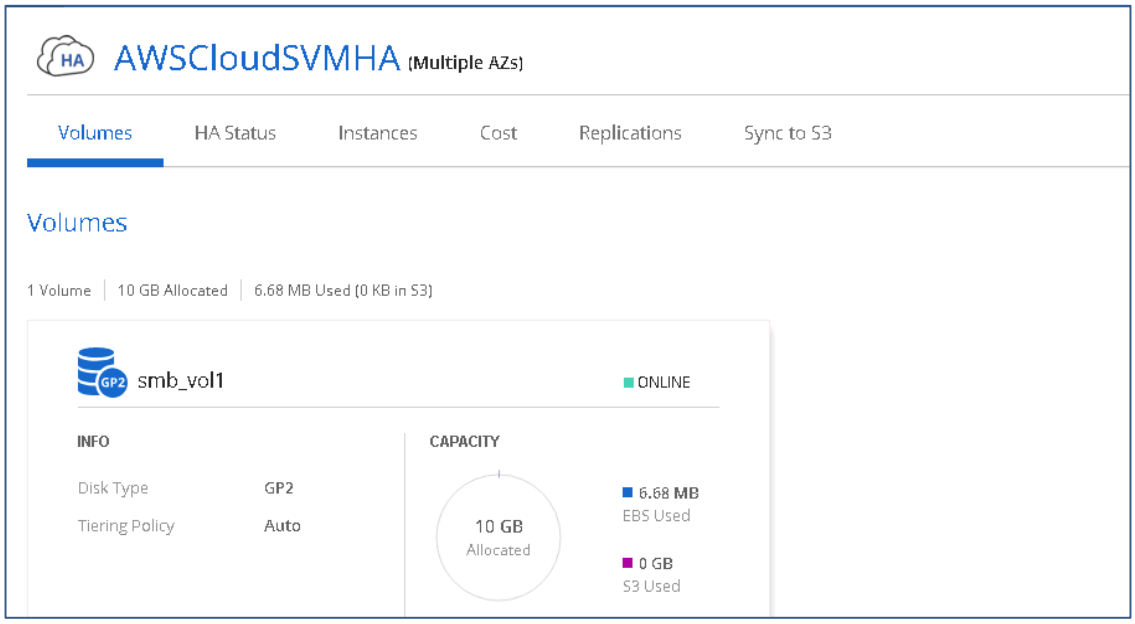
Task 3: Review the Cloud Volumes ONTAP High Availability by Using Cloud Manager

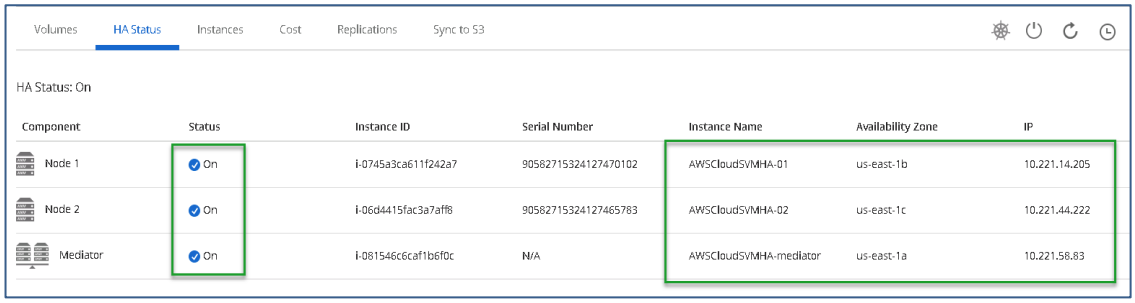
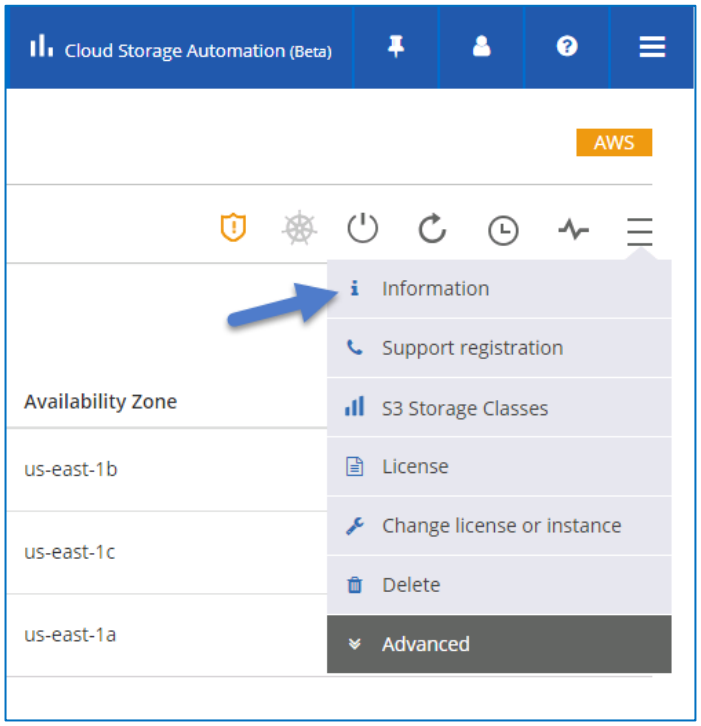
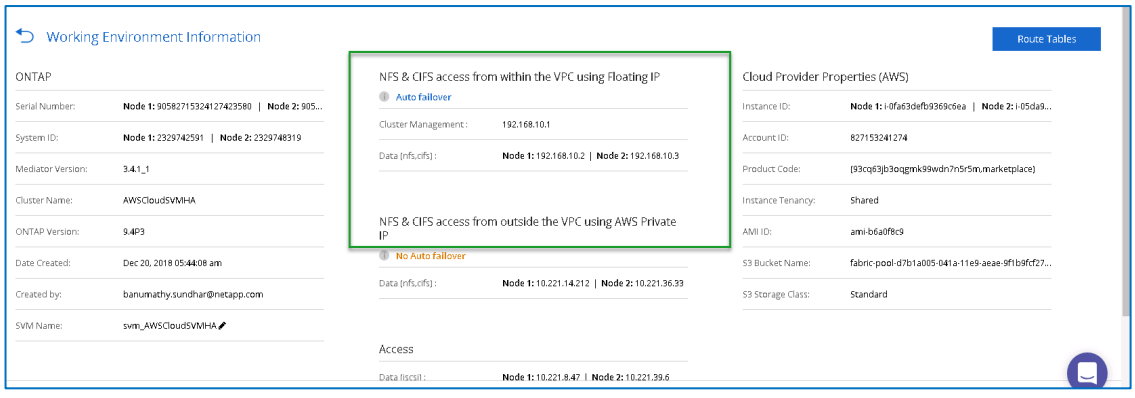
In this task, you review the Cloud Volumes ONTAP high availability nodes that are deployed with the floating IPs for data access and review the SMB volume.

Step	Action
3-1	Go back to the Working Environments in Cloud Manager.
3-2	Verify that you see the following when Cloud Volumes ONTAP high availability has deployed successfully. 

Step	Action
3-3	Click the AWSCloud image in the browser to see the cluster management IP and the node serial numbers on the right.



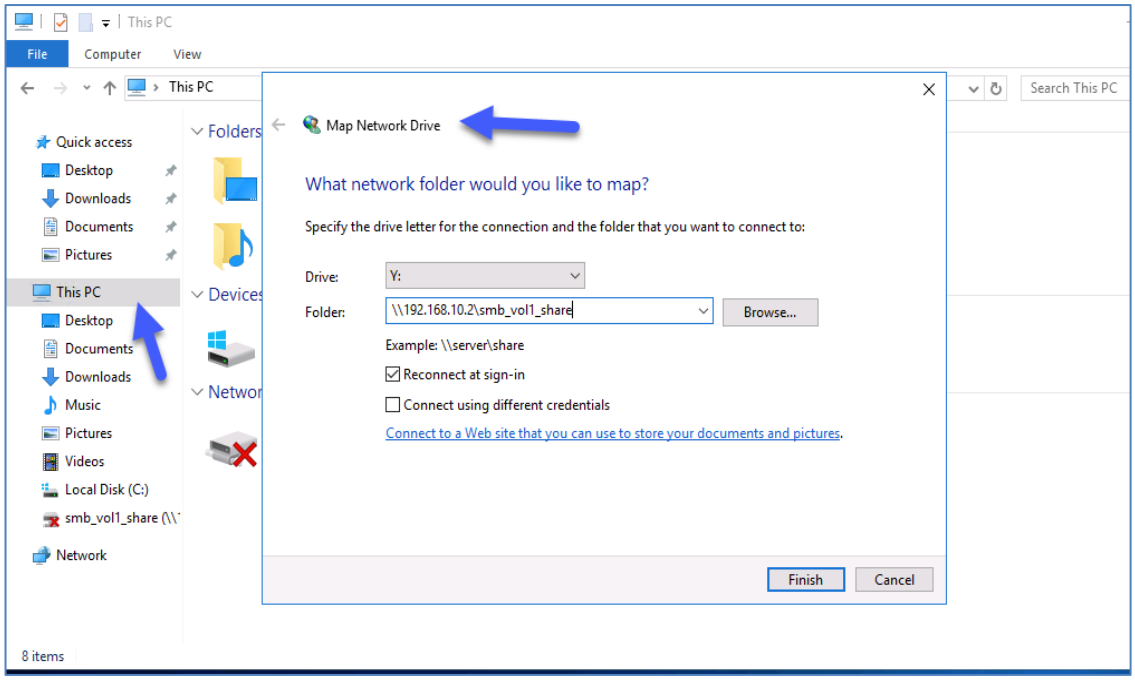
Step	Action
3-4	Under QUICK NAVIGATION, click **Resources**. 
3-5	Verify that you see the Volumes information. 

