

NETAPP UNIVERSITY

Integrating Hybrid Clouds with NetApp Data Fabric

Exercise Guide
Content Version 3



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

© 2019 NetApp, Inc. All rights reserved. Printed in the U.S.A. Specifications subject to change without notice.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of NetApp, Inc.

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

WELCOME.....	E-1
MODULE 0: INTRODUCTION	
<i>EXERCISE 0: CHECKING THE LAB EQUIPMENT</i>	<i>M0-E0-1</i>
MODULE 1: DATA FABRIC OVERVIEW	
<i>EXERCISE 1: CONTROL CLOUD RESOURCES WITH WINDOWS POWERSHELL</i>	<i>M1-E1-1</i>
<i>EXERCISE 2: ASSESS AZURE AND AMAZON WEB SERVICES ENVIRONMENTS.....</i>	<i>M1-E2-1</i>
MODULE 2: AWS VPC AND CONNECTIVITY TO OTHER NETWORKS	
<i>EXERCISE 1: CONFIGURE AWS VIRTUAL PRIVATE CLOUD RESOURCES</i>	<i>M2-E1-1</i>
<i>EXERCISE 2: OPERATIONALIZE ON-PREMISES TO CLOUD CONNECTIVITY.....</i>	<i>M2-E2-1</i>
MODULE 3: NETAPP CLOUD VOLUMES ONTAP	
<i>EXERCISE 1: USING ONCOMMAND CLOUD MANAGER.....</i>	<i>M3-E1-1</i>
MODULE 4: IMPLEMENTING DISASTER RECOVERY	
<i>EXERCISE 1: CONFIGURE AND MANAGE DISASTER RECOVERY IN THE DATA FABRIC.....</i>	<i>M4-E1-1</i>
MODULE 5: AZURE VIRTUAL NETWORK AND CONNECTIVITY	
<i>EXERCISE 1: CONFIGURING AZURE VIRTUAL NETWORK TO ON-PREMISES VPN</i>	<i>M5-E1-1</i>
MODULE 6: NETAPP CLOUD VOLUMES ONTAP DATA TIERING	
<i>EXERCISE 1: TIER BACKUP DATA TO AMAZON SIMPLE STORAGE SERVICE.....</i>	<i>M6-E1-1</i>
MODULE 7: NETAPP CLOUD VOLUMES ONTAP HIGH AVAILABILITY	
<i>EXERCISE 1: IMPLEMENT CLOUD VOLUMES ONTAP HIGH AVAILABILITY</i>	<i>M7-E1-1</i>
MODULE 8: CLOUD SYNC SERVICE	
<i>EXERCISE 1: SYNC DATA FROM ON-PREMISES TO AMAZON SIMPLE STORAGE SERVICE ...</i>	<i>M8-E1-1</i>
MODULE 9: NETAPP CLOUD VOLUMES SERVICE	
<i>EXERCISE 1: CREATE NFS AND CIFS VOLUMES.....</i>	<i>M9-E1-1</i>

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:

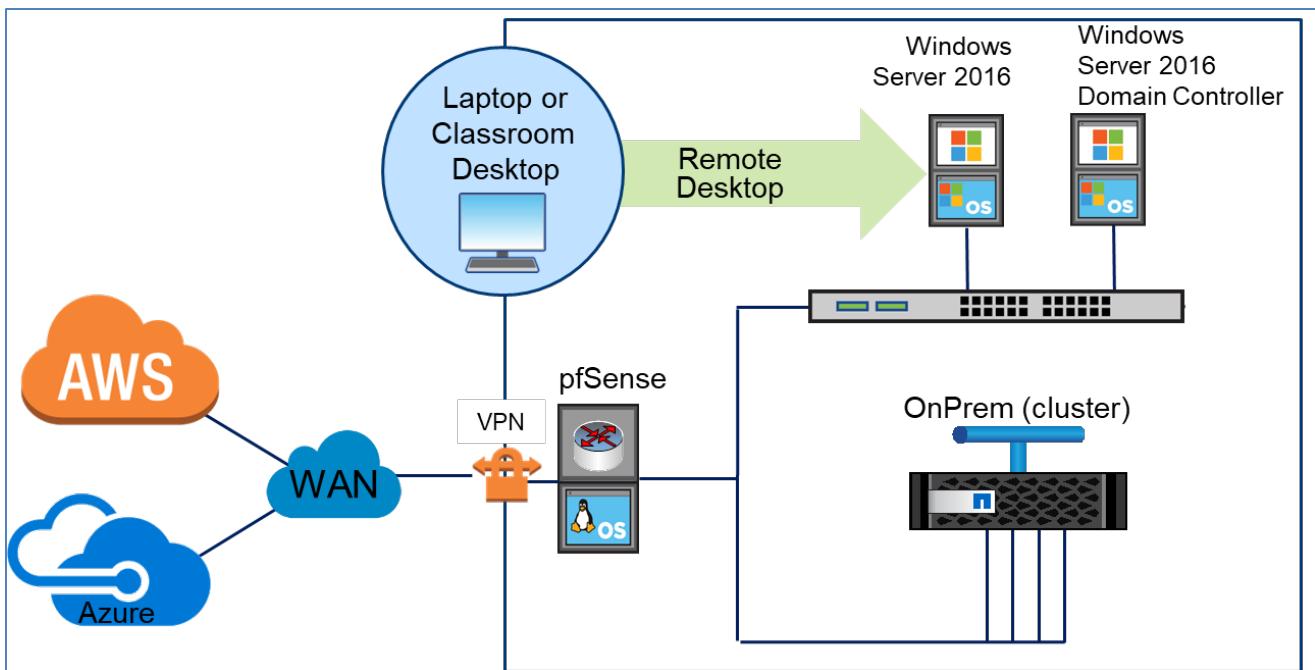
- Ensure connectivity to an ONTAP cluster
- Ensure that required licenses are installed on the ONTAP clusters
- Verify that you can log in to your assigned AWS and Azure accounts

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

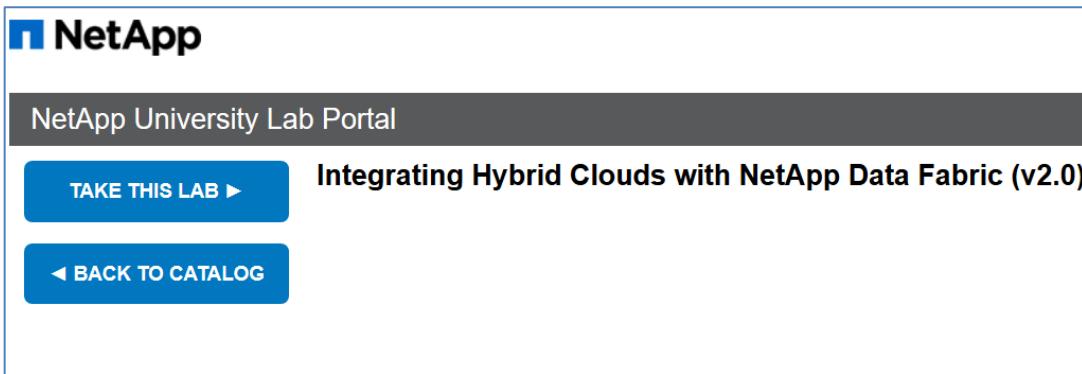
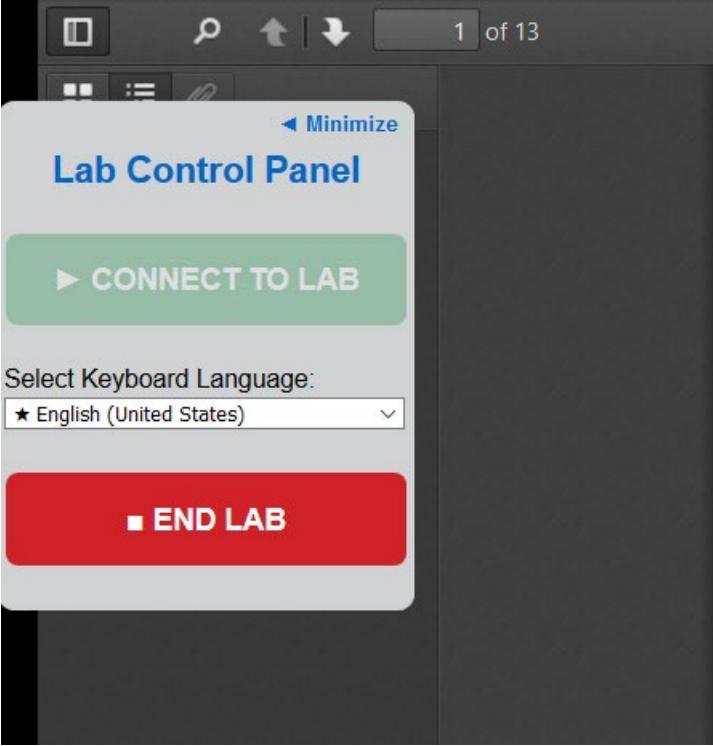
When you use the connection information that was assigned to you by your instructor, you are first connected by Remote Desktop Connection (Remote Desktop or RDC) to a Windows Server 2016. From this Windows desktop, you connect to the other servers in your exercise environment.

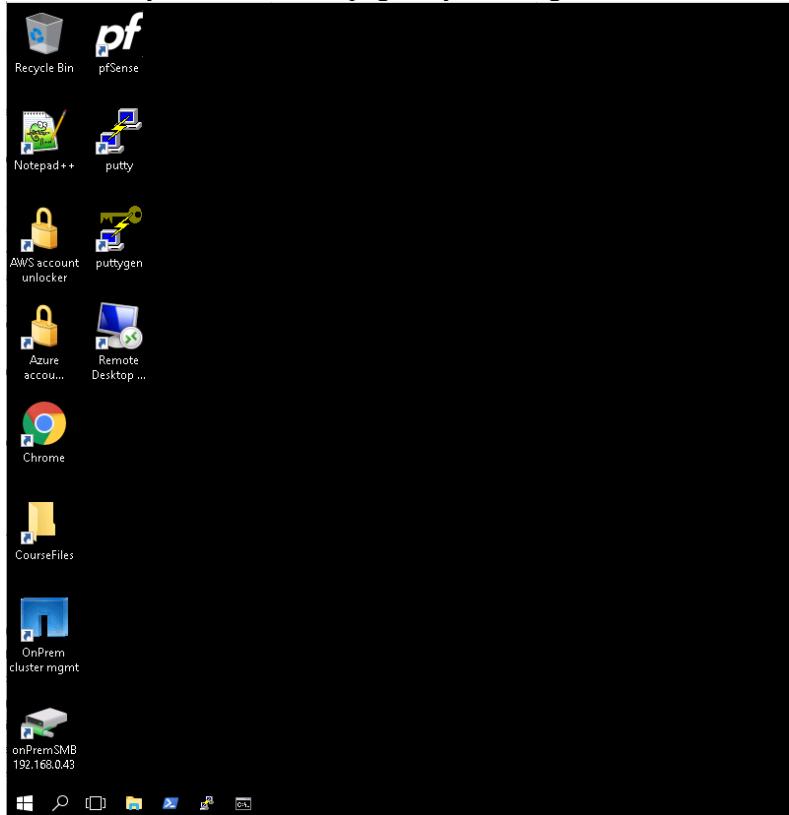


Task 0: Provision Your Lab Environment

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 : <ul style="list-style-type: none">• 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 .
	

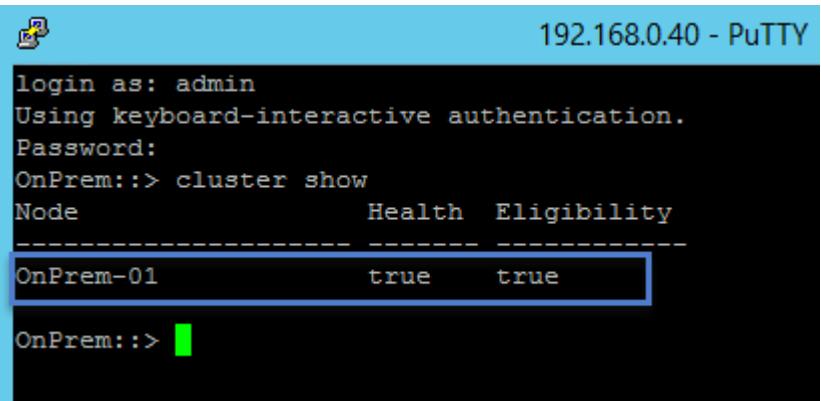
Step	Action
0-7	<p>Ensure that you see the Start page of your assigned Windows Server 2016.</p> 

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

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 .