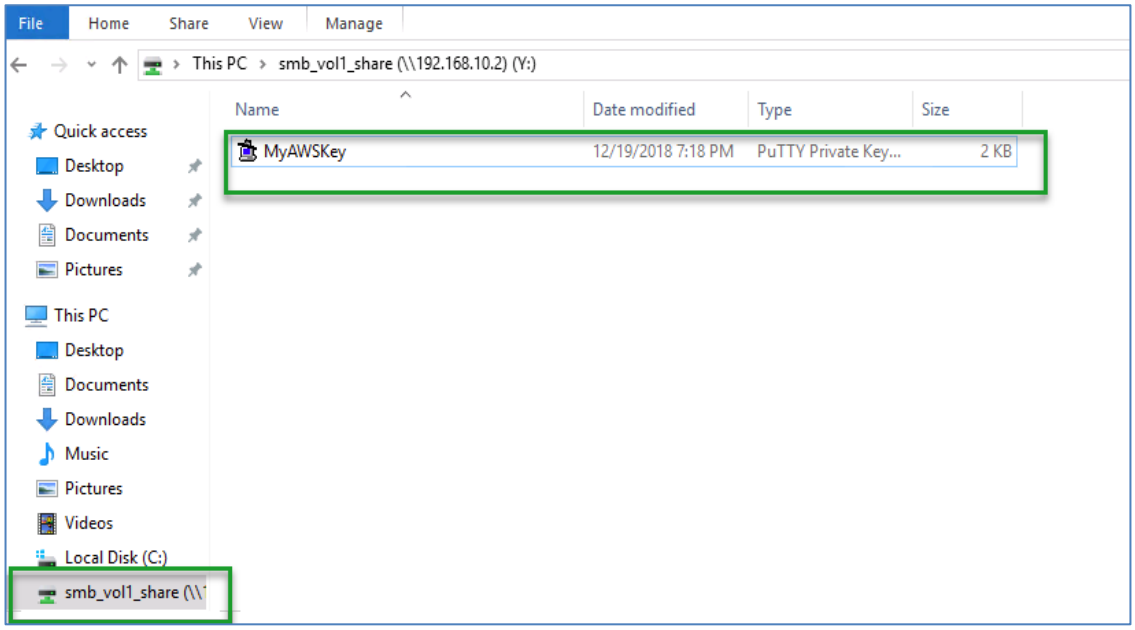
Step	Action
3-6	Click **HA Status** and review the information about the HA nodes and the mediator node. 
3-7	Click the menu icon with 3 bars on the far right, and then click **Information**. 
3-8	Review all information in the Working Environment Information page and pay attention to the NFS & CIFS access from within the VPC using Floating IP, which supports Auto failover. 

Step	Action
3-9	 The data LIFs on Node 1 or Node 2 are floating IPs. The LIF on Node 1 is used in the next task when you are mapping an SMB client to the SMB share on Cloud Volumes ONTAP high availability.

Task 4: Connect an SMB Client to the SMB Volume in Cloud Volumes ONTAP High Availability

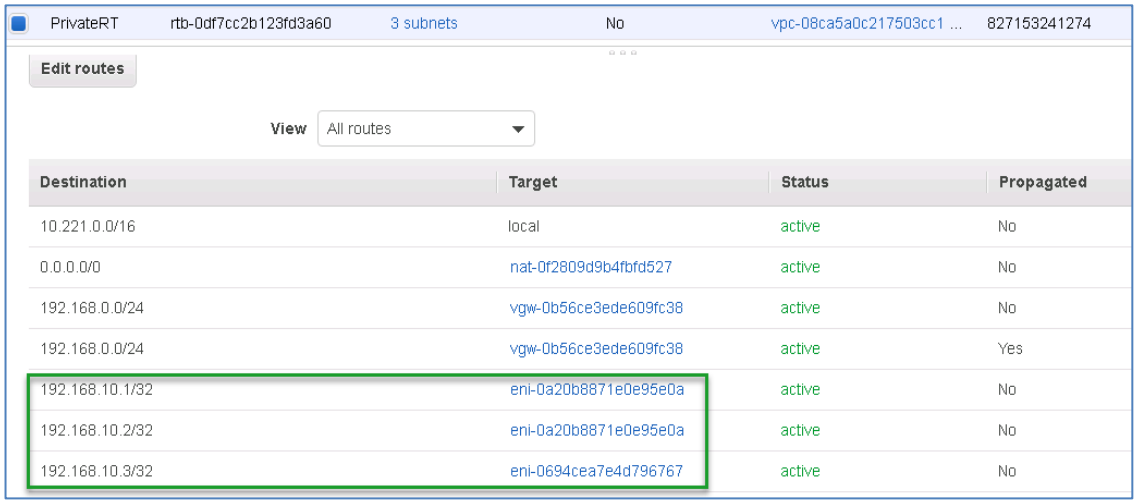
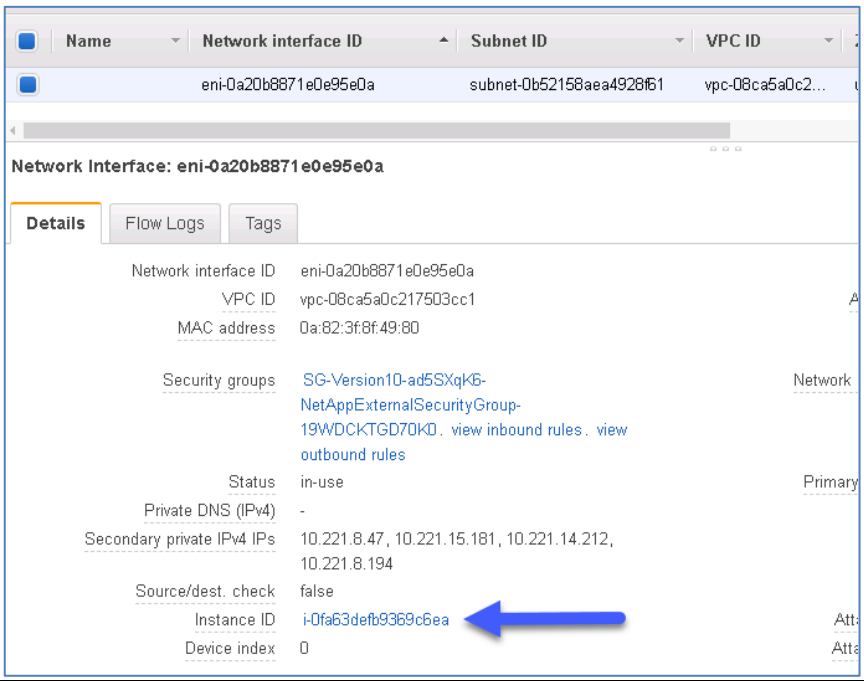
In this task, you connect an SMB client to the SMB volume in your Cloud Volumes ONTAP high availability and write data into it.

Step	Action
4-1	The Cloud Volumes ONTAP HA nodes are in multiple AZs. You provided floating IPs during deployment of Cloud Volumes ONTAP high availability for client data access. The floating IPs are automatically failed over to the partner node in a failover. These floating IPs can be reached by only a client that is within the same VPC to access the share. In the lab, you use the Win2k16_Public instance in the PublicSubnet as your SMB client. You connect to it by using the data LIF on Node 1.
4-2	If you have disconnected from your Win2k16_Public, reconnect to it by using Remote Desktop Protocol (RDP) from your jump host. **Note**: The public IP, user name, and password are in the Win2k16_Public_Login.txt file in the CourseFiles folder.
4-3	Open the File Explorer on the Win2k16_Public instance, and then map a network drive to the SMB share in the Cloud Volumes ONTAP high availability by using the following information: ▪ Folder: **\\192.168.10.2\smb_vol1_share** ▪ User name: **Demo\Administrator** ▪ Password: **Netapp1!** 

Step	Action
4-4	Copy the file MyAWSKey from your downloads folder to the mapped network drive. 