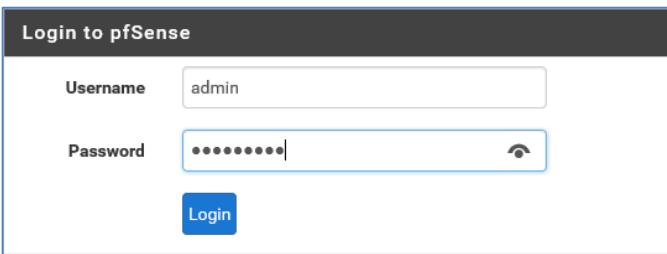
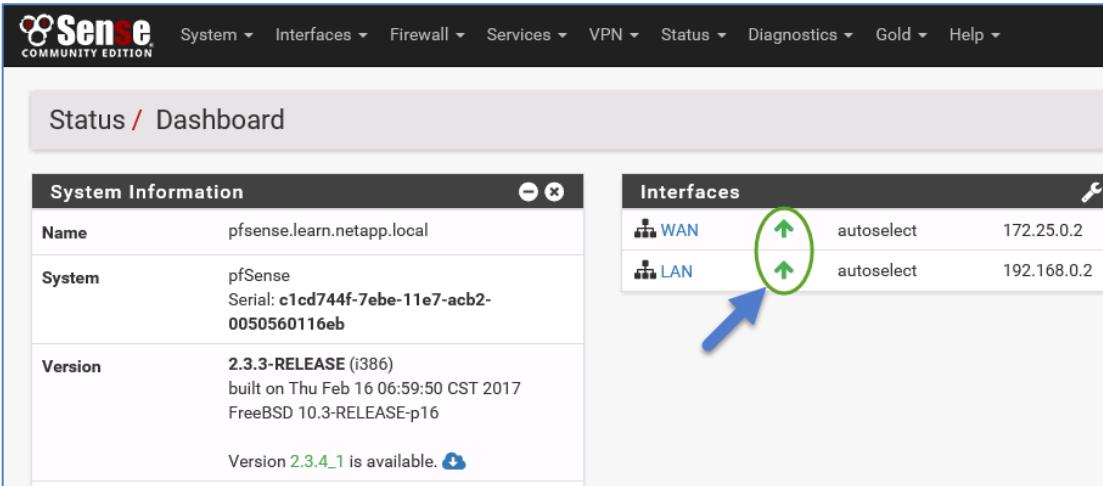
Step	Action										
1-5	<p>At the ONTAP cluster login prompt, provide the OnPrem cluster credentials:</p> <ul style="list-style-type: none"> ▪ Login as: admin ▪ Password: Netapp1! <p>The ONTAP cluster CLI prompt and cursor appear.</p> 										
1-6	 <p>If you have difficulty logging in to the ONTAP 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).</p> <table border="1"> <thead> <tr> <th>System</th> <th>Host Name</th> <th>IP Address</th> <th>User Name</th> <th>Password</th> </tr> </thead> <tbody> <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> </tbody> </table>	System	Host Name	IP Address	User Name	Password	ONTAP cluster-management LIF	OnPrem	192.168.0.40	admin (case-sensitive)	Netapp1!
System	Host Name	IP Address	User Name	Password							
ONTAP cluster-management LIF	OnPrem	192.168.0.40	admin (case-sensitive)	Netapp1!							
1-7	<p>Verify that the ONTAP cluster node is healthy and eligible:</p> <pre>cluster show</pre> 										
1-8	 <p>If the health of the node is listed as false, alert your instructor.</p> <pre>OnPrem::> cluster show</pre> <table border="1"> <thead> <tr> <th>Node</th> <th>Health</th> <th>Eligibility</th> </tr> </thead> <tbody> <tr> <td>OnPrem-01</td> <td>false</td> <td>false</td> </tr> </tbody> </table>	Node	Health	Eligibility	OnPrem-01	false	false				
Node	Health	Eligibility									
OnPrem-01	false	false									

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.

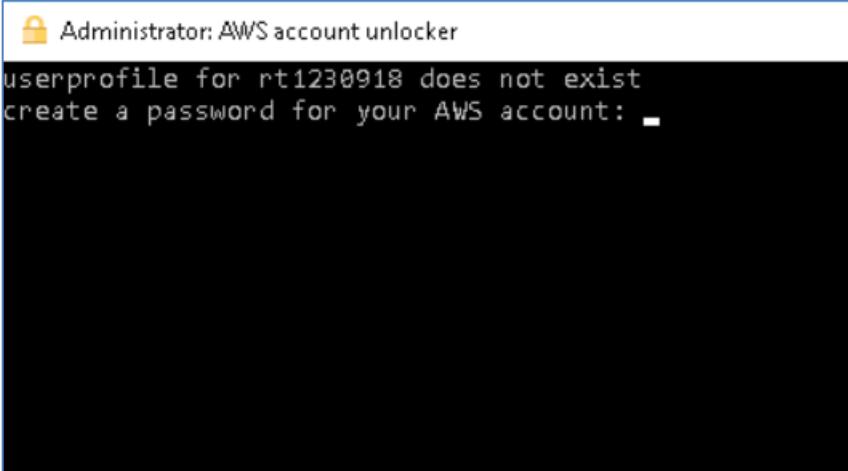
Step	Action
2-1	<p>In the OnPrem-mgmt CLI, enter the following command:</p> <pre>license show</pre> <div style="background-color: black; color: white; padding: 10px;"><pre>OnPrem:::> license show (system license show) Serial Number: 1-80-000054 Owner: OnPrem Package Type Description Expiration ----- license Cluster Base License - Base license Cluster Base License - Serial Number: 1-81-000000000000000000000000000071 Owner: OnPrem-01 Package Type Description Expiration ----- license 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 </pre></div>
2-2	<p>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:</p> <ul style="list-style-type: none">▪ 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.

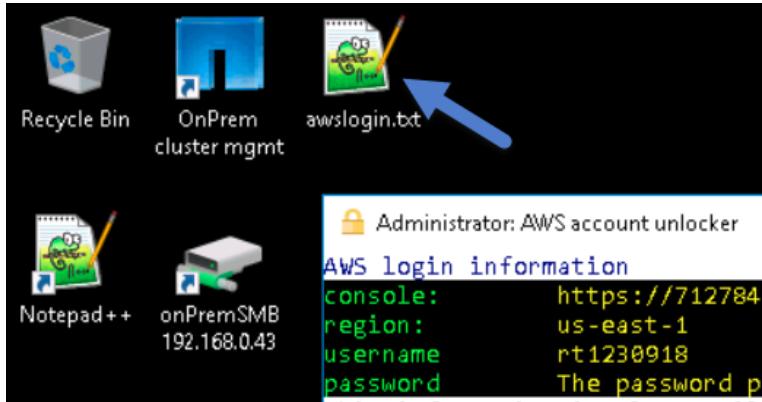
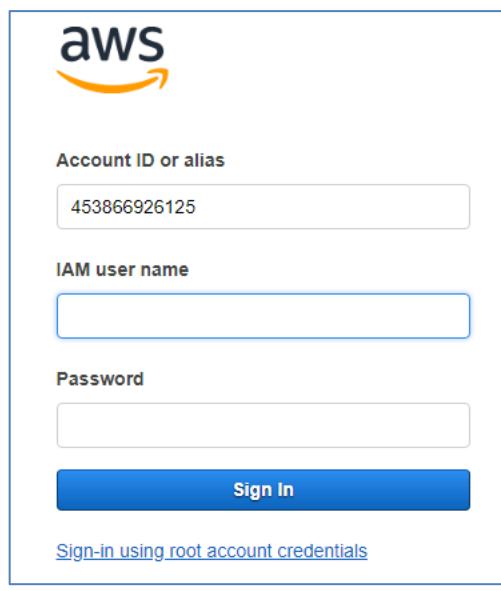
Task 3: Verify That pfSense Is Operational

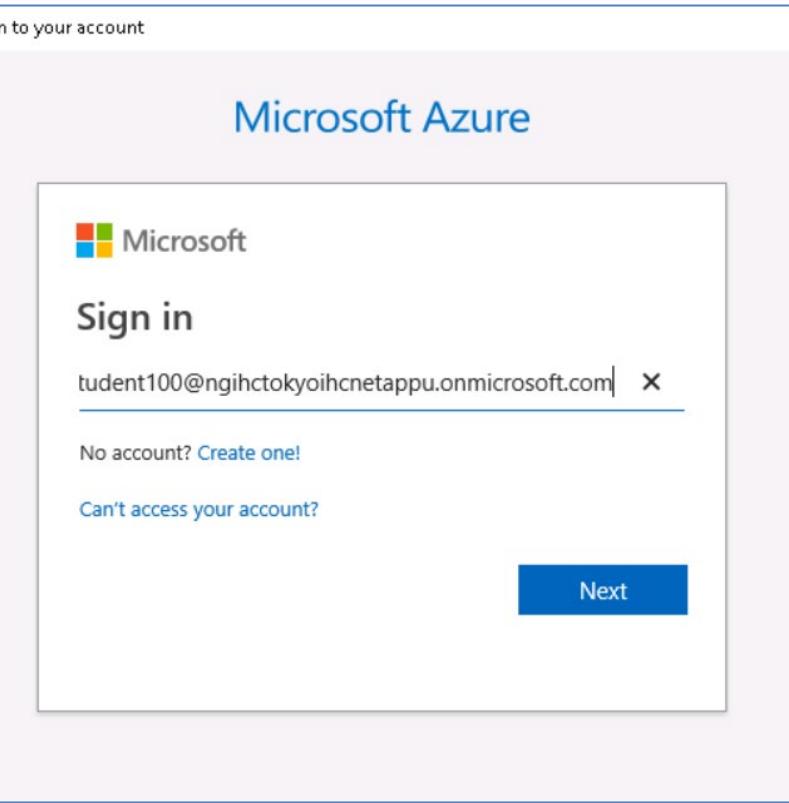
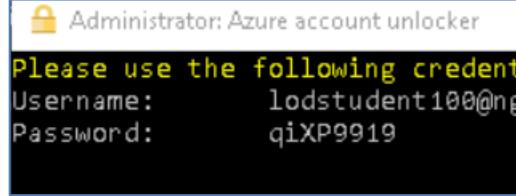
Step	Action																								
3-1																									
3-2	If a security warning appears, click Click Advanced and then click Proceed to 192.168.0.1(unsafe) .																								
3-3	<p>Enter the following credentials:</p> <p>Username: admin</p> <p>Password: Netapp1!</p> 																								
3-4	<p>Verify that the pfSense interface appears and that the WAN and LAN interfaces are up.</p>  <table border="1"> <thead> <tr> <th colspan="3">System Information</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td colspan="2">pfSense.learn.netapp.local</td> </tr> <tr> <td>System</td> <td colspan="2">pfSense Serial: c1cd744f-7ebe-11e7-acb2-0050560116eb</td> </tr> <tr> <td>Version</td> <td colspan="2">2.3.3-RELEASE (i386) built on Thu Feb 16 06:59:50 CST 2017 FreeBSD 10.3-RELEASE-p16</td> </tr> <tr> <td colspan="3">Version 2.3.4 is available. </td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="3">Interfaces</th> </tr> </thead> <tbody> <tr> <td> WAN</td> <td>autoselect</td> <td>172.25.0.2</td> </tr> <tr> <td> LAN</td> <td>autoselect</td> <td>192.168.0.2</td> </tr> </tbody> </table>	System Information			Name	pfSense.learn.netapp.local		System	pfSense Serial: c1cd744f-7ebe-11e7-acb2-0050560116eb		Version	2.3.3-RELEASE (i386) built on Thu Feb 16 06:59:50 CST 2017 FreeBSD 10.3-RELEASE-p16		Version 2.3.4 is available. 			Interfaces			 WAN	autoselect	172.25.0.2	 LAN	autoselect	192.168.0.2
System Information																									
Name	pfSense.learn.netapp.local																								
System	pfSense Serial: c1cd744f-7ebe-11e7-acb2-0050560116eb																								
Version	2.3.3-RELEASE (i386) built on Thu Feb 16 06:59:50 CST 2017 FreeBSD 10.3-RELEASE-p16																								
Version 2.3.4 is available. 																									
Interfaces																									
 WAN	autoselect	172.25.0.2																							
 LAN	autoselect	192.168.0.2																							

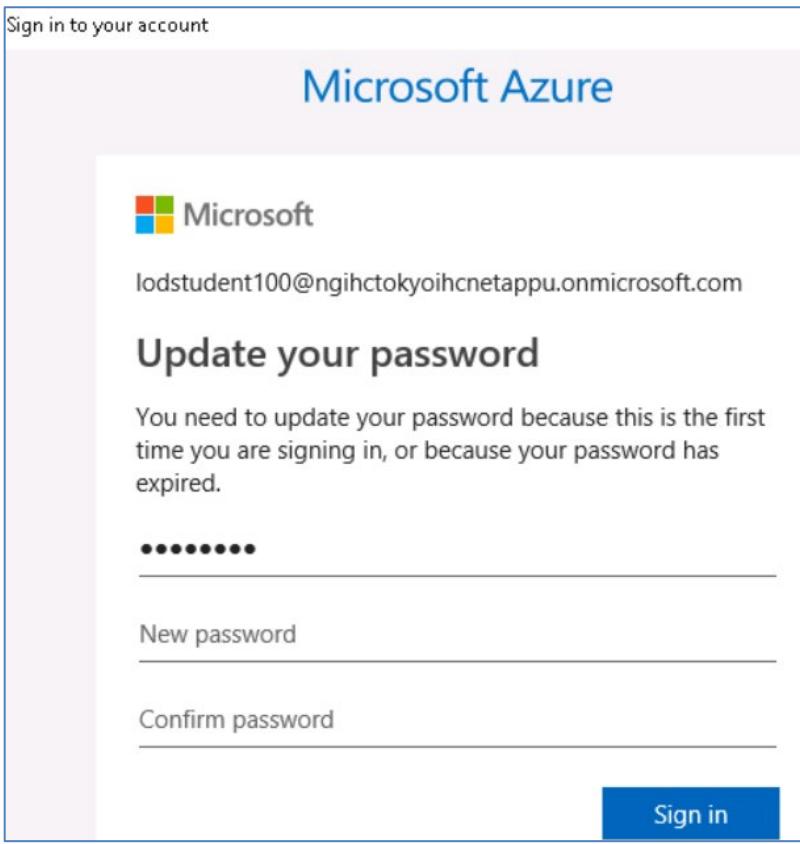
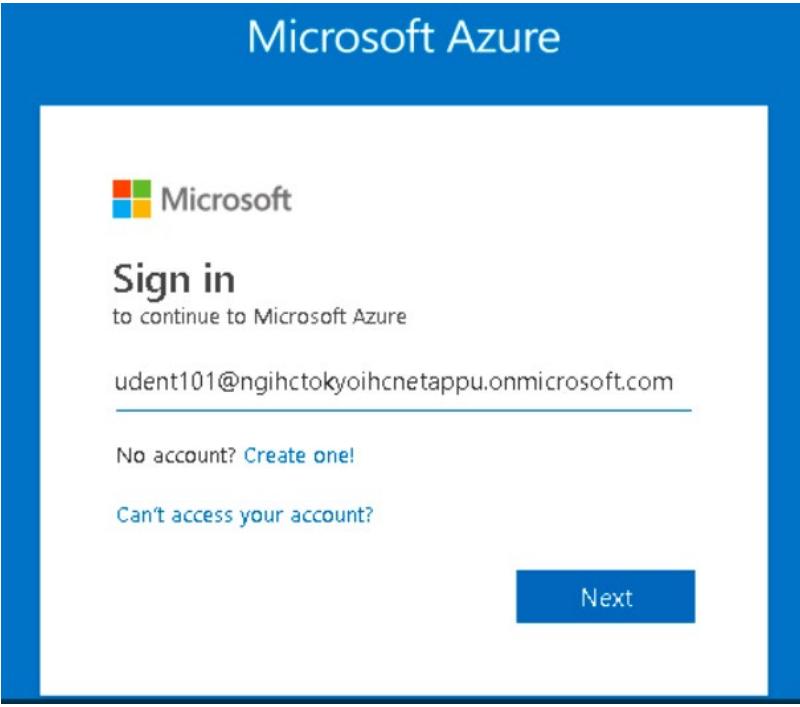
Task 4: Validate the AWS and Azure Accounts