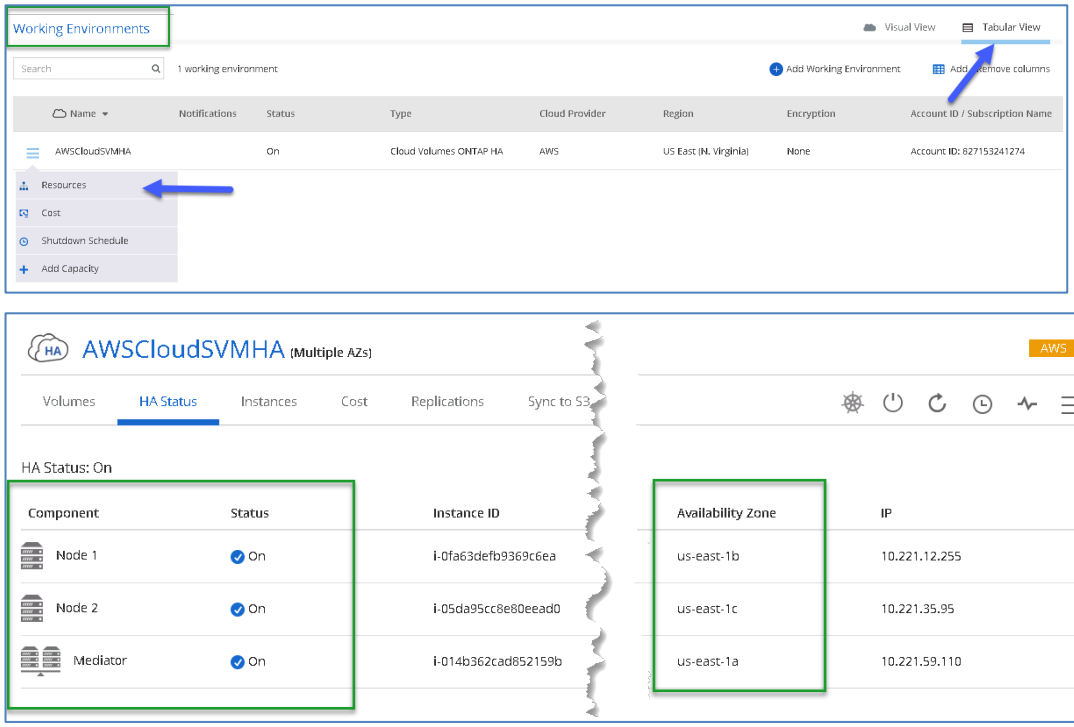
Task 5: Review the Routes in AWS

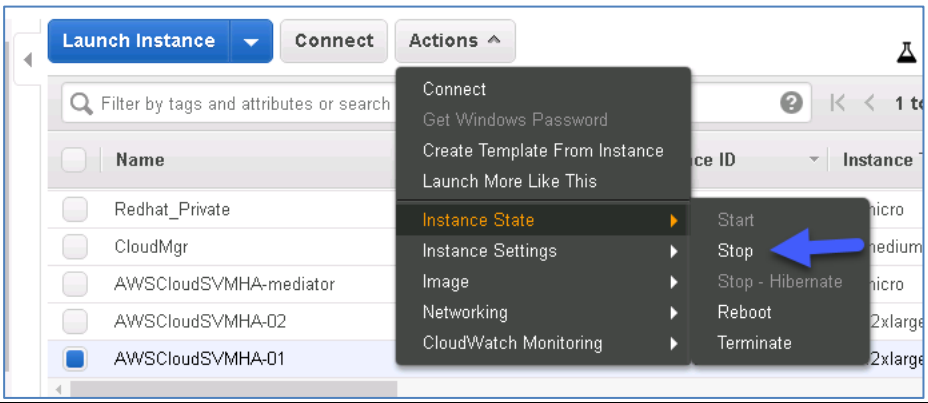
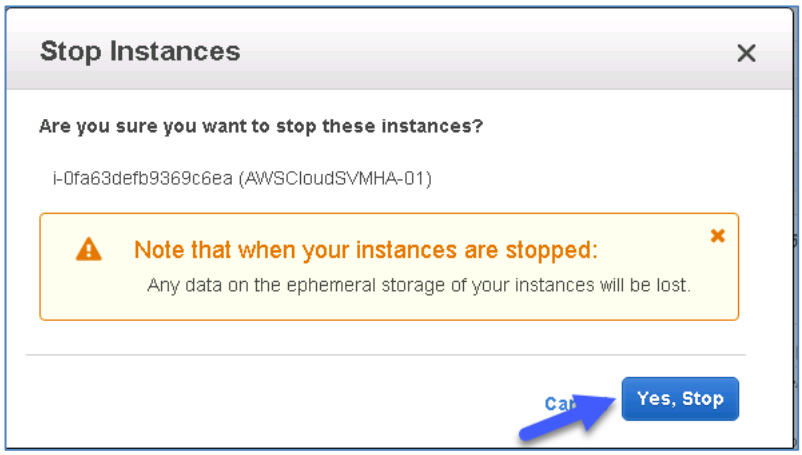
In this task, you review the Route Tables in AWS and verify the target for the data LIF that was used to connect the SMB client in the previous task.

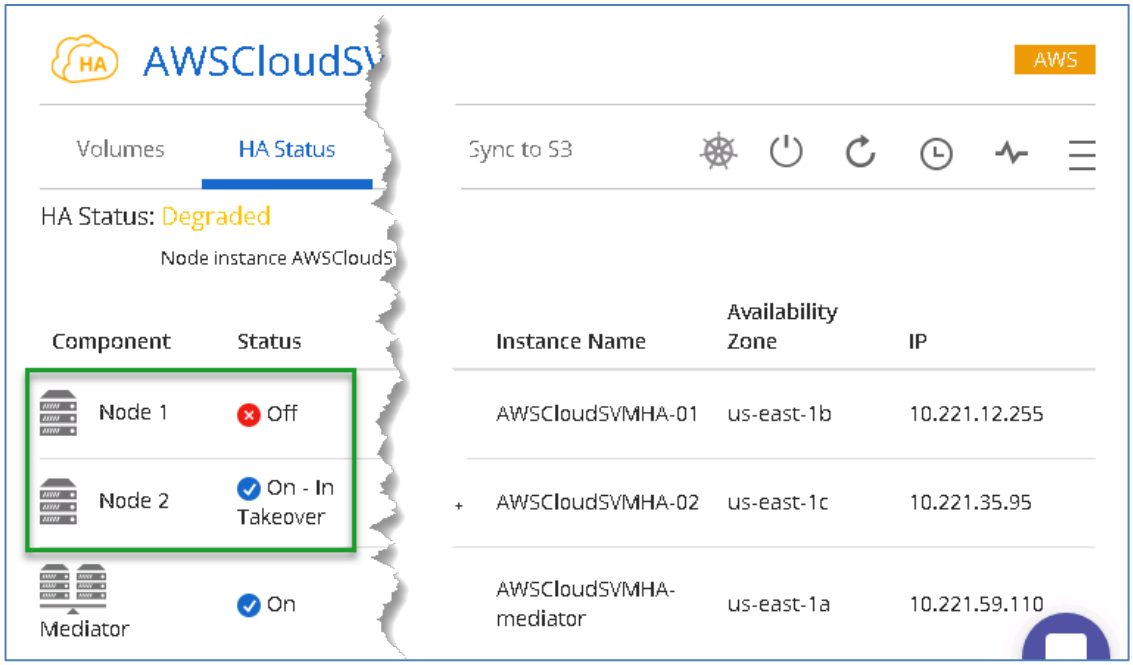
Step	Action
5-1	Return to your browser tab with AWS Console.
5-2	Select **VPC > Route Tables**.
5-3	Select the **Routes** tab, and review the routes for the floating IPs. 
5-4	Click the target eni for the route destination 192.168.10.2/32.
5-5	In the Networking Interfaces page that appears click the Instance ID. 
5-6	Verify that the instance is **AWSCloudSVMHA-01**.

Task 6: Perform a Failover

In this task, you simulate an unplanned shutdown by stopping the Amazon Elastic Compute Cloud (Amazon EC2) instance for the node AWSCloudSVMHA-01.

Step	Action
6-1	In the browser tab for the Cloud Manager UI, review the HA Status.
6-2	You can click Working Environments > Tabular View > Resources > HA Status to review the HA Status. 
6-3	Go back to the Amazon EC2 dashboard, and select **AWSCloudSVMHA-01**.
6-4	You stop this instance to simulate an unplanned failover of the node to its partner. The data LIF (192.168.10.2 for NAS data access) and the cluster management LIF (192.168.10.1) on this node automatically fails over to the partner node AWSCloudSVMHA-02. Clients can continue to access the data without a need to remap a network drive to the share.

Step	Action
6-5	Click **Actions > Instance State > Stop**. 
6-6	In the dialog box, click **Yes, Stop**. 

Step	Action
6-7	Go back to your Cloud Manager UI and review the HA status again. Node 1 is Off after a few minutes. 
6-8	Node 1 status shows Off because the Amazon EC2 instance in AWS has been stopped. Node 2 shows it is in Takeover. This process takes a few minutes.
6-9	Verify that you are still connected to your SMB share on your client.
6-10	You can ensure that you are still connected to your share by clicking your desktop folder and then clicking back on your mapped network drive.

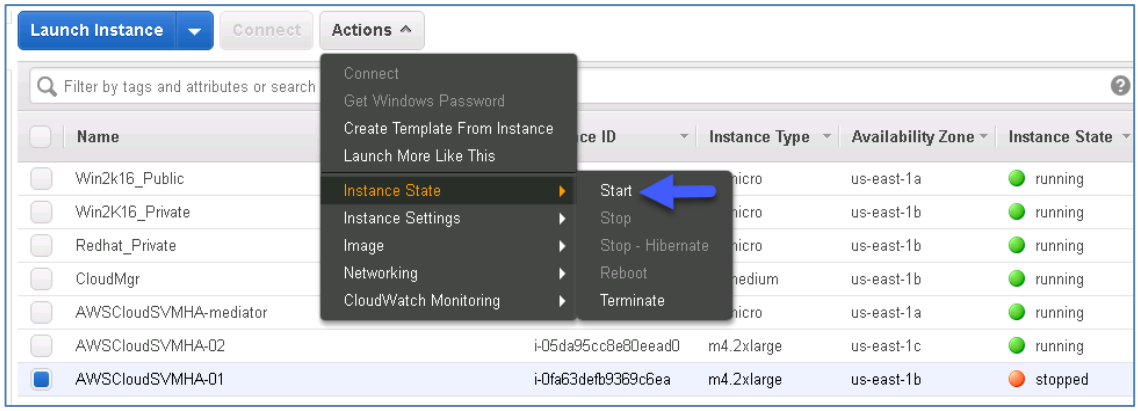
Task 7: Verify That Routes Are Updated After Failover

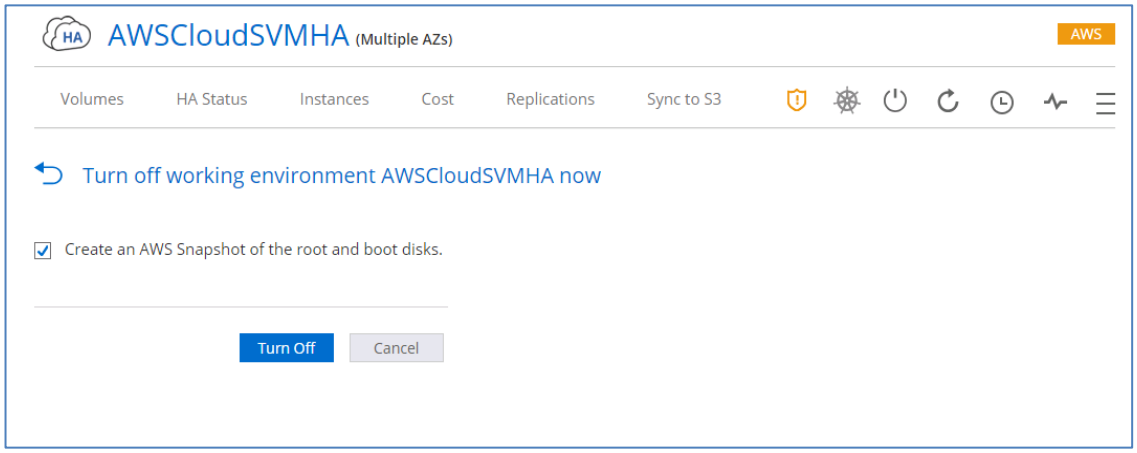
In this task, you confirm the route destination for the data LIF 192.168.10.2 that was used to connect from the client after the failover.

Step	Action
7-1	Repeat the steps in Task 5 to review the target eni for route 192.168.10.2 and the instance that is associated with it.
7-2	Verify that the instance is AWSCloudSVMHA-02.
7-3	 The instance was AWSCloudSVMHA-01 before failover in Task 4. Now, after the failover, the instance is AWSCloudSVMHA-02. The route tables have been automatically updated by the mediator to route the data LIF to the partner destination after the failover.

Task 8: Perform a Failback

In this task, you simulate a failback by starting the stopped Amazon EC2 instance.

Step	Action
8-1	Go back to the Amazon EC2 dashboard, and select **AWSCloudSVMHA-01**.
8-2	Click **Actions > Instance State > Start**. 
8-3	Go back to your Cloud Manager UI and review the HA status again. Node 1 status changes to On after several minutes. 
8-4	Verify that you are still connected to your SMB share on your client.
8-5	Verify that route tables are updated in AWS.

Step	Action
8-6	Power down the AWSCloudSVMHA. This will stop the Cloud Volumes ONTAP instances so that you don't accumulate costs when not in use. (Note: You can turn on the instance when you want to work with it again) a) Return to the Cloud Manager UI b) Go back to Working Environments. c) Double-click AWSCloudSVMHA. d) Click the power button on the top right. e) Click **Turn Off**. 
8-7	This is powering down the entire working environment, both nodes. If you want to power down just a single node you can use OnCommand System Manager. If you are upgrading ONTAP software, Cloud Manager handles the powering down and up of the nodes automatically.

End of Exercise

Module 8: Cloud Sync Service

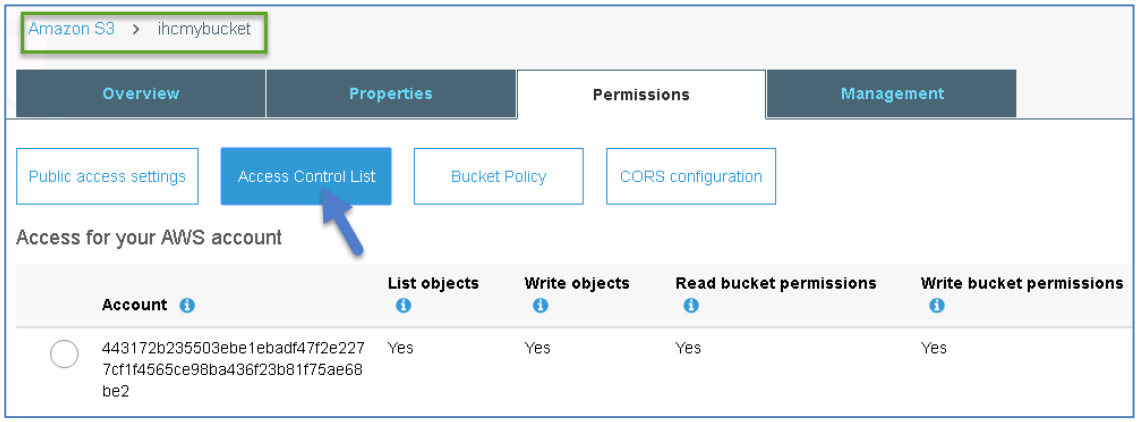
Exercise 1: Synchronize Data From On-Premises to Amazon Simple Storage Service

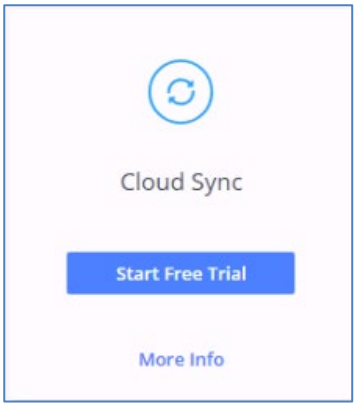
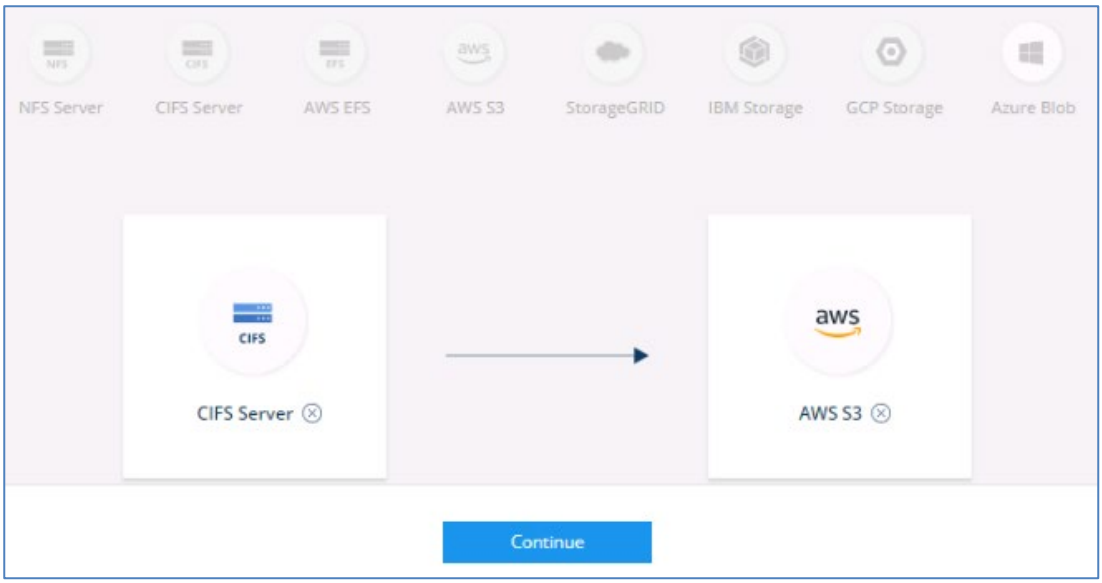
In this exercise, you implement the Cloud Sync service within the Data Fabric to synchronize data between the on-premises cluster and Amazon Simple Storage Service (Amazon S3 or S3).

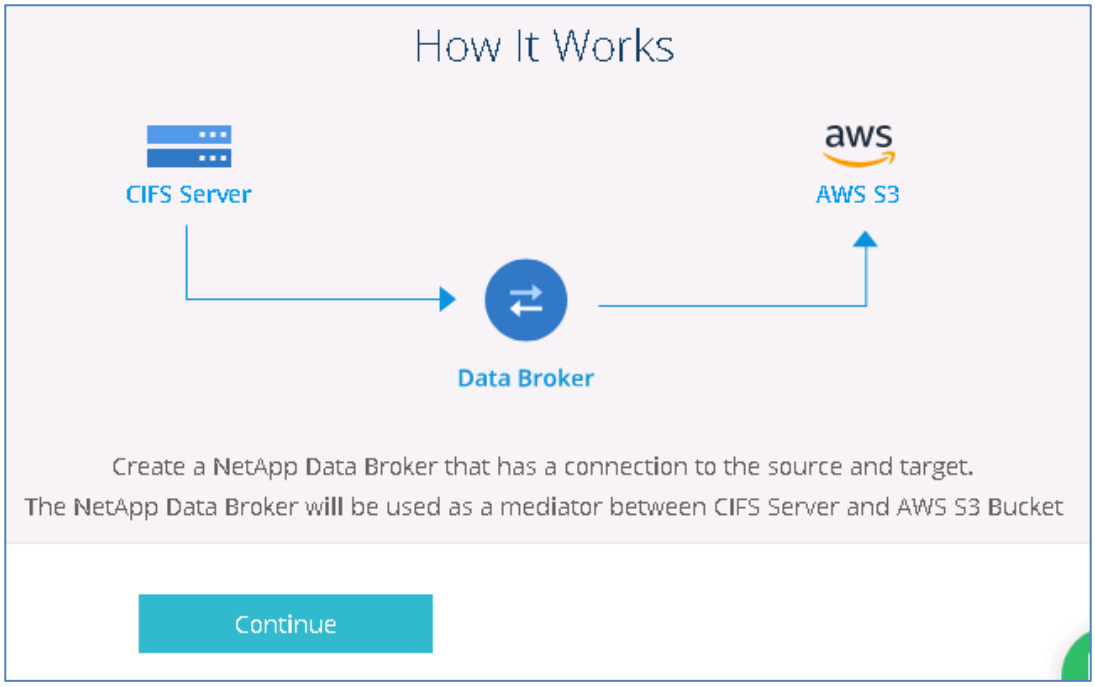
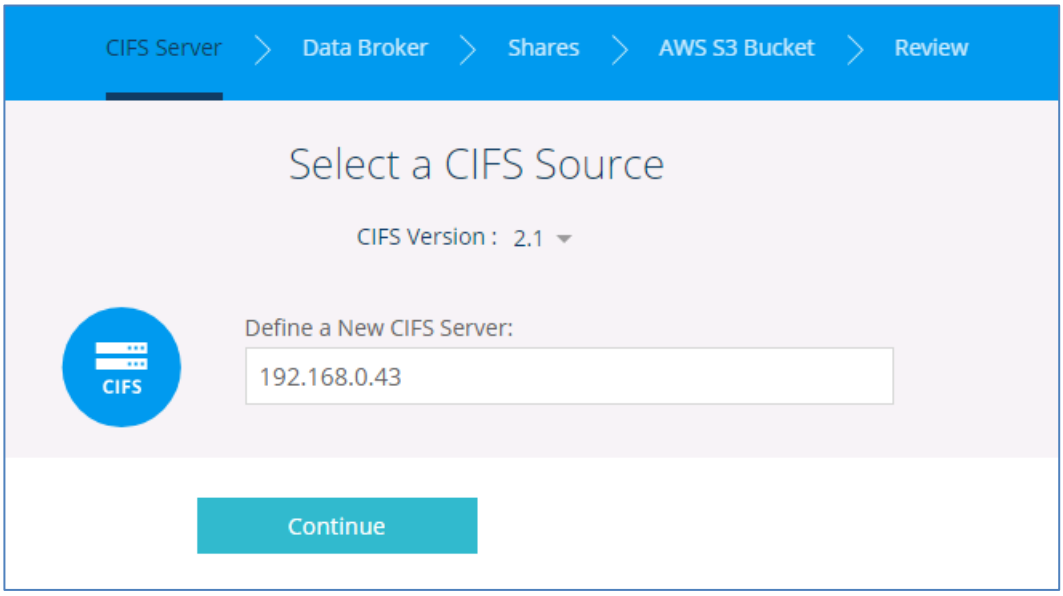
Objectives

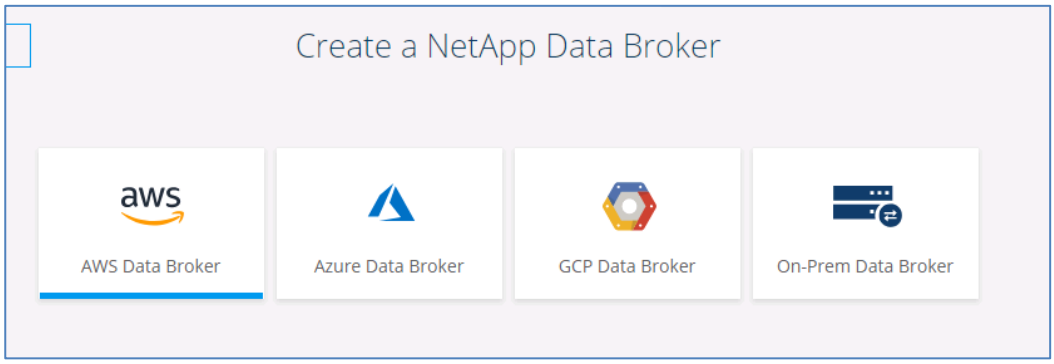
This exercise focuses on enabling you to apply your Data Fabric knowledge, including an understanding of Amazon Web Services (AWS) architectures, to implement the Cloud Sync service.