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

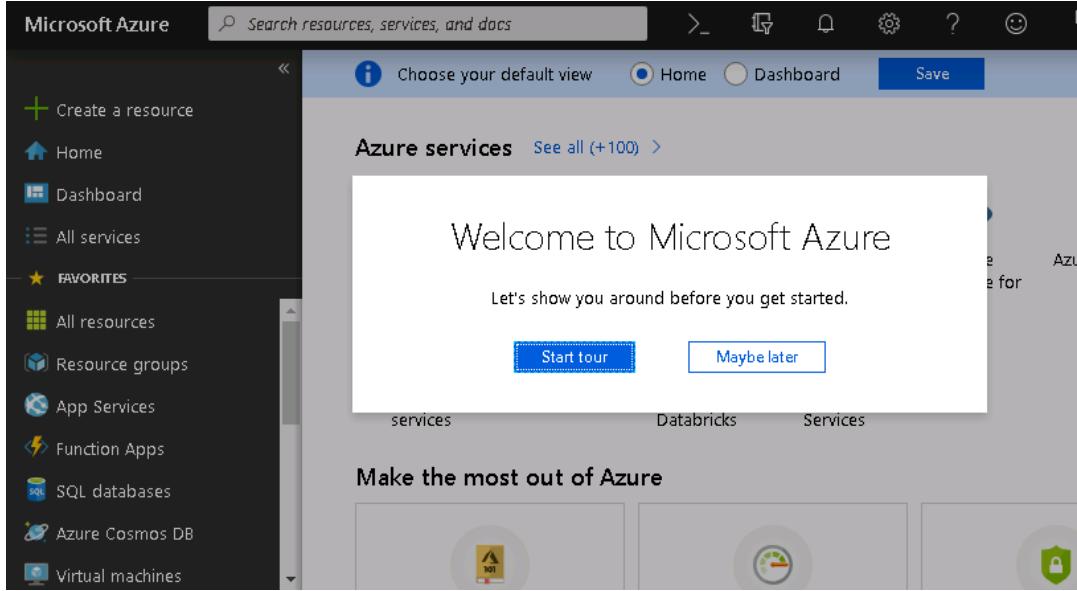
Step	Action
4-1	On your Windows Server jump host, double-click the AWS account unlocker shortcut. 
4-2	In the Administrator AWS account unlocker window, create a password for your AWS account, (for example, Netapp1!). 
4-3	Re-enter your password and press Enter . 

Step	Action
4-4	<p>Verify that an awslogin.txt file is created on the desktop.</p> <p>Note this text file contains your username and the AWS console login link if you need it later.</p>  <pre> lock icon: Administrator: AWS account unlocker AWS login information console: https://712784 region: us-east-1 username: rt1230918 password: The password p </pre>
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	<p>Update the password to a password of your choice, and click Sign in.</p> 
4-15	When you are returned to the Azure account unlocker, press Enter to get to the Azure portal.
4-16	<p>Enter your username and click Next.</p> 

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: <pre>PS C:\Users\Administrator> \$PSVersionTable</pre> <p>Sample output:</p> <table><thead><tr><th>PSV Name</th><th>Value</th></tr></thead><tbody><tr><td>PSVersion</td><td>5.1.14393.206</td></tr><tr><td>PSEdition</td><td>Desktop</td></tr><tr><td>PSCompatibleVersions</td><td>{1.0, 2.0, 3.0, 4.0...}</td></tr><tr><td>BuildVersion</td><td>10.0.14393.206</td></tr><tr><td>CLRVersion</td><td>4.0.30319.42000</td></tr><tr><td>WSManStackVersion</td><td>3.0</td></tr><tr><td>PSRemotingProtocolVersion</td><td>2.3</td></tr><tr><td>SerializationVersion</td><td>1.1.0.1</td></tr></tbody></table> <p>Note: AWS requires at least version 2.0 of PowerShell.</p>	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
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																		

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: <ol style="list-style-type: none"> Open a browser, and then enter the following URL: http://aws.amazon.com/powershell Click AWS Tools for Windows. Run the downloaded MSI installer. Follow the installation instructions that appear. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <h2>AWS Tools for Windows PowerShell</h2> <p>The AWS Tools for Windows PowerShell lets developers and administrators manage their AWS services from the Windows PowerShell scripting environment. Now you can manage your AWS resources with the same Windows PowerShell tools you use to manage your Windows environment.</p> <div style="float: right;"> Downloads AWS Tools for Windows » </div> </div>
1-5	Return to the PowerShell window, and then check the PowerShell execution policy: <pre>PS> Get-ExecutionPolicy</pre> Sample output: Restricted
1-6	If the execution policy is not set to RemoteSigned, enter the following command: <pre>PS> Set-ExecutionPolicy RemoteSigned</pre>
1-7	 If the execution policy is not set correctly, PowerShell generates the following message: <pre>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.</pre>
1-8	If you changed the execution policy, close the current PowerShell window, and then open a new PowerShell window.

Step	Action								
1-9	<p>Verify that the module is loaded:</p> <pre>PS> Get-Module -ListAvailable</pre> <p>Sample output:</p> <pre>...</pre> <table> <thead> <tr> <th>ModuleType</th> <th>Version</th> <th>Name</th> <th>ExportedCommands</th> </tr> </thead> <tbody> <tr> <td>Binary</td> <td>3.3.84.0</td> <td>AWSPowerShell</td> <td>{Clear-AWSHistory, Set-AWSHistoryConfiguration, Initialize...}</td> </tr> </tbody> </table> <p>...</p> <p>Note: The AWS Tools for Windows PowerShell installer automatically updates the PSMODULEPATH to include the location of the directory.</p>	ModuleType	Version	Name	ExportedCommands	Binary	3.3.84.0	AWSPowerShell	{Clear-AWSHistory, Set-AWSHistoryConfiguration, Initialize...}
ModuleType	Version	Name	ExportedCommands						
Binary	3.3.84.0	AWSPowerShell	{Clear-AWSHistory, Set-AWSHistoryConfiguration, Initialize...}						

Step	Action																																													
1-10	<p>Determine which version of AWS Tools for Windows PowerShell is installed and which services are available:</p> <pre>PS> Get-AWSPowerShellVersion -ListServices</pre> <p>Sample output:</p> <pre>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.</pre> <p>Release notes: https://aws.amazon.com/releasenotes/PowerShell</p> <p>This software includes third party software subject to the following copyrights:</p> <ul style="list-style-type: none"> - Logging from log4net, Apache License [http://logging.apache.org/log4net/license.html] <table> <thead> <tr> <th>Service</th> <th>Noun Prefix</th> <th>API Version</th> </tr> </thead> <tbody> <tr> <td>AWS AppStream</td> <td>APS</td> <td>2016-12-01</td> </tr> <tr> <td>AWS Batch</td> <td>BAT</td> <td>2016-08-10</td> </tr> <tr> <td>AWS Budgets</td> <td>BGT</td> <td>2016-10-20</td> </tr> <tr> <td>AWS Certificate Manager</td> <td>ACM</td> <td>2015-12-08</td> </tr> <tr> <td>AWS Cloud Directory</td> <td>CDIR</td> <td>2016-05-10</td> </tr> <tr> <td>AWS Cloud HSM</td> <td>HSM</td> <td>2014-05-30</td> </tr> <tr> <td>AWS CloudFormation</td> <td>CFN</td> <td>2010-05-15</td> </tr> <tr> <td>AWS CloudTrail</td> <td>CT</td> <td>2013-11-01</td> </tr> <tr> <td>AWS CodeBuild</td> <td>CB</td> <td>2016-10-06</td> </tr> <tr> <td>AWS CodeCommit</td> <td>CC</td> <td>2015-04-13</td> </tr> <tr> <td>AWS CodeDeploy</td> <td>CD</td> <td>2014-10-06</td> </tr> <tr> <td>AWS CodePipeline</td> <td>CP</td> <td>2015-07-09</td> </tr> <tr> <td>AWS CodeStar</td> <td>CST</td> <td>2017-04-19</td> </tr> <tr> <td>...</td> <td></td> <td></td> </tr> </tbody> </table>	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	...		
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	 <p>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.</p>																																													
1-12	<p>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):</p> <pre>PS> Set-AWSCredentials -AccessKey <the access key in the awslogin.txt file> -SecretKey <the secret key in the awslogin.txt file> -StoreAs default</pre>																																													

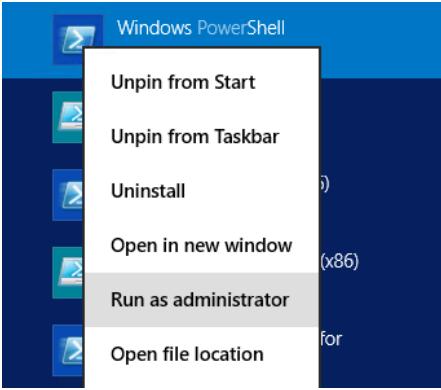
Step	Action
1-13	 If you ever need to generate new AWS Access Keys, you perform these steps: (For information only) <ul style="list-style-type: none"> a. In the AWS console, select Services > IAM > Users. b. Click the user for which you want to generate the keys. c. Click the Security credentials tab. d. Click Create access key. d. Click Download .csv file.
1-14	Set the default region: <pre>PS> Set-DefaultAWSRegion -Region us-east-1</pre>
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: <pre>PS> Get-EC2AvailabilityZone</pre> Sample output: <pre>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</pre>
1-17	Run the following command to list the IAM Users in your AWS account: <pre>PS> Get-IAMUsers</pre> Sample output: <pre>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</pre>

Step	Action
1-18	<p>Run the following command to list of EC2 images that you can use:</p> <pre>PS> Get-EC2ImageByName</pre> <p>Sample output:</p> <pre>WINDOWS_2016_BASE WINDOWS_2016_NANO WINDOWS_2016_CORE WINDOWS_2016_CONTAINER WINDOWS_2016_SQL_SERVER_ENTERPRISE_2016 WINDOWS_2016_SQL_SERVER_STANDARD_2016 WINDOWS_2016_SQL_SERVER_WEB_2016 WINDOWS_2016_SQL_SERVER_EXPRESS_2016 WINDOWS_2012R2_BASE WINDOWS_2012R2_CORE WINDOWS_2012R2_SQL_SERVER_EXPRESS_2016 WINDOWS_2012R2_SQL_SERVER_STANDARD_2016 WINDOWS_2012R2_SQL_SERVER_WEB_2016 WINDOWS_2012R2_SQL_SERVER_EXPRESS_2014 WINDOWS_2012R2_SQL_SERVER_STANDARD_2014 WINDOWS_2012R2_SQL_SERVER_WEB_2014 WINDOWS_2012_BASE WINDOWS_2012_SQL_SERVER_EXPRESS_2014 WINDOWS_2012_SQL_SERVER_STANDARD_2014 WINDOWS_2012_SQL_SERVER_WEB_2014 WINDOWS_2012_SQL_SERVER_EXPRESS_2012 WINDOWS_2012_SQL_SERVER_STANDARD_2012 WINDOWS_2012_SQL_SERVER_WEB_2012 WINDOWS_2012_SQL_SERVER_EXPRESS_2008 WINDOWS_2012_SQL_SERVER_STANDARD_2008 WINDOWS_2012_SQL_SERVER_WEB_2008 WINDOWS_2008R2_BASE WINDOWS_2008R2_SQL_SERVER_EXPRESS_2012 WINDOWS_2008R2_SQL_SERVER_STANDARD_2012 WINDOWS_2008R2_SQL_SERVER_WEB_2012 WINDOWS_2008R2_SQL_SERVER_EXPRESS_2008 WINDOWS_2008R2_SQL_SERVER_STANDARD_2008 WINDOWS_2008R2_SQL_SERVER_WEB_2008 WINDOWS_2008RTM_BASE WINDOWS_2008RTM_SQL_SERVER_EXPRESS_2008 WINDOWS_2008RTM_SQL_SERVER_STANDARD_2008 WINDOWS_2008_BEANTALK_IIS75 WINDOWS_2012_BEANTALK_IIS8 VPC_NAT</pre>

Step	Action
1-19	<p>Run the following command to list of EC2 images that you can use:</p> <pre>PS> Get-EC2ImageByName -Name WINDOWS_2016_BASE</pre> <p>Sample output:</p> <pre>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</pre>

Task 2: Install Azure PowerShell

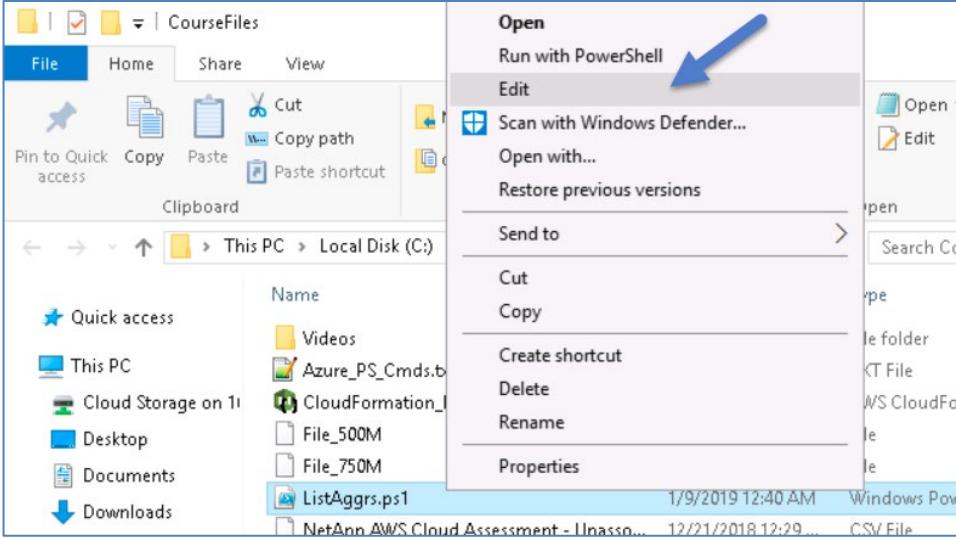
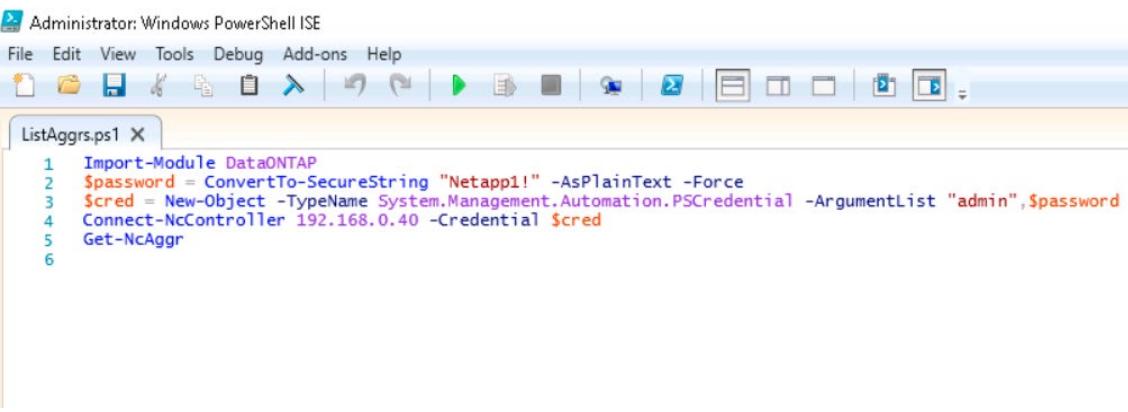
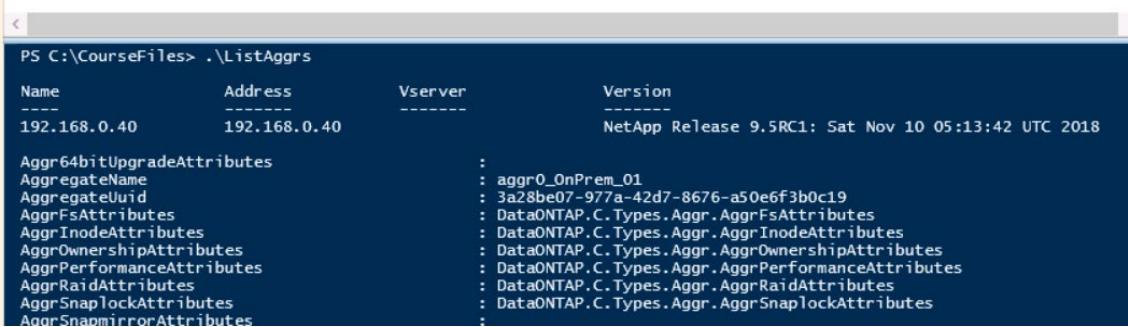
Step	Action
2-1	 <p>The Azure PowerShell tools are installed on your jump host. In a production environment, you install the tools by completing the following actions:</p> <ol style="list-style-type: none"> Open a browser, and then enter the following URL: https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-1.0.0 Click Install Azure PowerShell with PowerShellGet. In PowerShell, enter <code>Install-Module -Name AzureRM</code> Follow the installation instructions that appear.

Step	Action
2-2	<p>Open your PowerShell window:</p> <ol style="list-style-type: none"> Select the Windows PowerShell application. Select Run as administrator. 
2-3	<p>Enter the following command:</p> <pre>PS C:\Users\Administrator.DEMO> Get-Module -ListAvailable</pre> <p>Sample concatenated output</p> <pre>Directory: C:\Program Files (x86)\Microsoft SDKs\Azure\PowerShell\ResourceManager\AzureResourceManager ModuleType Version Name ExportedCommands ----- ----- ---- ----- Manifest 1.1.1 AzureRM.ApiManagement {Add-AzureRmApiManagementRegion, Get-AzureRmApiMan... Manifest 1.0.9 AzureRM.Automation {Get-AzureRmAutomationJobOutputRecord, Import-Azur... Binary 0.9.6 AzureRM.AzureStackAdmin {Get-AzureRMManagedLocation, New-AzureRMManagedLoc... Manifest 0.9.7 AzureRM.AzureStackStorage {Add-ACSFarm, Get-ACSEvent, Get-ACSEventQuery, Get... Manifest 1.0.9 AzureRM.Backup {Backup-AzureRmBackupItem, Enable-AzureRmBackupCor... Manifest 1.1.1 AzureRM.Batch {Remove-AzureRmBatchAccount, Get-AzureRmBatchAccou... Manifest 1.0.3 AzureRM.Cdn {Get-AzureRmCdnCustomDomain, New-AzureRmCdnCustomD... Manifest 1.3.1 AzureRM.Compute {Remove-AzureRmAvailabilitySet, Get-AzureRmAvailab... Manifest 1.0.9 AzureRM.DataFactories {Get-AzureRmDataFactory, Get-AzureRmDataFactory... Manifest 1.1.1 AzureRM.DataLakeAnalytics {Get-AzureRmDataLakeAnalyticsDataSource, Remove-Az... Manifest 1.0.9 AzureRM.DataLakeStore {Add-AzureRmDataLakeStoreItemContent, Export-Azure...</pre>
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	<p>Enter the following command:</p> <pre>PS> Login-AzureRmAccount</pre>
2-6	<p>In the Sign in to your account window, enter the following information:</p> <ul style="list-style-type: none"> Email or phone: <<i>Found in azurelogin.txt file on your desktop</i>> Password: <<i>Password that you set up for your Azure account</i>> <p>Note: If a dialog box asks whether the account is a Work or Personal account, select Personal.</p>

Step	Action
2-7	<p>In the PowerShell window, confirm your account information.</p> <pre>PS C:\Users\Administrator.DEMO> Login-AzureRmAccount</pre> <pre>Account : l0dstudent111@ngihctokyoiohcnetappu.onmicrosoft.com SubscriptionName : Pay-As-You-Go SubscriptionId : fe092[REDACTED]cc13edf9c959 TenantId : 2eb8e[REDACTED]7c0f3063 Environment : AzureCloud</pre>
2-8	<p>View all subscriptions for your account:</p> <pre>PS> Get-AzureRmSubscription</pre> <p>Sample output:</p> <pre>Name : Pay-As-You-Go Id : fe09285f-[REDACTED]-cc13edf9c959 TenantId : 2eb8eb0a-[REDACTED]-0c467c0f3063 State : Enabled</pre>
2-9	<p>View the VM sizes available in us-east.</p> <pre>PS> Get-AzureRmVmSize -Location "East US"</pre> <p>Sample concatenated output:</p> <pre>Name NumberOfCores MemoryInMB MaxDataDiskCount OSDiskSizeInMB ResourceDiskSizeInMB ---- ----- Standard_B1ms 1 2048 2 1047552 4096 Standard_B1s 1 1024 2 1047552 2048 Standard_B2ms 2 8192 4 1047552 16384 Standard_B2s 2 4096 4 1047552 8192 Standard_B4ms 4 16384 8 1047552 32768 Standard_B8ms 8 32768 16 1047552 65536 Standard_DS1_v2 1 3584 4 1047552 7168 Standard_DS2_v2 2 7168 8 1047552 14336 Standard_DS3_v2 4 14336 16 1047552 28672 Standard_DS4_v2 8 28672 32 1047552 57344 Standard_DS5_v2 16 57344 64 1047552 114688 Standard_DS11-1_v2 2 14336 8 1047552 28672 Standard_DS11_v2 2 14336 8 1047552 28672 Standard_DS12-1_v2 4 28672 16 1047552 57344 Standard_DS12-2_v2 4 28672 16 1047552 57344 Standard_DS12_v2 4 28672 16 1047552 57344 Standard_DS13-2_v2 8 57344 32 1047552 114688 Standard_DS13-4_v2 8 57344 32 1047552 114688 Standard_DS13_v2 8 57344 32 1047552 114688 Standard_DS14-4_v2 16 114688 64 1047552 229376 Standard_DS14-8_v2 16 114688 64 1047552 229376</pre>

Task 3: Install the NetApp PowerShell Toolkit

Step	Action
3-1	 <p>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:</p> <ol style="list-style-type: none"> Open a browser, and then enter the following URL: http://mysupport.netapp.com/tools/info/ECMLP2310788I.html?productID=61926/ Select I have read and agree to the License Terms & Conditions. Click Continue. Click NetApp_PowerShell_Toolkit_4.7.0.msi. Run the downloaded installer. Follow the installation instructions that appear.
3-2	<p>Import the ONTAP module:</p> <pre>PS C:\Users\Administrator> Import-Module DataONTAP</pre>
3-3	<p>Review the basic commands for ONTAP software:</p> <pre>PS> Show-NcHelp</pre>
3-4	<p>Confirm the details of a connect command:</p> <pre>PS> Get-Help Connect-NcController</pre> <p>Sample output:</p> <pre>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 <PSCredential>] [-Transient] [-Vserver <String>] [-Timeout <Int32>] [-Add] [-ApplicationName <String>] [-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 CurrentNcController. Most clustered ONTAP cmdlets in the Data ONTAP PowerShell Toolkit utilize this global variable if no connection object is provided. The clustered Data ONTAP Toolkit is capable of connecting to multiple controllers; use the -Add parameter to use that feature. Connections are established using HTTPS by default with automatic fallback to HTTP. Use the -Protocol 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"</pre>

Step	Action
3-5	<p>Using Windows Explorer, go to the CourseFiles folder, right-click the file ListAggrs.ps1 and then select Edit.</p> 
3-6	<p>Review the commands:</p>  <pre> 1 Import-Module DataONTAP 2 \$password = ConvertTo-SecureString "Netapp1!" -AsPlainText -Force 3 \$cred = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList "admin",\$password 4 Connect-NcController 192.168.0.40 -Credential \$cred 5 Get-NcAggr 6 </pre>
3-7	<p>At the bottom of the screen run the script: <code>PS C:\CourseFiles> .\ListAggrs.ps1</code></p> <p>Sample concatenated output:</p>  <pre> PS C:\CourseFiles> .\ListAggrs Name Address Vserver Version ---- ----- ----- ----- 192.168.0.40 192.168.0.40 Aggr64bitUpgradeAttributes : AggregateName : aggr0_OnPrem_01 AggregateUuid : 3a28be07-977a-42d7-8676-a50e6f3b0c19 AggrFsAttributes : DataONTAP.C.Types.Aggr.AggrFsAttributes AggrInodeAttributes: DataONTAP.C.Types.Aggr.AggrInodeAttributes AggrOwnershipAttributes: DataONTAP.C.Types.Aggr.AggrOwnershipAttributes AggrPerformanceAttributes: DataONTAP.C.Types.Aggr.AggrPerformanceAttributes AggrRaidAttributes : DataONTAP.C.Types.Aggr.AggrRaidAttributes AggrSnaplockAttributes : DataONTAP.C.Types.Aggr.AggrSnaplockAttributes AggrSnapmirrorAttributes : </pre>

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:

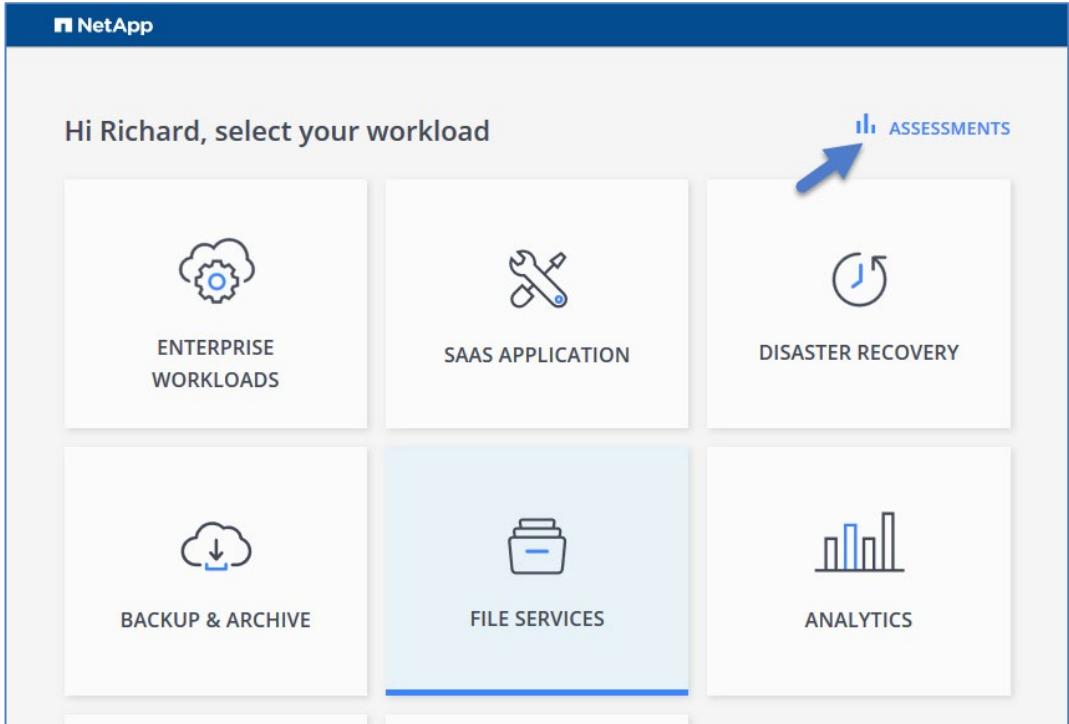
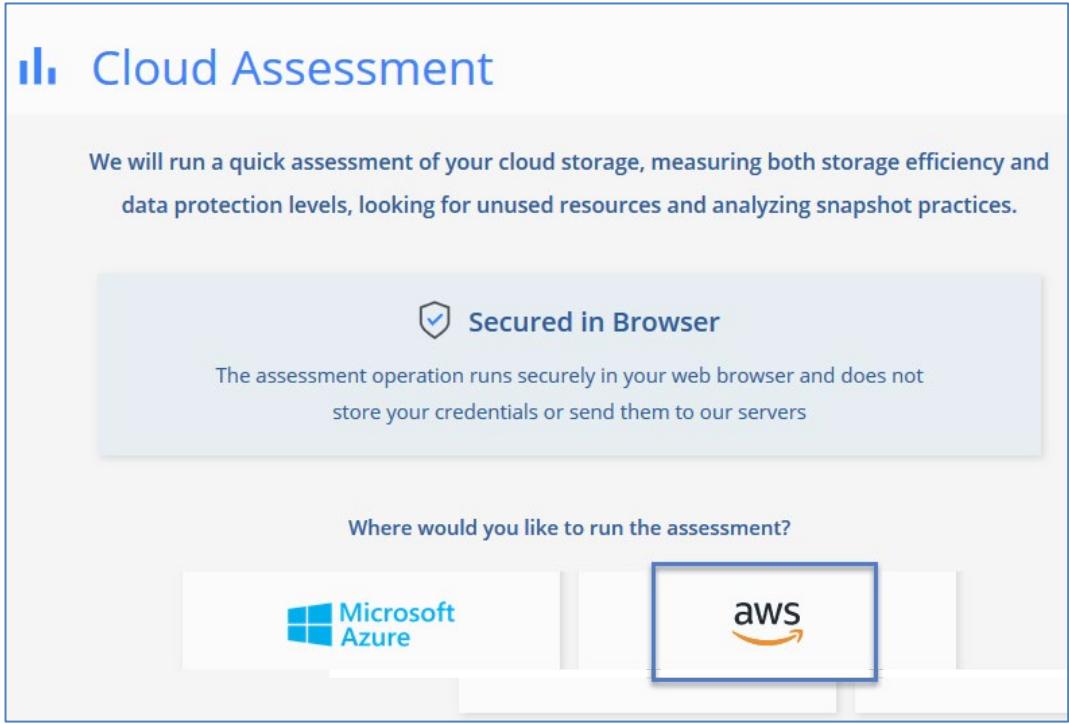
- Find unattached Amazon Elastic Block Store (Amazon EBS) volumes (AWS) and unattached disks (Azure)
- Find unassociated snapshots

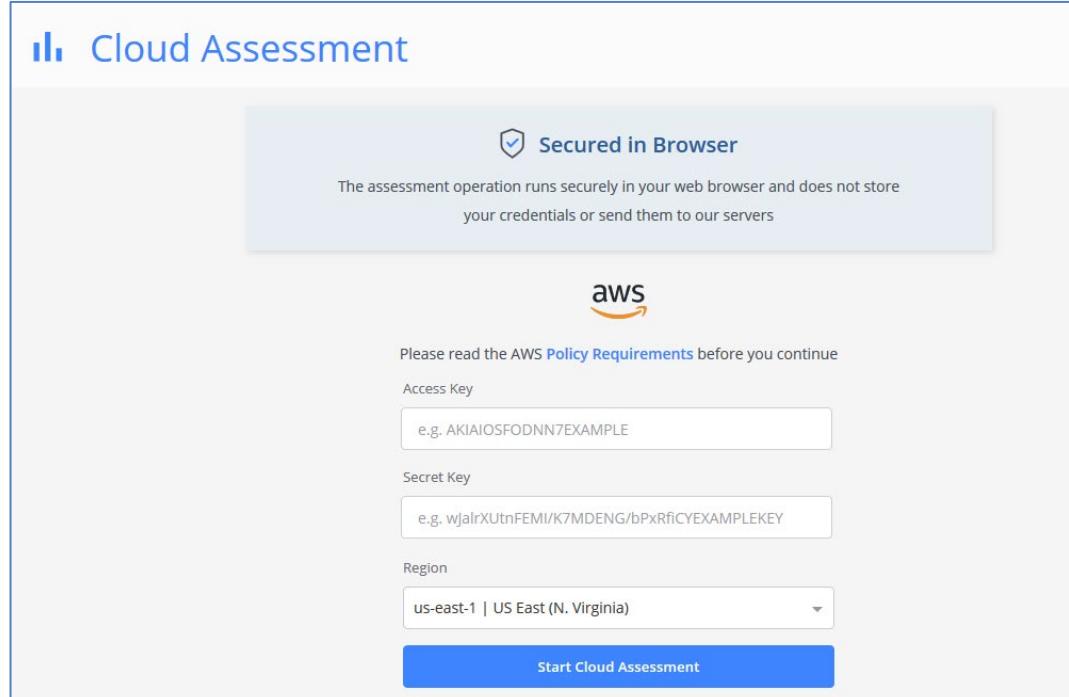
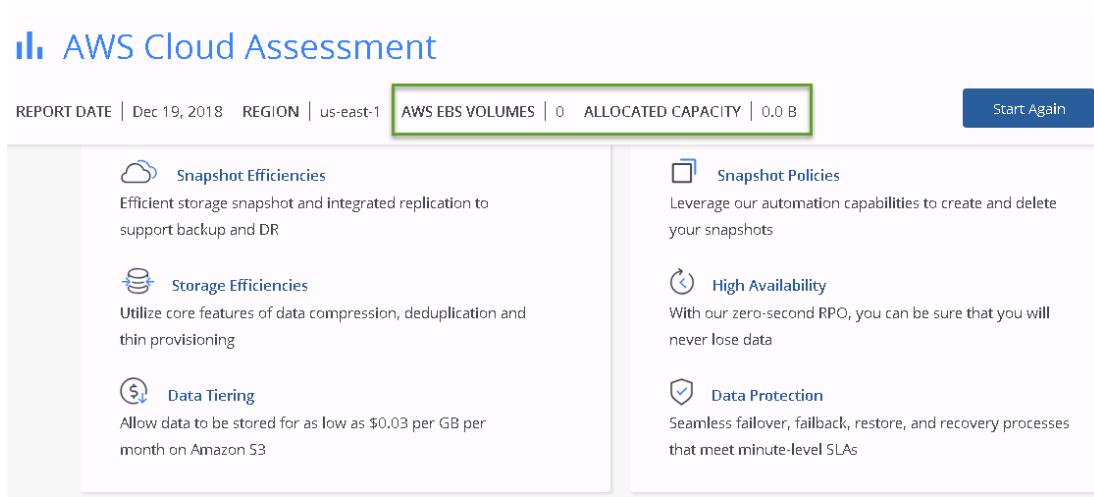
Task 1: Perform Cloud Assessments by Using Cloud Central

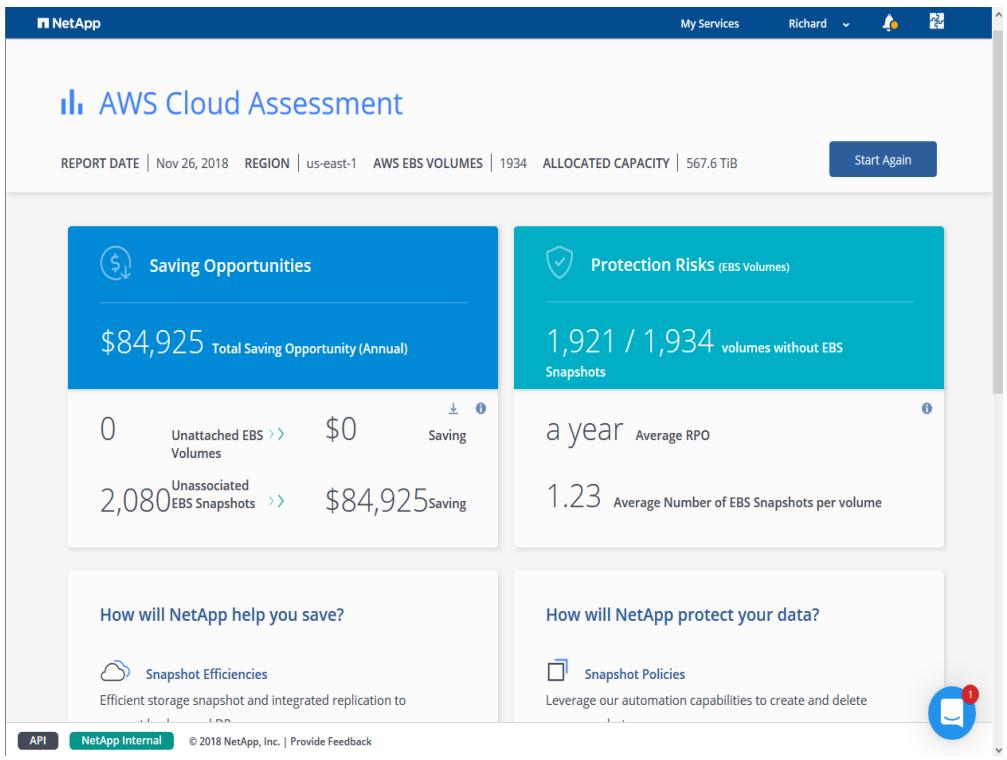
In this task, you run cloud assessments on your AWS and Azure accounts.

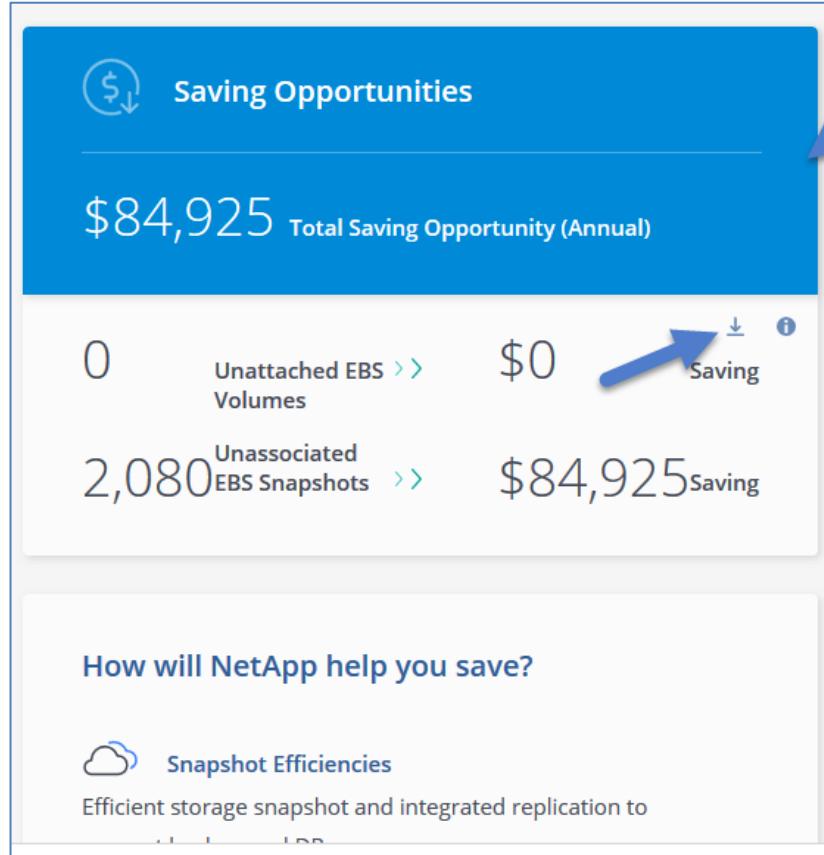
Step	Action
1-1	Navigate to cloud.netapp.com .
1-2	Click SIGN UP .

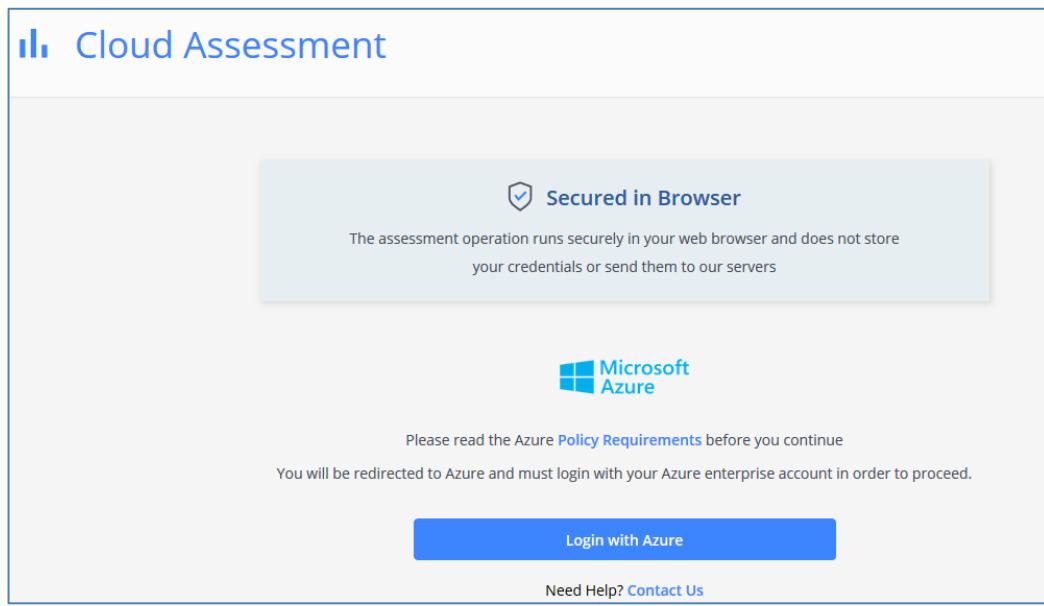
Step	Action
1-3	<p>On the SIGN UP tab, enter the following information:</p> <ul style="list-style-type: none"> • Email: <your user name in the awslogin.txt file>@demo.netapp.com • Password: Netapp1! • Company: NetApp • Full Name: <your user name in the awslogin.txt file> • Select I accept the terms and conditions check box.
1-4	Click SIGN UP .