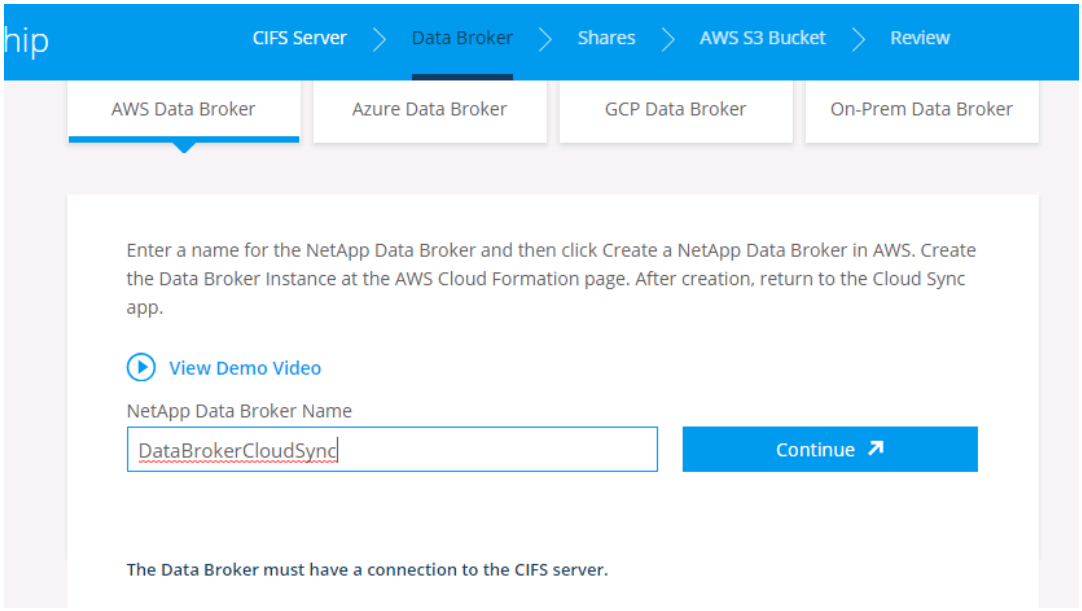
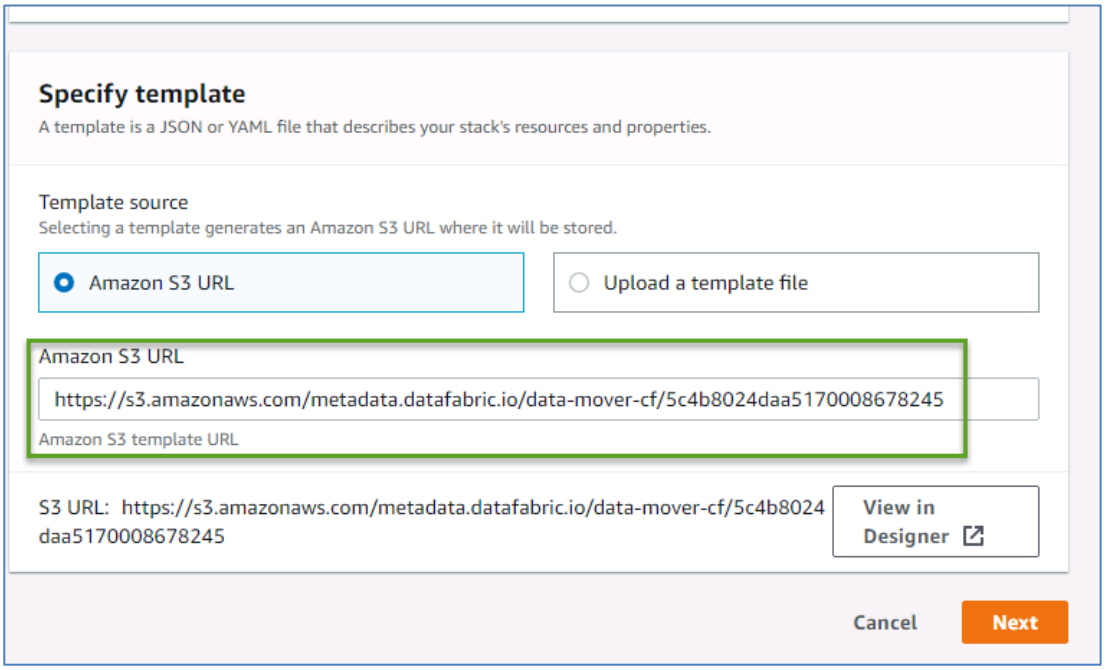
Task 1: Deploy the Cloud Sync Service

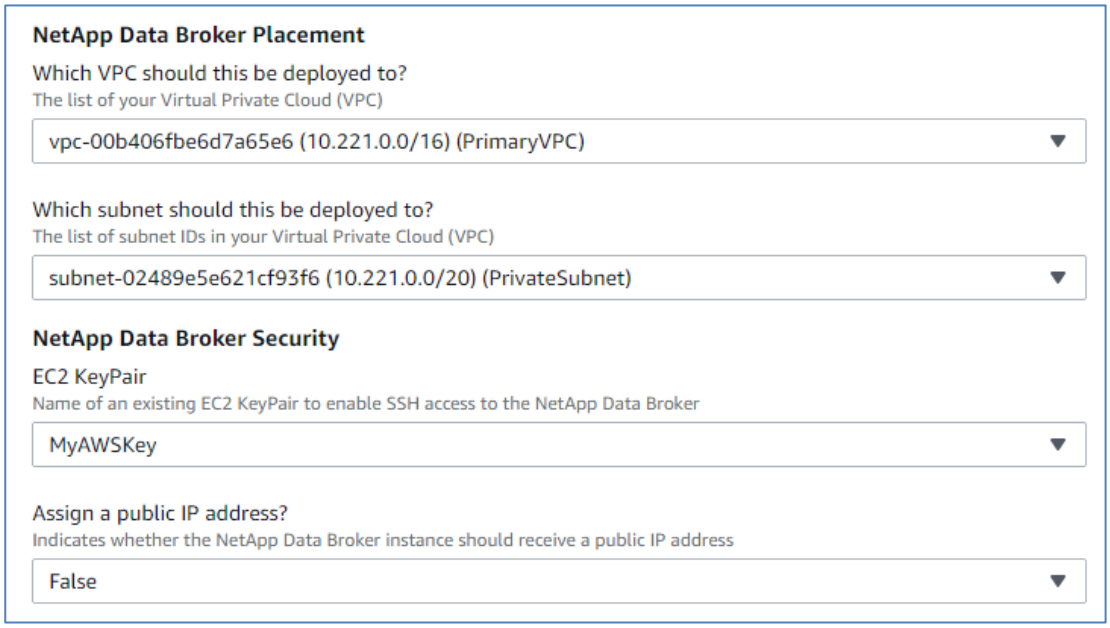
Step	Action
1-1	Create an empty S3 bucket for the Cloud Sync service to use by going to the AWS console and doing the following: a. Select **Services** > **S3**. b. Click **Create bucket**. c. For bucket name, enter anything unique. d. Click **Create**. **NOTE:** The bucket permissions must enable your AWS account's user ID, which is configured in the access control list by default. 