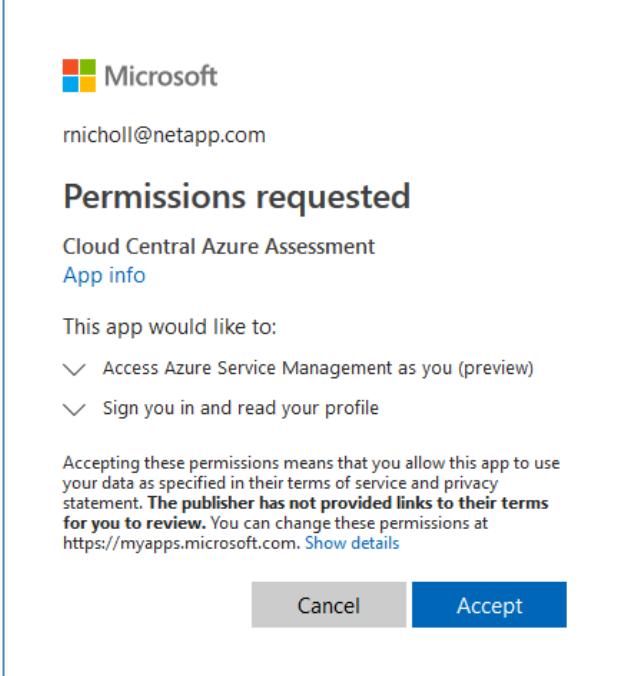
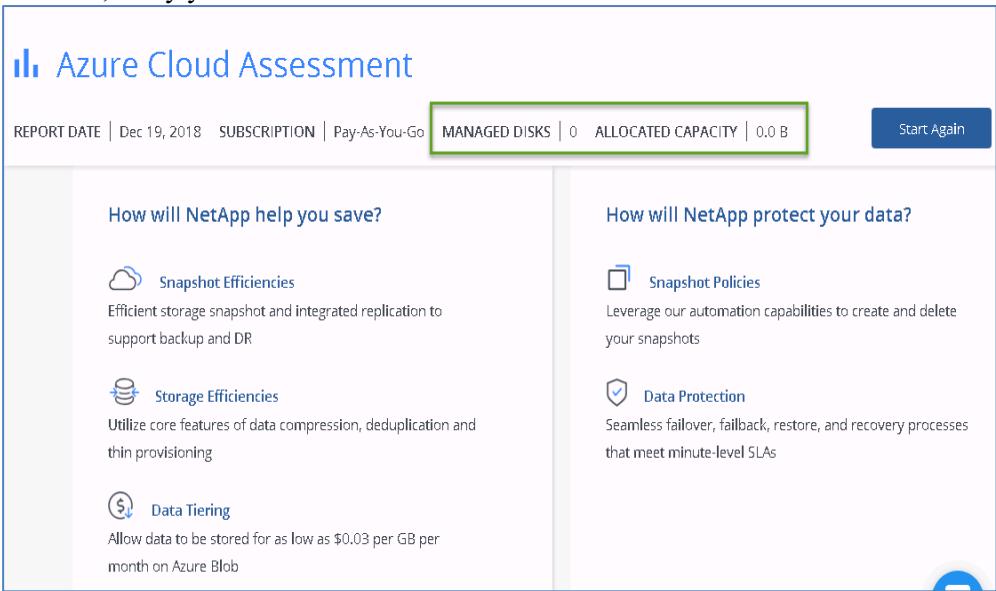
Step	Action
1-5	<p>On the top of the window, click ASSESSMENTS.</p> 
1-6	<p>Click the AWS icon.</p> 

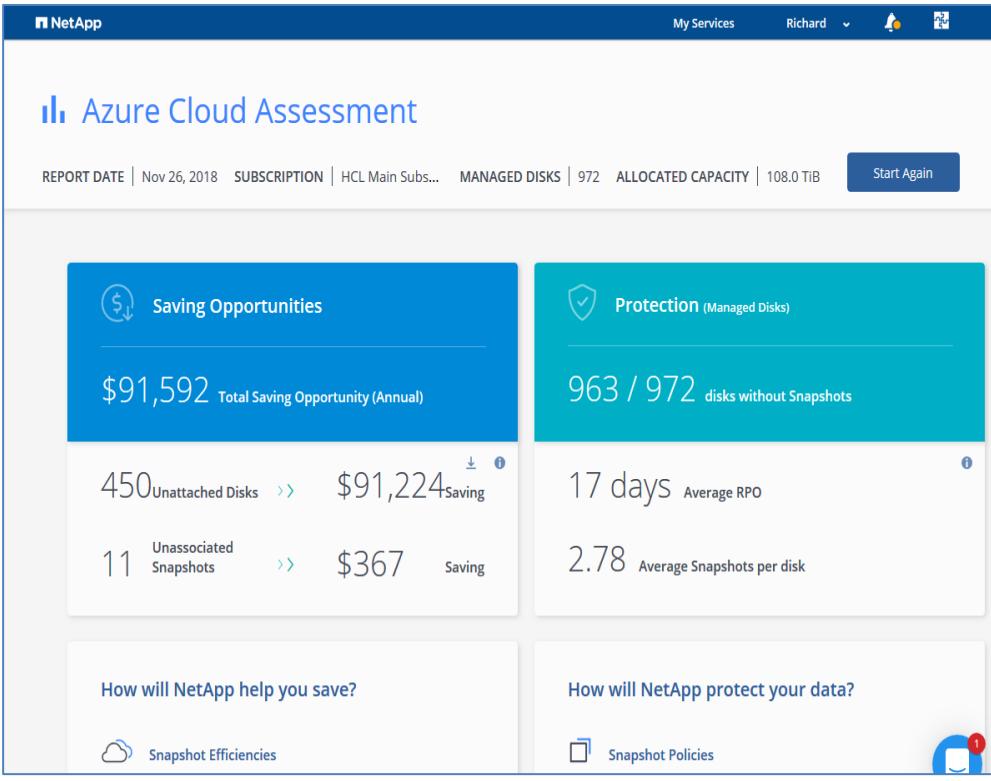
Step	Action
1-7	Enter the Access Key and Secret Key from the awslogin.txt file on your jump host desktop.
	 <p>The screenshot shows the AWS Cloud Assessment interface. It includes a 'Secured in Browser' notice, the AWS logo, and fields for Access Key (e.g. AKIAIOSFODNN7EXAMPLE), Secret Key (e.g. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY), and Region (us-east-1 US East (N. Virginia)). A large blue 'Start Cloud Assessment' button is at the bottom.</p>
1-8	Click Start Cloud Assessment .
1-9	 <p>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.</p>  <p>The screenshot shows the AWS Cloud Assessment report. It displays sections for Snapshot Efficiencies, Storage Efficiencies, and Data Tiering on the left, and Snapshot Policies, High Availability, and Data Protection on the right. Each section has a title, a brief description, and a green-bordered status bar indicating they are empty.</p>

Step	Action
1-10	 <p>Following is what the report would look like with an AWS account with many active resources.</p>  <p>The screenshot shows the AWS Cloud Assessment report interface. At the top, it displays the report date (Nov 26, 2018), region (us-east-1), AWS EBS volumes (1934), and allocated capacity (567.6 TiB). A 'Start Again' button is also present. Below this, there are two main sections: 'Saving Opportunities' and 'Protection Risks (EBS Volumes)'. The 'Saving Opportunities' section shows a total annual saving opportunity of \$84,925, broken down into unattached EBS volumes (\$0 saving) and unassociated EBS snapshots (\$84,925 saving). It also includes a link to 'Snapshot Efficiencies'. The 'Protection Risks' section shows 1,921 / 1,934 volumes without EBS snapshots, an average RPO of a year, and an average number of EBS snapshots per volume of 1.23. It also includes a link to 'Snapshot Policies'. At the bottom, there are links for 'API', 'NetApp Internal', and copyright information (© 2018 NetApp, Inc. Provide Feedback).</p>

Step	Action
1-11	<p>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.</p>  <p>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.</p>

Step	Action
1-12	<p> In the Protection Risks, review your average recovery point objective (RPO) and click the info icon to get an explanation of this calculation.</p>  <p>How will NetApp protect your data?</p> <ul style="list-style-type: none">  Snapshot Policies <p>Leverage our automation capabilities to create and delete </p>
1-13	Click the back arrow to return to the top-level Cloud Assessment page and click the Microsoft Azure icon.
1-14	<p>Click Login with Azure.</p> 

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	

Step	Action
1-19	<p></p> <p>Following is what the report would look like with an Azure account with many active resources:</p>  <p>The screenshot displays the NetApp Azure Cloud Assessment interface. At the top, it shows the report date (Nov 26, 2018), subscription (HCL Main Subs...), managed disks (972), and allocated capacity (108.0 TiB). A 'Start Again' button is also present. Below this, there are two main sections: 'Saving Opportunities' and 'Protection (Managed Disks)'. The 'Saving Opportunities' section shows a total annual saving opportunity of \$91,592, broken down into \$91,224 for unattached disks and \$367 for unassociated snapshots. The 'Protection' section shows 963 out of 972 disks without snapshots. Other metrics shown include 450 unattached disks, 11 unassociated snapshots, an average RPO of 17 days, and an average of 2.78 snapshots per disk. At the bottom, there are links for 'Snapshot Efficiencies' and 'Snapshot Policies'.</p>
1-20	<p></p> <p>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.</p>

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

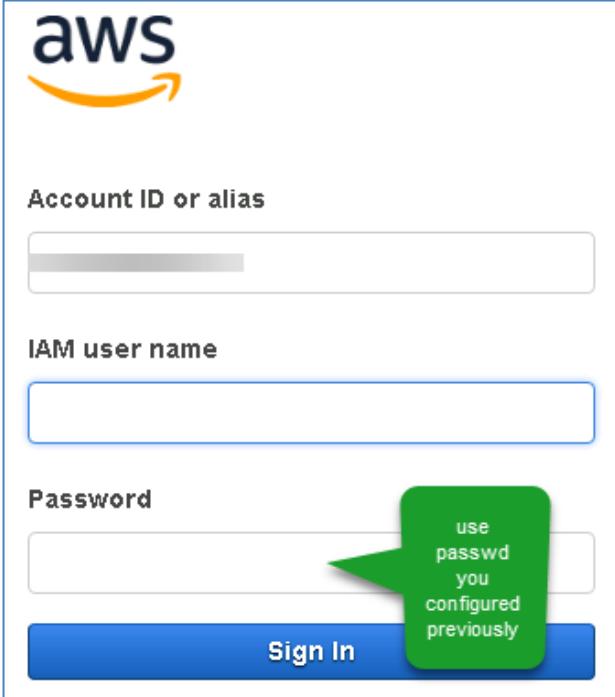
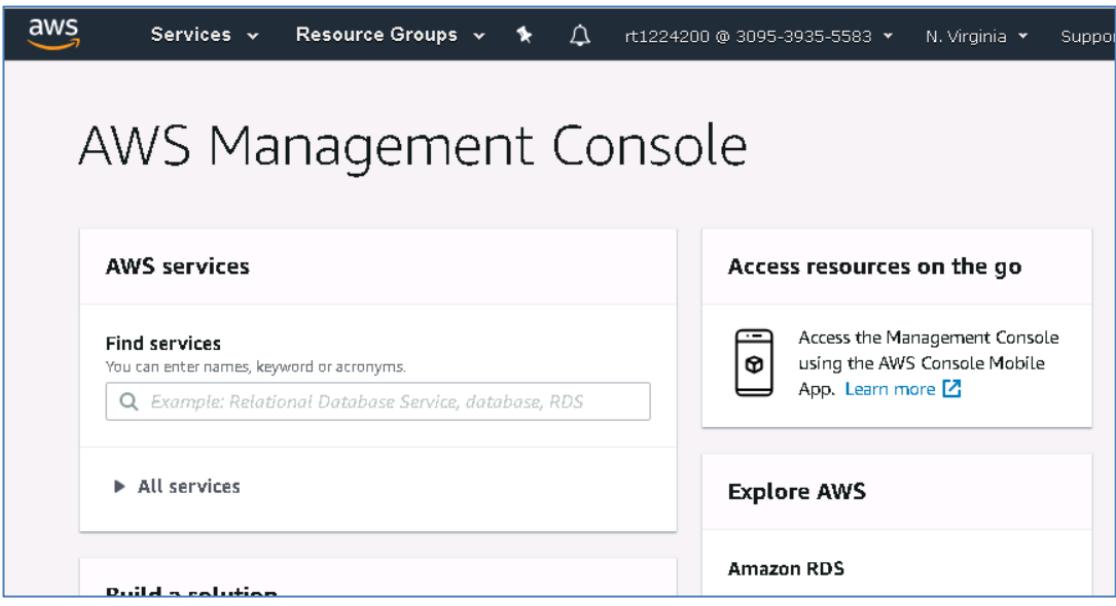
This exercise focuses on enabling you to do the following:

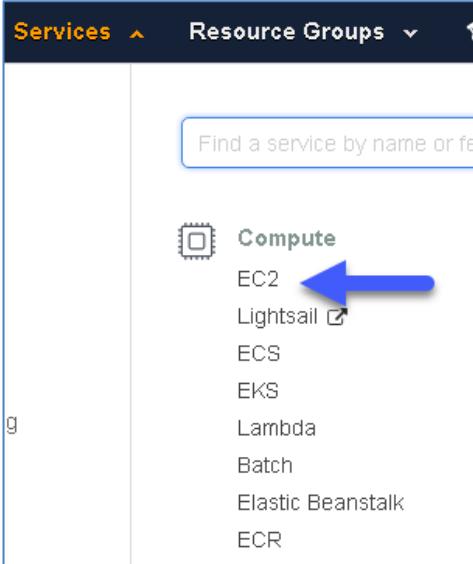
- Create an AWS VPC and associated subnets, internet gateways, and NAT gateway
- Provide security, routes, and access controls for the VPC
- Launch virtual machines VMs in private and public subnets and verify access between subnets

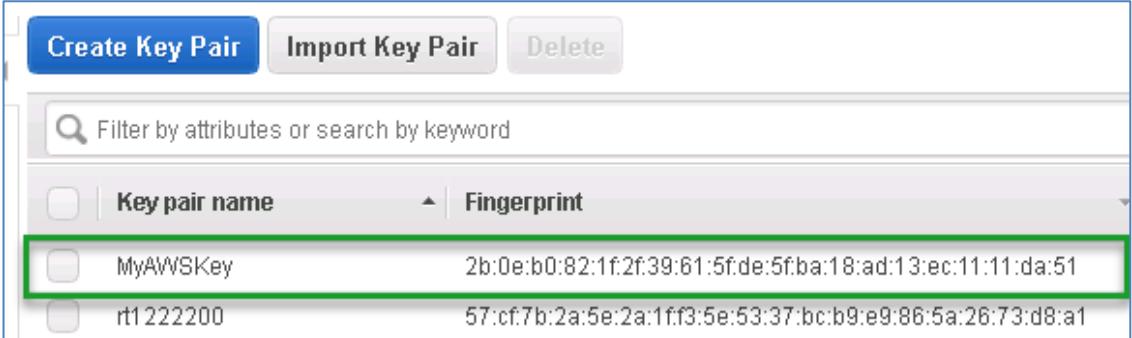
Task 1: Create a Key Pair for Use by CloudFormation Stack

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.  The icon is a black square with a white 'AWS' logo in the top left corner and the words 'AWS Console' in white at the bottom.