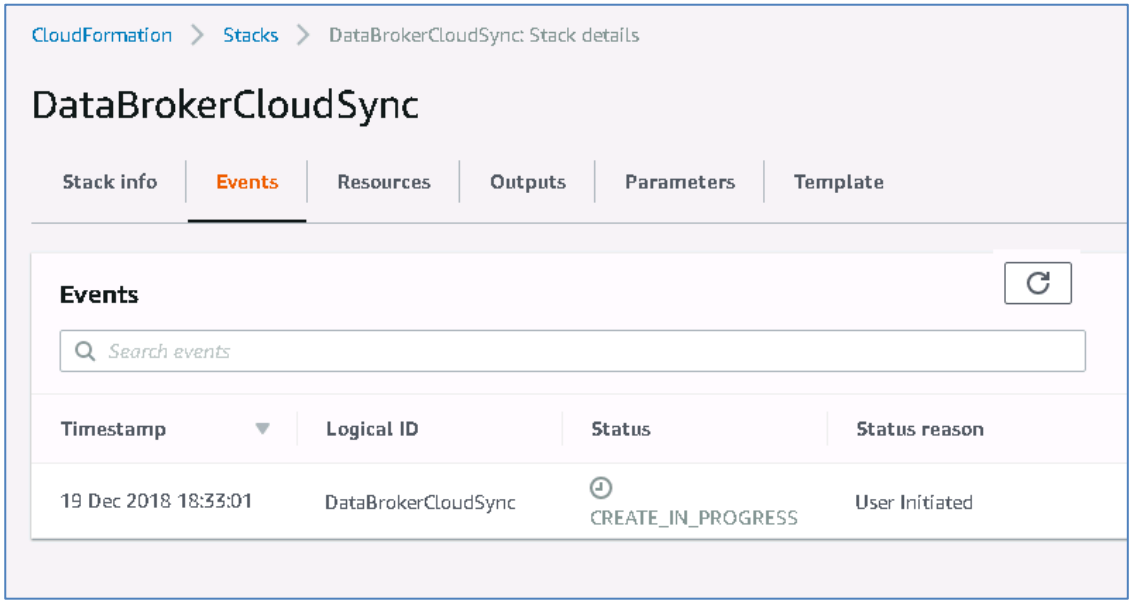
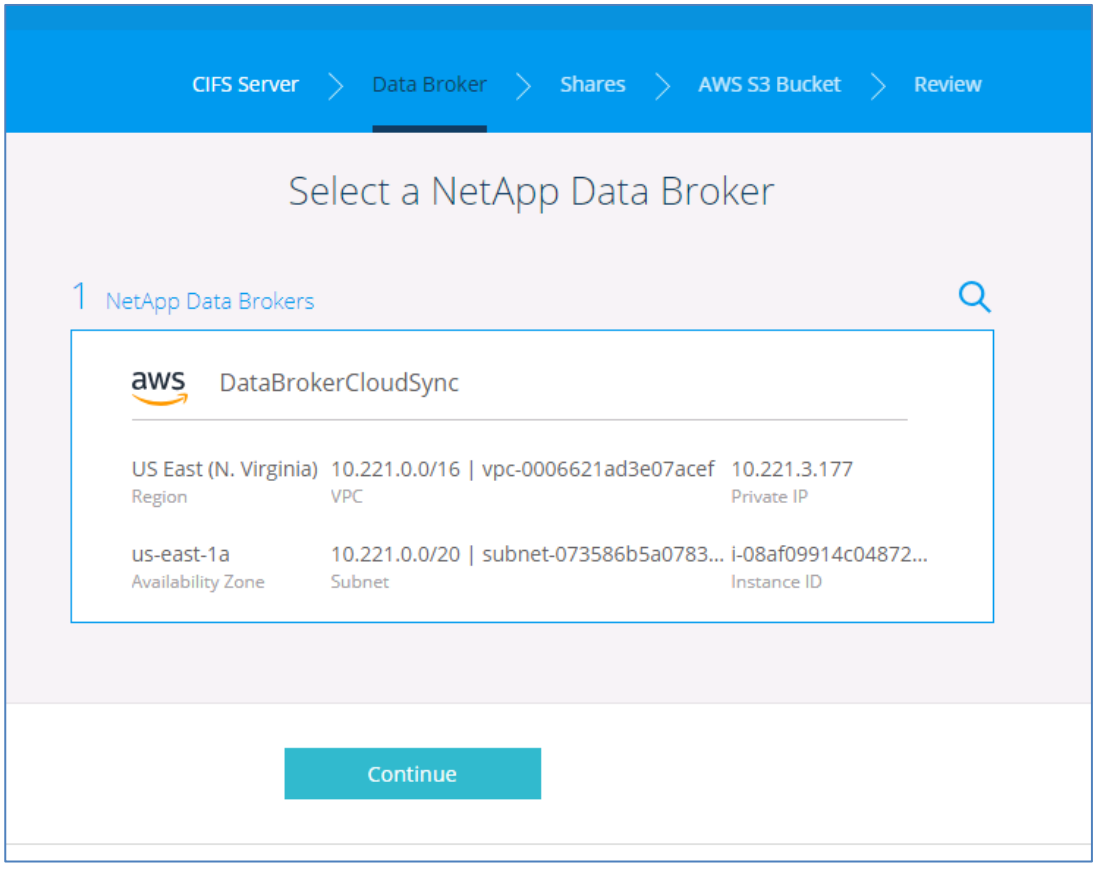
Step	Action
1-2	Go to cloud.netapp.com and click **Start Free Trial**. 
1-3	Drag the CIFS Server icon to the source bubble and drag the AWS S3 icon to the destination bubble. Note: You may have to reduce the font size of your web browser for example use <CTRL -- > to see the source and destination bubbles. 
1-4	Click **Continue**.

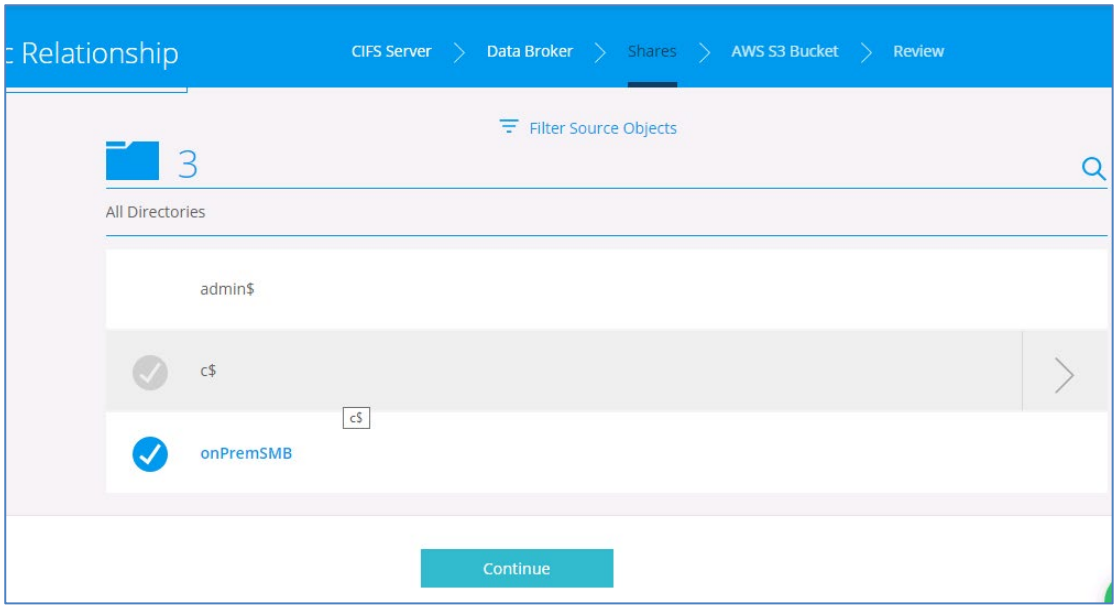
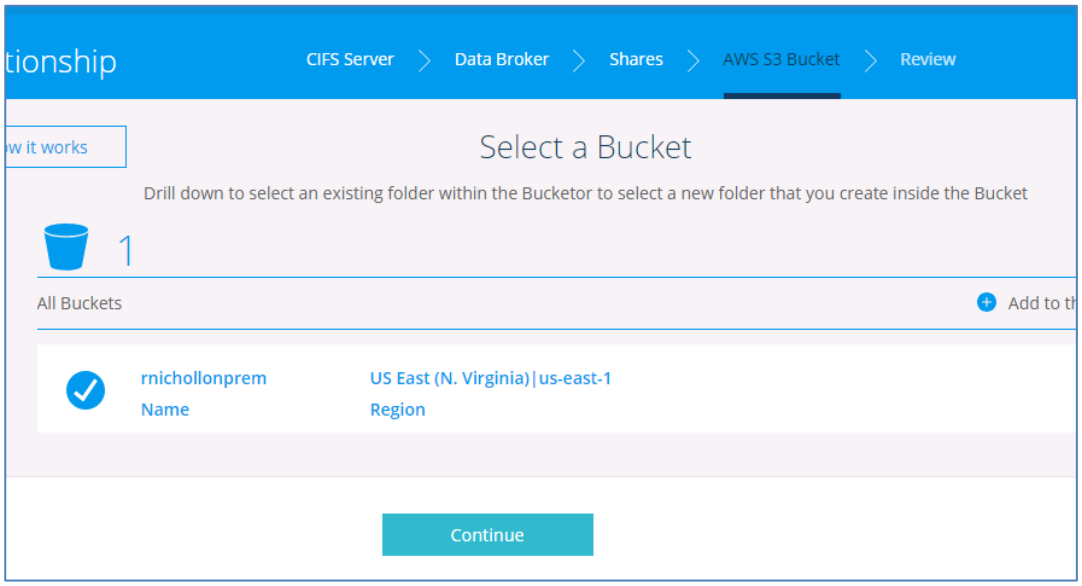
Step	Action
1-5	Click **Continue**. 
1-6	Enter the Data LIF of the on-premises storage virtual machine (SVM) **192.168.0.43**, and then click **Continue.**  :

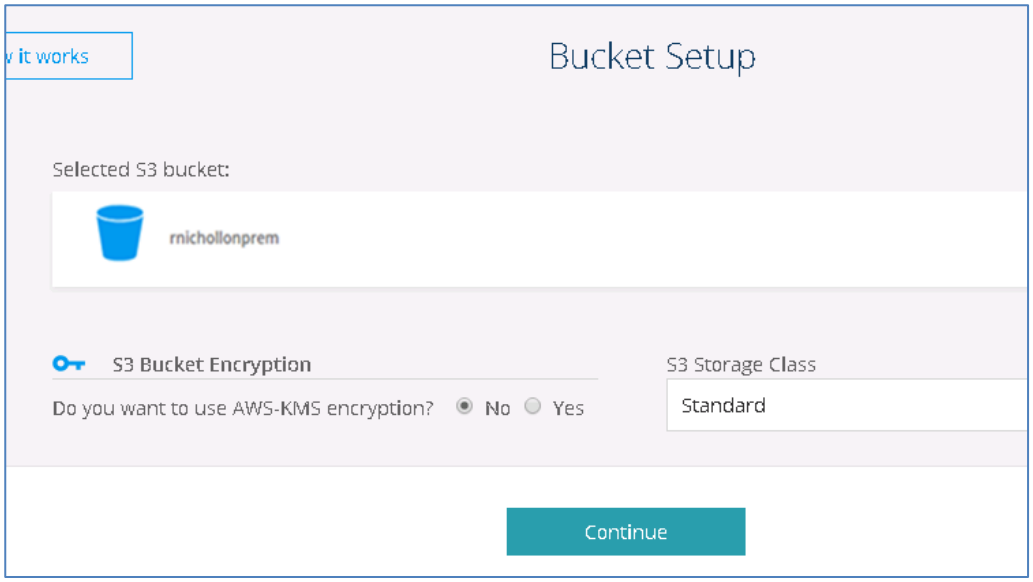
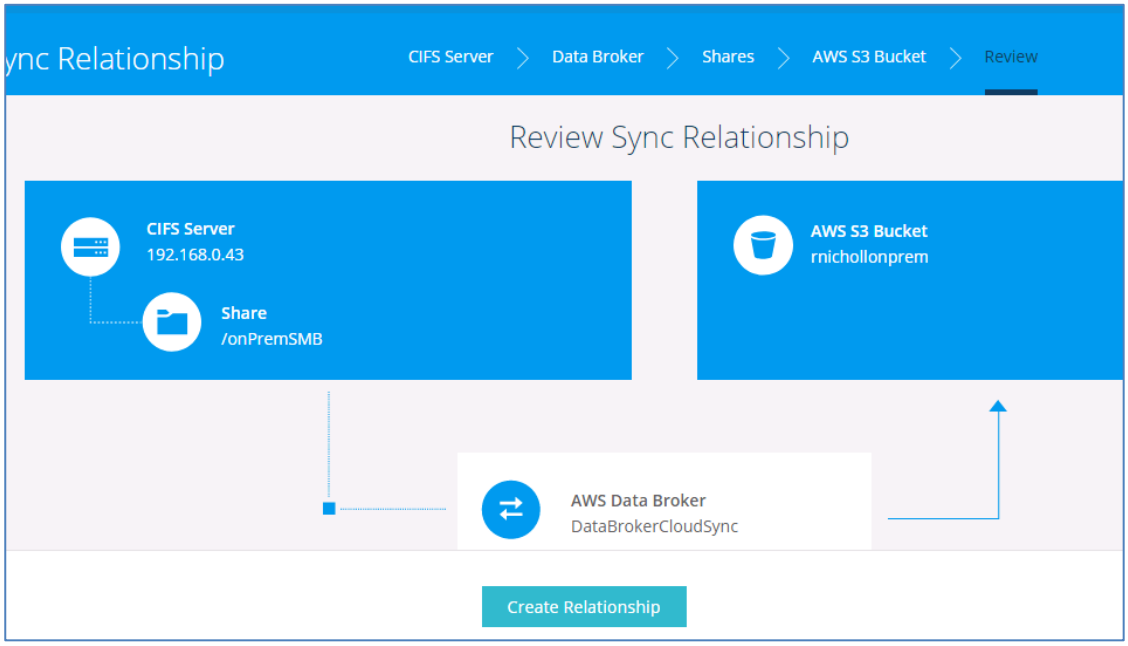
Step	Action
1-7	Enter the following CIFS credentials: • User Name: **Administrator** • Password: **Netapp1!** • Domain: **Demo** 
1-8	Click **Continue**.
1-9	Click **AWS Data Broker**. 
1-10	You can click **View Demo Video** link to watch the procedure for launching a Data Broker in AWS. You can also follow the instructions shown below.

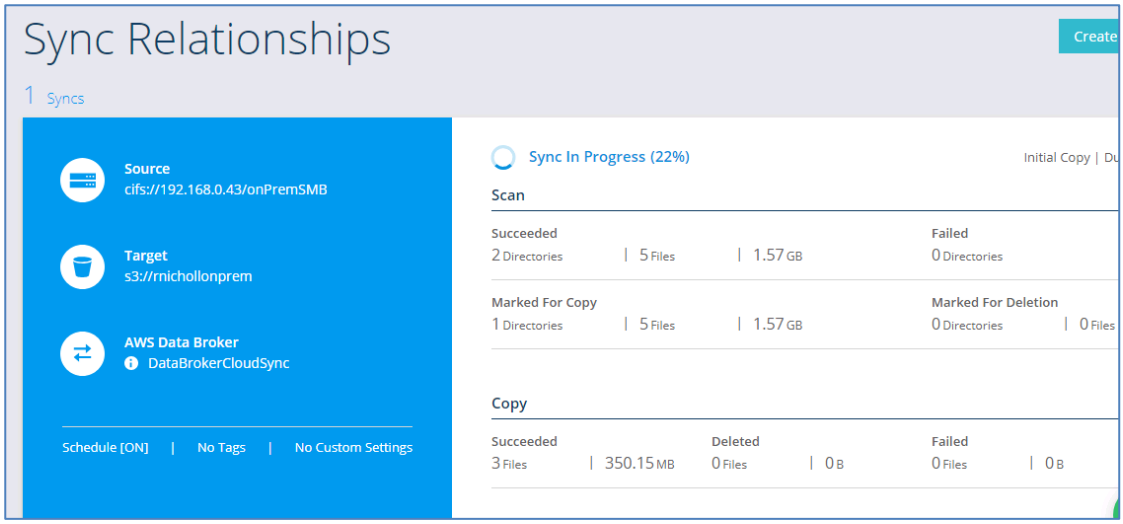
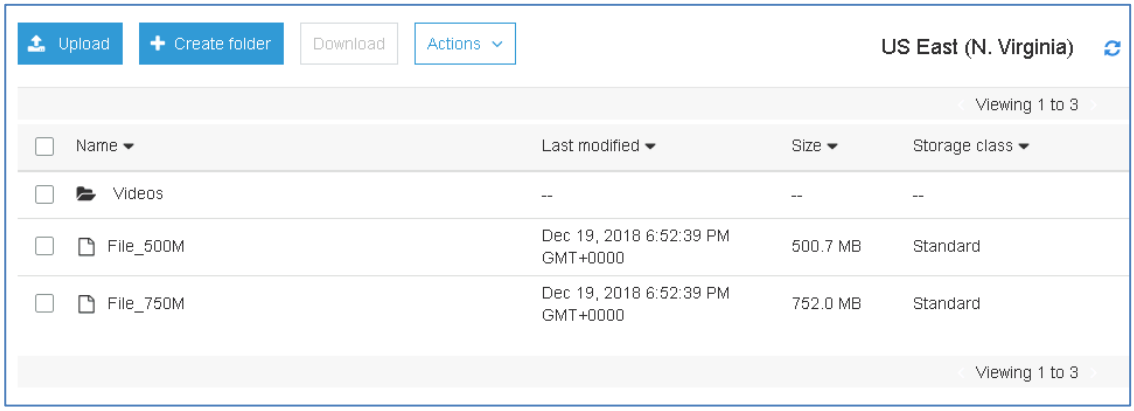
Step	Action
1-11	Enter the NetApp Data Broker Name **DataBrokerCloudSync**, and then click **Continue**. 
1-12	In the Cloud Formation Create Stack page, verify that an S3 URL is prepopulated and click **Next**. 

Step	Action
1-13	In the Specify stack details, do the following: • For Which VPC should this be deployed to, select **Primary VPC**. • For Which subnet should this be deployed to select **PrivateSubnet**. • For the EC2 KeyPair select **MyAWSKey**. • For Assign a public IP address, select **False**. • Leave all other values as default and click **Next**. 
1-14	On the Configure stack options page, leave all values as default and click **Next**.
1-15	On the Review page, scroll to the bottom of the page, select the **I acknowledge that AWS CloudFormation might create IAM resources** checkbox, and then click **Create stack**.

Step	Action
1-16	To watch CloudFormation stack, might need to press refresh to see DataBrokerCloudSync stack appear. 
1-17	When CloudFormation reaches the Status CREATE_COMPLETE, return to the Cloud Sync tab, and click **Continue**. 

Step	Action
1-18	Select **onPremSMB**, and click **Continue**. 
1-19	Select your bucket, and click **Continue**. 

Step	Action
1-20	In the Bucket Setup page, click **Continue**. 
1-21	Click **Create Relationship**. 

Step	Action
1-22	Click **View in Dashboard**. 
1-23	Return to the AWS Console, and verify that contents exist in your S3 bucket. 

End of Exercise

Module 9: NetApp Cloud Volumes Service

Exercise 1: Create NFS and CIFS Volumes

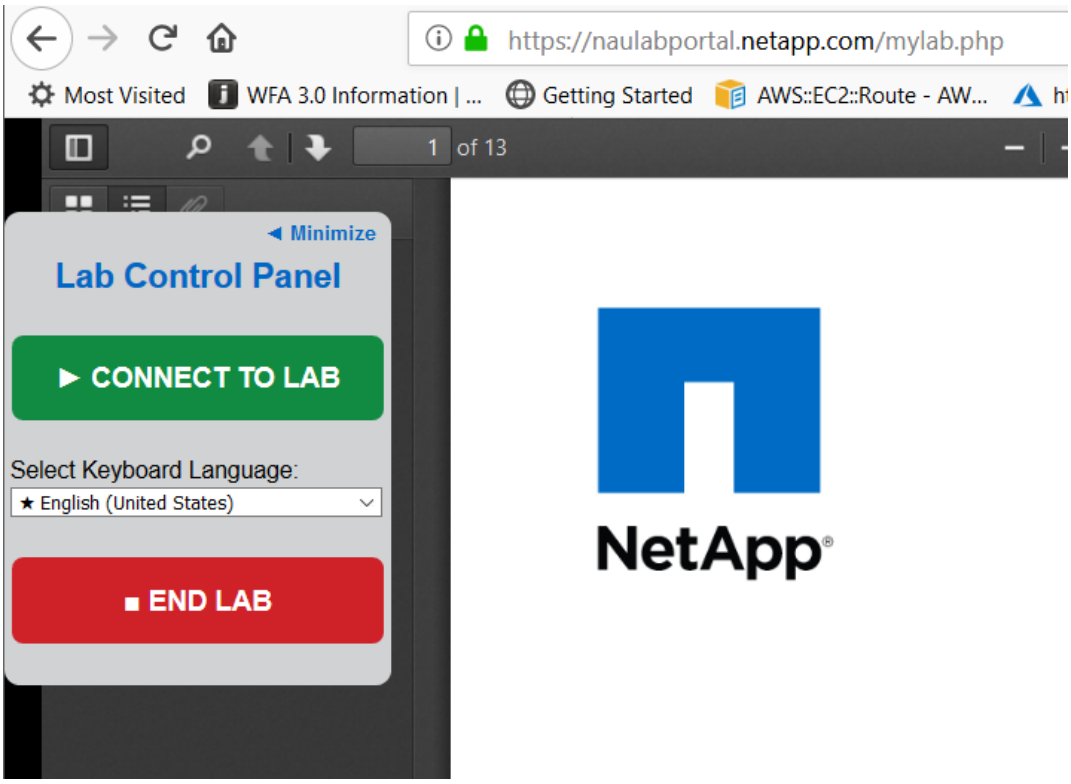
In this exercise, you tier secondary data from Cloud Volumes ONTAP to Amazon Simple Storage Service (Amazon S3).