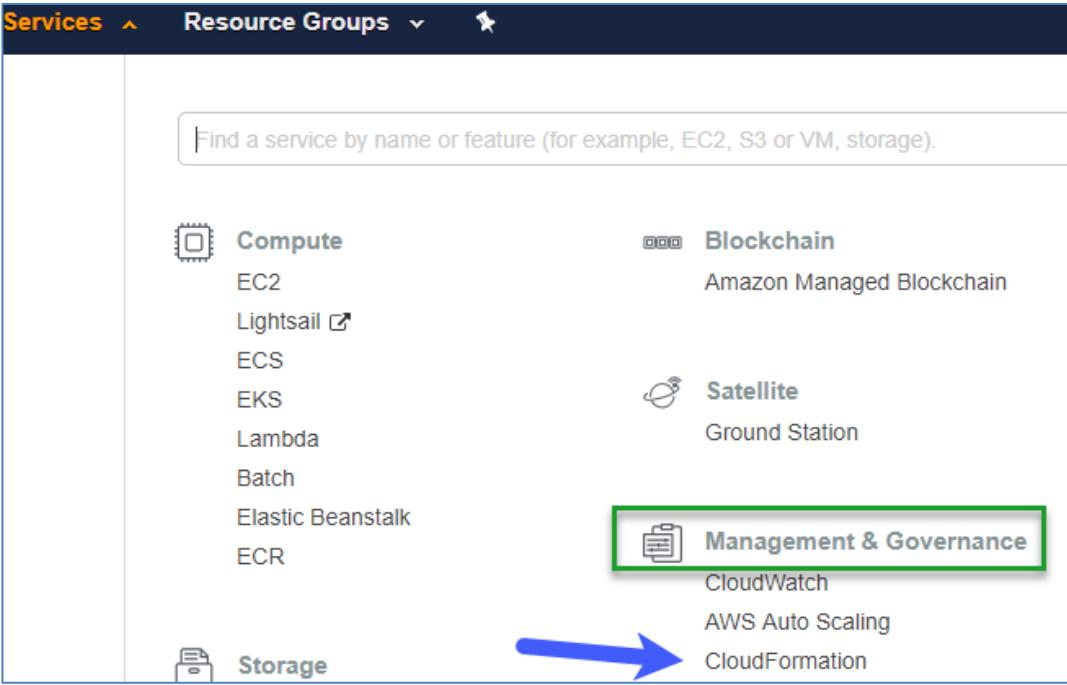
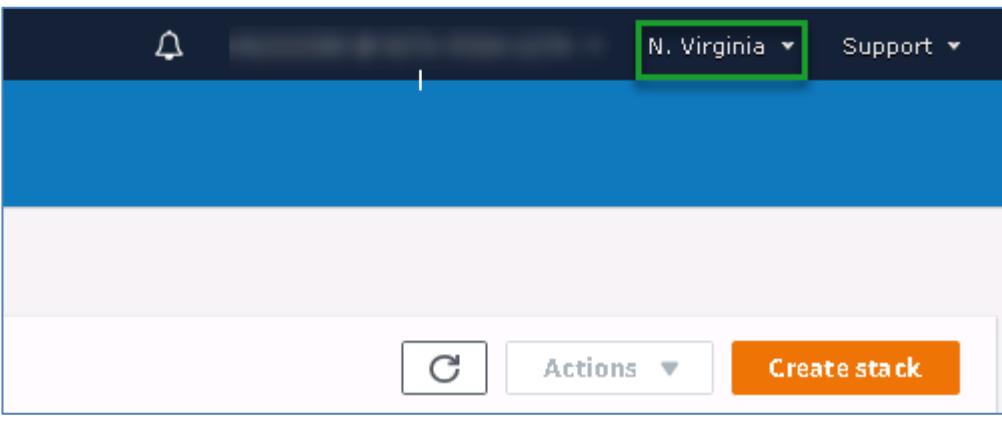
Step	Action
1-2	
1-3	 <p>Verify that you are in the N. Virginia region. If you are not in N. Virginia, select that region in the list. The NetApp University labs are in the same region, so making this selection decreases latency.</p> 
1-4	<p>Verify that the Console home page appears.</p> 

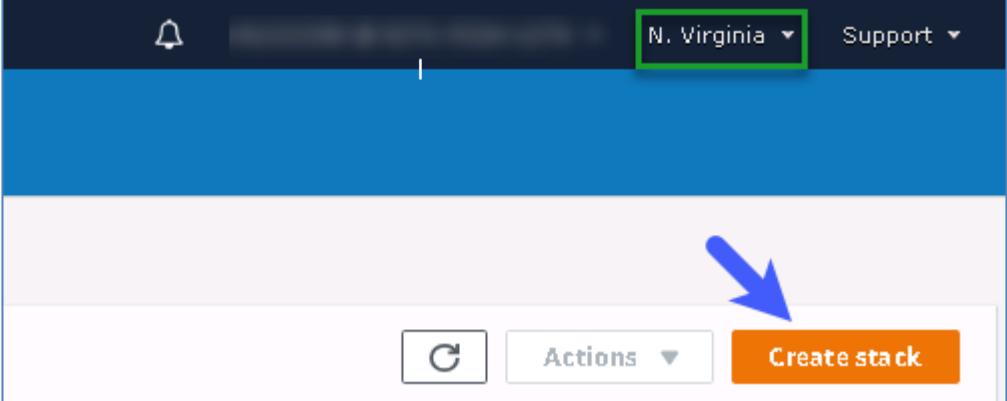
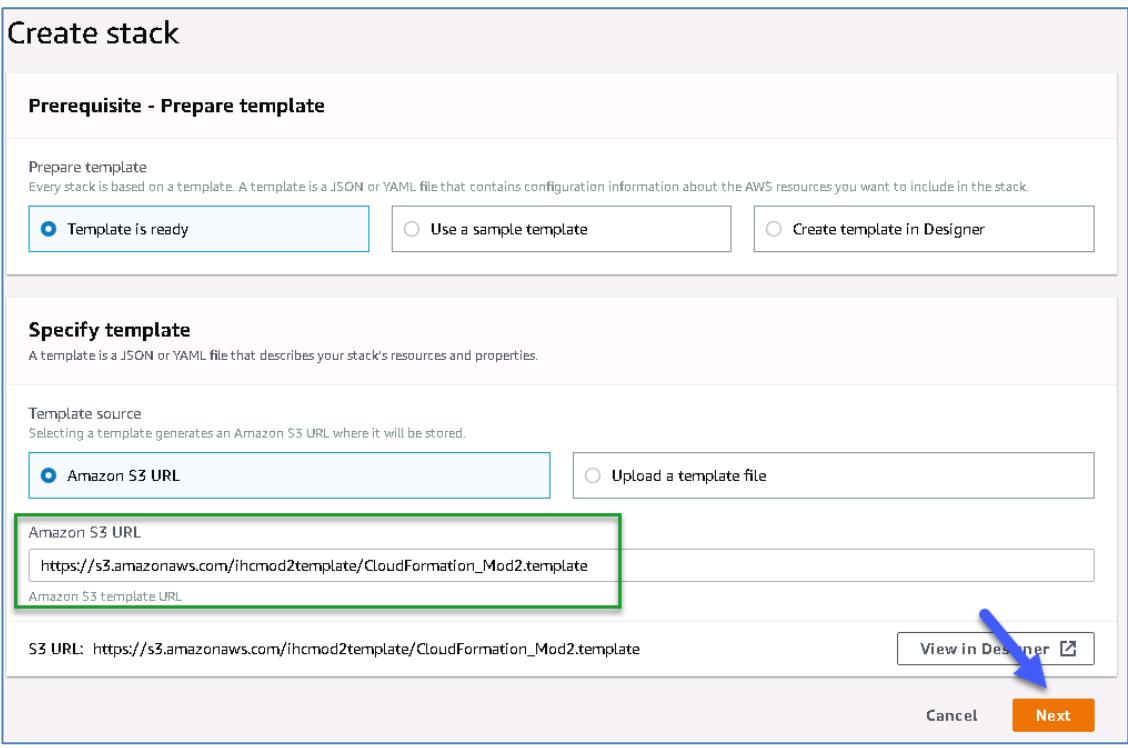
Step	Action
1-5	Select Services > EC2.
	
1-6	 You can start to type the name of the service, and it appears. After you have used a service, it appears on the History menu as well.
1-7	In the EC2 dashboard, select Key Pairs.
	
1-8	Click Create Key Pair.
1-9	In the Create Key Pair dialog box, enter the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

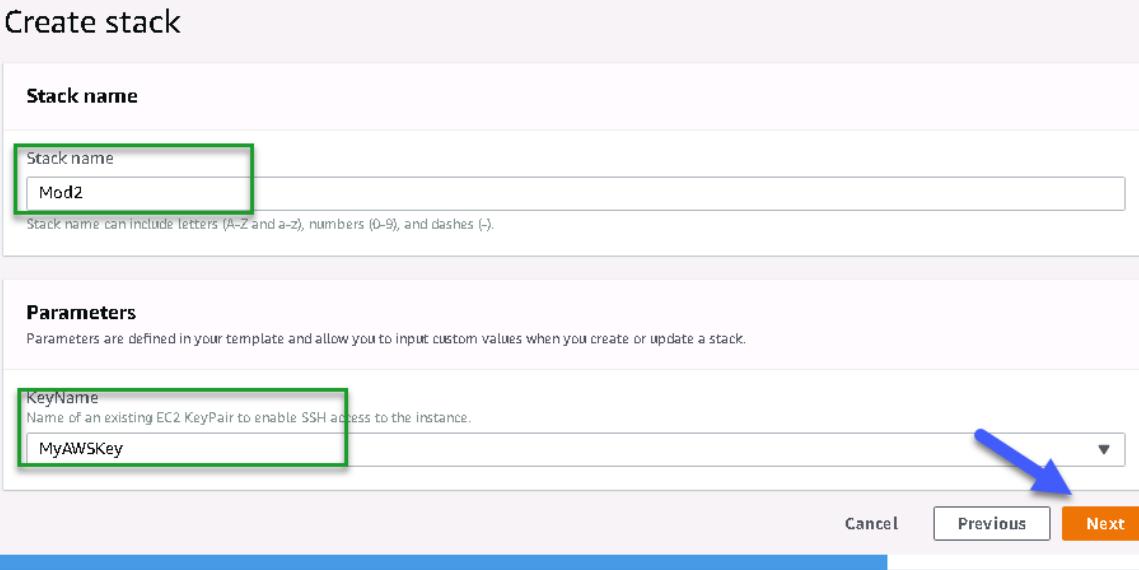
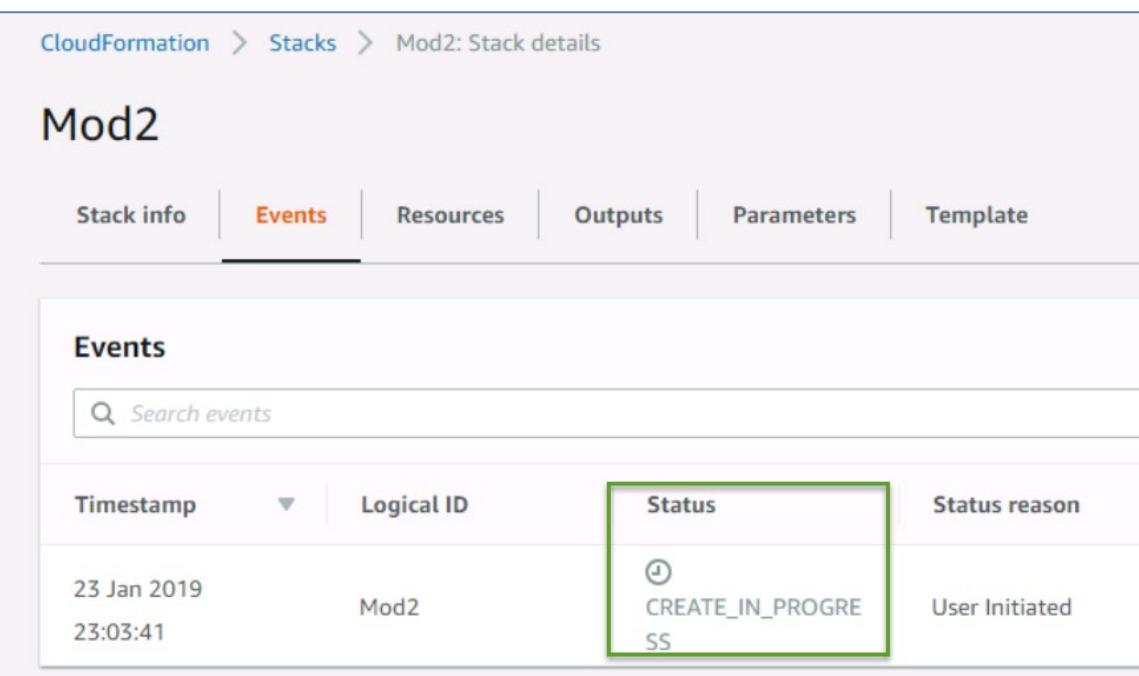
Step	Action						
1-10	<p>Verify that a Key Pair with the name MyAWSKey is created.</p>  <table border="1"> <thead> <tr> <th>Key pair name</th> <th>Fingerprint</th> </tr> </thead> <tbody> <tr> <td>MyAWSKey</td> <td>2b:0e:b0:82:1f:2f:39:61:5f:de:5f:ba:18:ad:13:ec:11:11:da:51</td> </tr> <tr> <td>rt1222200</td> <td>57:cf:7b:2a:5e:2a:1ff3:5e:53:37:bc:b9:e9:86:5a:26:73:d8:a1</td> </tr> </tbody> </table>	Key pair name	Fingerprint	MyAWSKey	2b:0e:b0:82:1f:2f:39:61:5f:de:5f:ba:18:ad:13:ec:11:11:da:51	rt1222200	57:cf:7b:2a:5e:2a:1ff3:5e:53:37:bc:b9:e9:86:5a:26:73:d8:a1
Key pair name	Fingerprint						
MyAWSKey	2b:0e:b0:82:1f:2f:39:61:5f:de:5f:ba:18:ad:13:ec:11:11:da:51						
rt1222200	57:cf:7b:2a:5e:2a:1ff3:5e:53:37:bc:b9:e9:86:5a:26:73:d8:a1						
1-11	 <p>The file MyAWSKey is automatically downloaded and is in your Downloads directory</p>						
1-12	<p>Move the MyAWSKey.pem file from the Downloads folder to the CourseFiles folder.</p>						