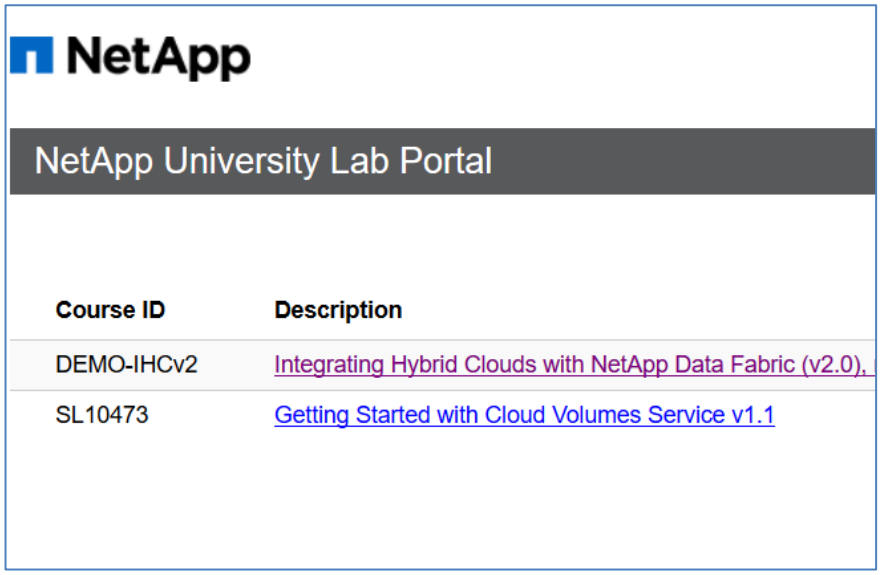
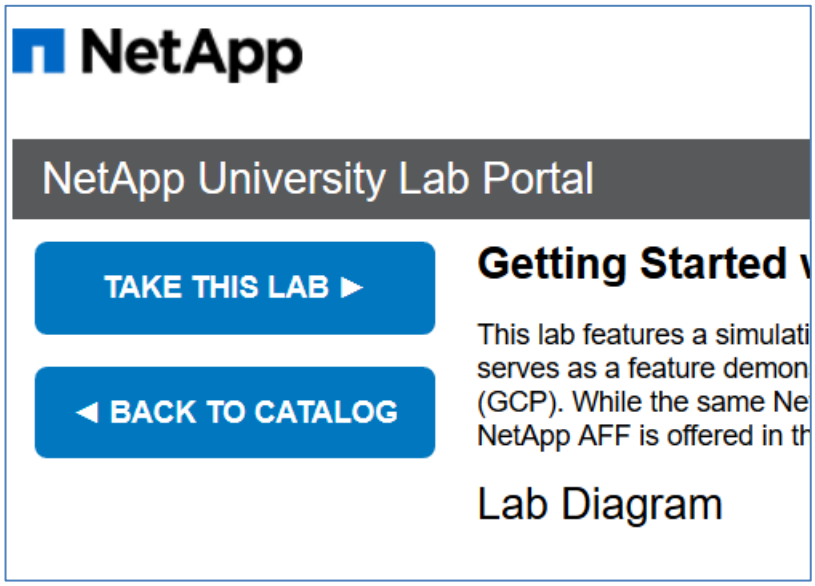
Objectives

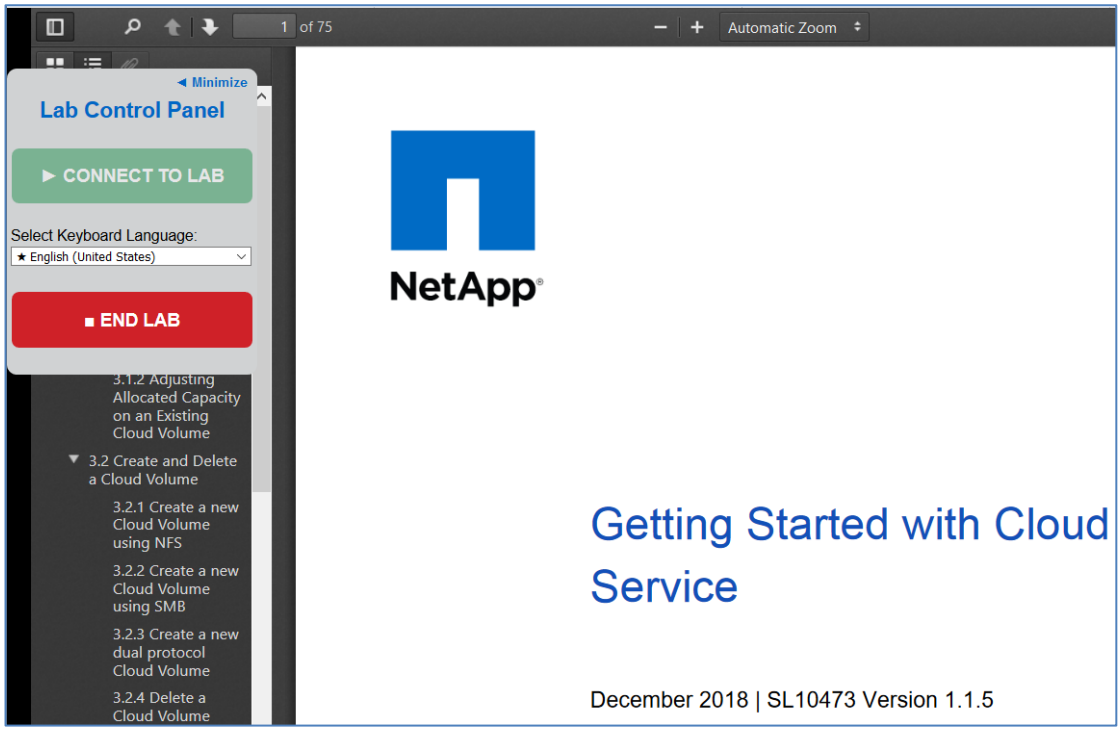
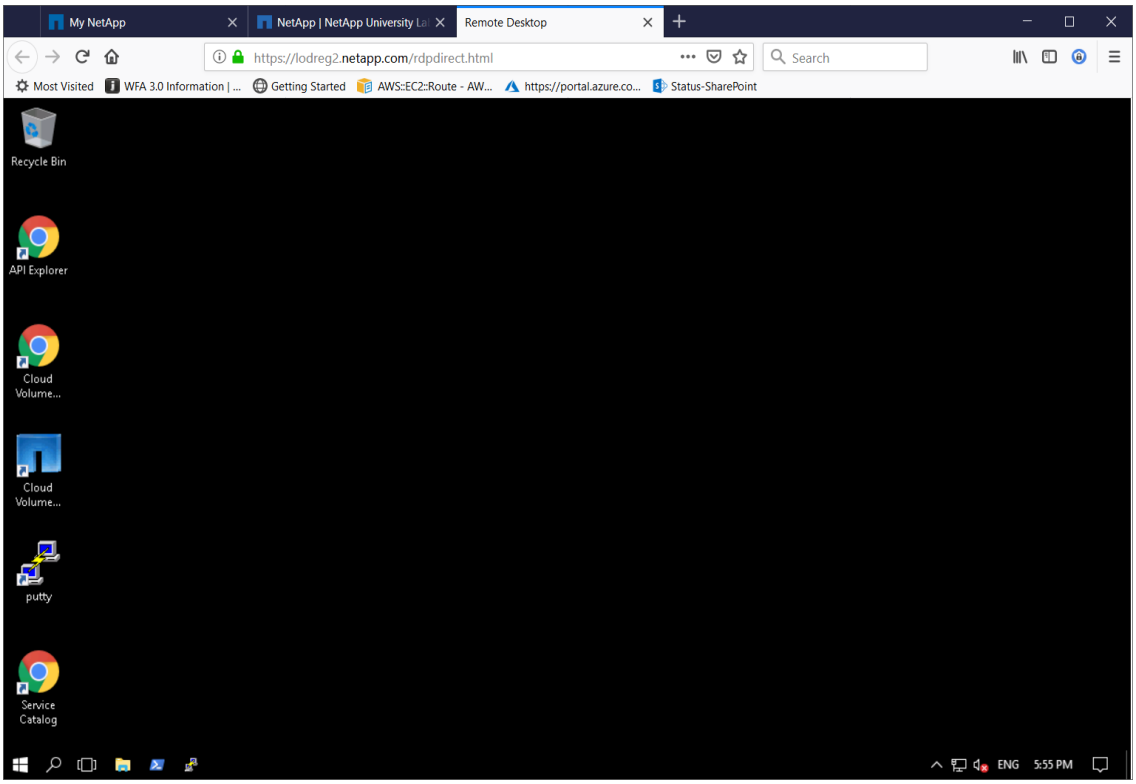
This exercise focuses on enabling you to do the following:

- Create NFS and CIFS volumes using Cloud Volumes Service
- Use clients to mount and access Cloud Volumes.

Task 1: Access Lab On Demand Kit

Step	Action
1-1	Open a new browser tab and then enter http://naulabportal.netapp.com
1-2	Log in with the credentials provided by your instructor.
1-3	Click **END LAB**. 

Step	Action
1-4	Click **Getting Started with Cloud Volumes Service 1.1**. 
1-5	Click **TAKE THIS LAB**. 
1-6	Click OK.

Step	Action
1-7	Verify that the lab guide appears in your browser tab. 
1-8	Click **CONNECT TO LAB**.
1-9	Verify a new tab is opened with the jump host desktop. 
1-10	Do the steps in **Task 3.1.1 Tour the Web Interface.**

Step	Action
1-11	Do the steps in **Task 3.2.1 – Create a New Cloud Volume using NFS**.
1-12	Do the steps in **Task 3.2.2 – Create a New Cloud Volume using SMB**.
1-13	Do the steps in **Task 3.4.1 - Mount an NFS Cloud Volume to a Compute resource**.
1-14	Do the steps in **Task 3.4.2 - Access an SMB Cloud Volume share from a client**. Note: use the newSMBvol4app volume in place of the newDUALvol4app volume.

End of Exercise