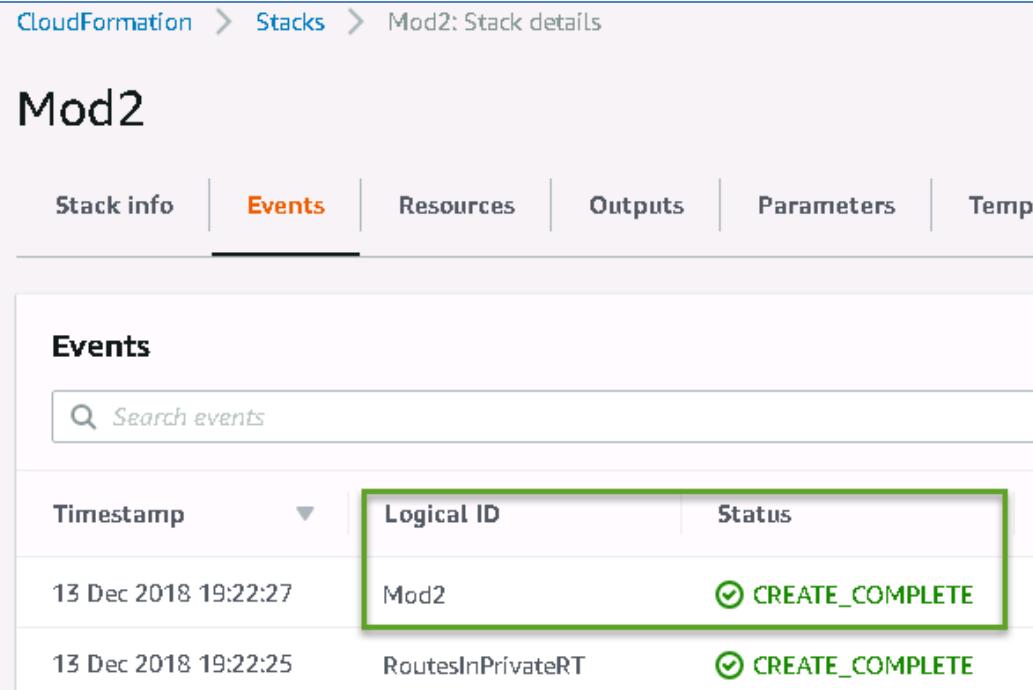
Task 2: Use a CloudFormation Template to Create a CloudFormation Stack

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. 

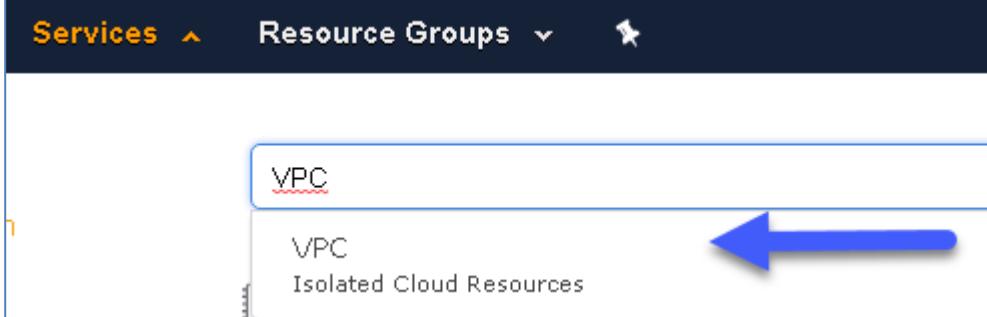
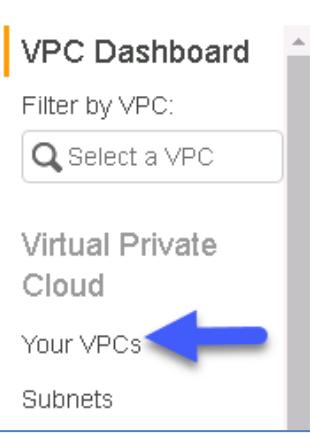
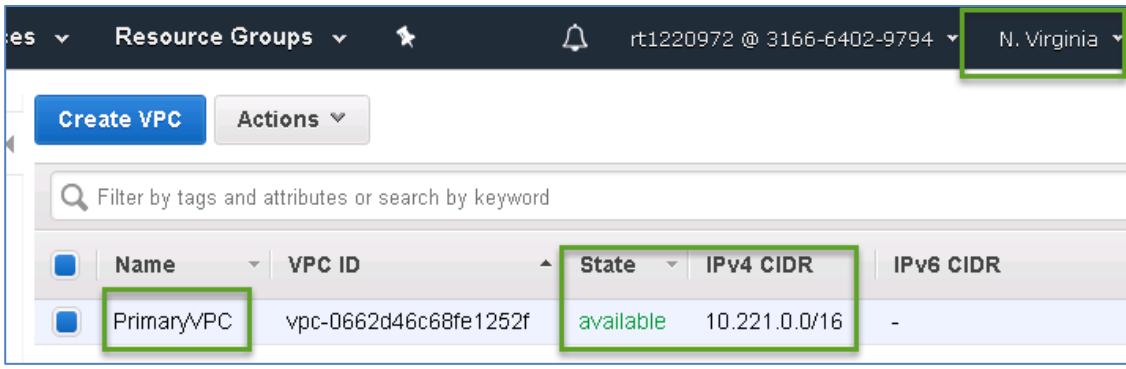
Step	Action
2-4	 CloudFormation stack creates resources in the region in which it runs. Because you need all your resources for this class to be in the N.Virginia region, you create the stack in the N.Virginia region.
2-5	Click Create stack . 
2-6	In the Specify template section, enter the following URL, and then click Next . Amazon S3 URL: https://s3.amazonaws.com/ihcmo2template/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.

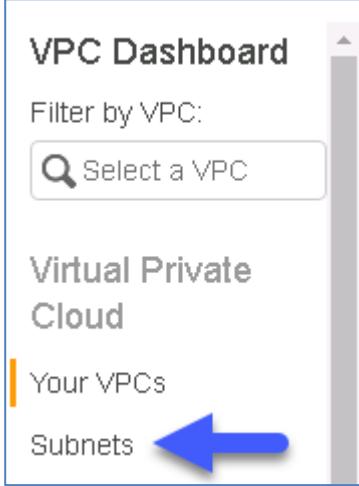
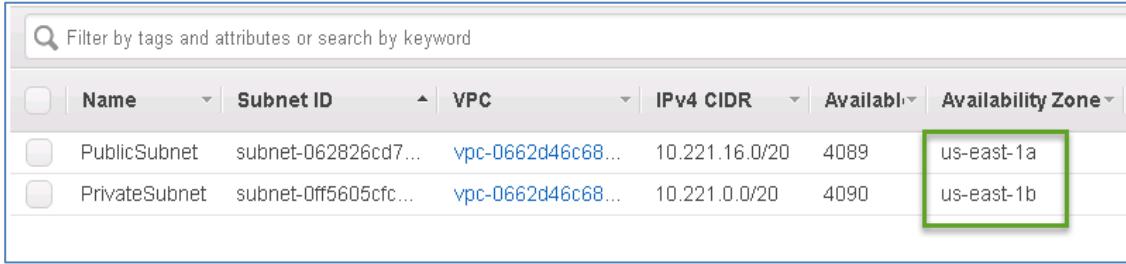
Step	Action
2-8	<p>In the Create stack page, enter the following information, and click Next.</p> <ul style="list-style-type: none"> • Stack Name: Mod2 • KeyName: Select MyAWSKey from the list. 
2-9	In the Configure stack options page, accept the defaults, and click Next .
2-10	In the Review Mod2 page, review your information, scroll to the bottom, and then click Create Stack .
2-11	<p>Verify that the status is CREATE_IN_PROGRESS.</p> 

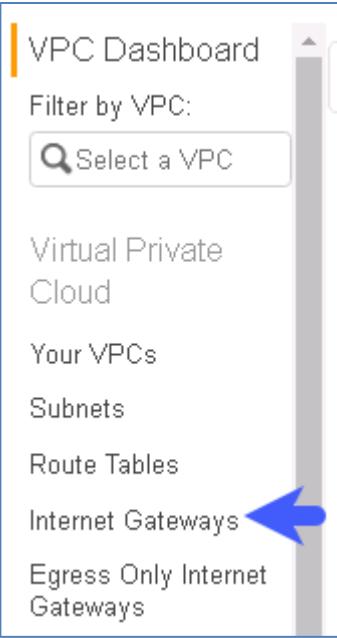
Step	Action									
2-12	 The stack starts running to create the resources that are specified in the template. When the stack finishes running, the status is CREATE_COMPLETE. This process should take no more than 3-5 minutes. Afterward, you review all the resources that are created.									
2-13	Click the Refresh button until the status for Mod2 becomes CREATE_COMPLETE . <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Timestamp</th> <th style="text-align: left;">Logical ID</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>13 Dec 2018 19:22:27</td> <td>Mod2</td> <td>✓ CREATE_COMPLETE</td> </tr> <tr> <td>13 Dec 2018 19:22:25</td> <td>RoutesInPrivateRT</td> <td>✓ CREATE_COMPLETE</td> </tr> </tbody> </table> </div>	Timestamp	Logical ID	Status	13 Dec 2018 19:22:27	Mod2	✓ CREATE_COMPLETE	13 Dec 2018 19:22:25	RoutesInPrivateRT	✓ CREATE_COMPLETE
Timestamp	Logical ID	Status								
13 Dec 2018 19:22:27	Mod2	✓ CREATE_COMPLETE								
13 Dec 2018 19:22:25	RoutesInPrivateRT	✓ CREATE_COMPLETE								

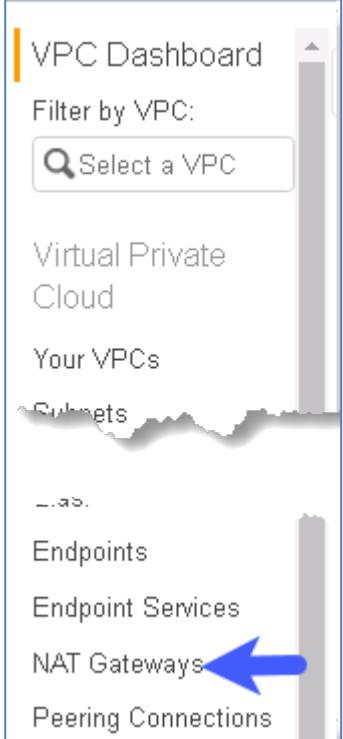
Task 3: Review VPC, Subnets, Internet Gateway, and NAT Gateway

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: <ul style="list-style-type: none">• Name: PrimaryVPC• State: available• IPv4 CIDR: 10.221.0.0/16• Region: N.Virginia  <table border="1"><thead><tr><th>Name</th><th>VPC ID</th><th>State</th><th>IPv4 CIDR</th><th>IPv6 CIDR</th></tr></thead><tbody><tr><td>PrimaryVPC</td><td>vpc-0662d46c68fe1252f</td><td>available</td><td>10.221.0.0/16</td><td>-</td></tr></tbody></table>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	PrimaryVPC	vpc-0662d46c68fe1252f	available	10.221.0.0/16	-
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR							
PrimaryVPC	vpc-0662d46c68fe1252f	available	10.221.0.0/16	-							

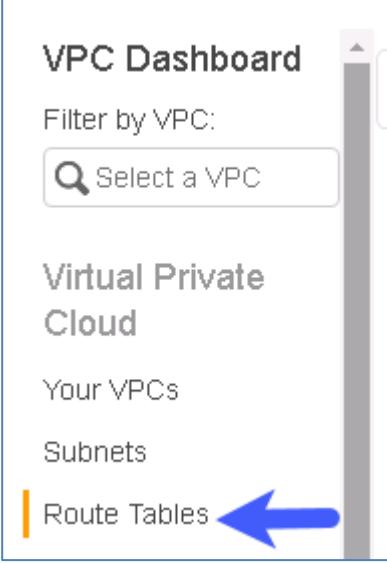
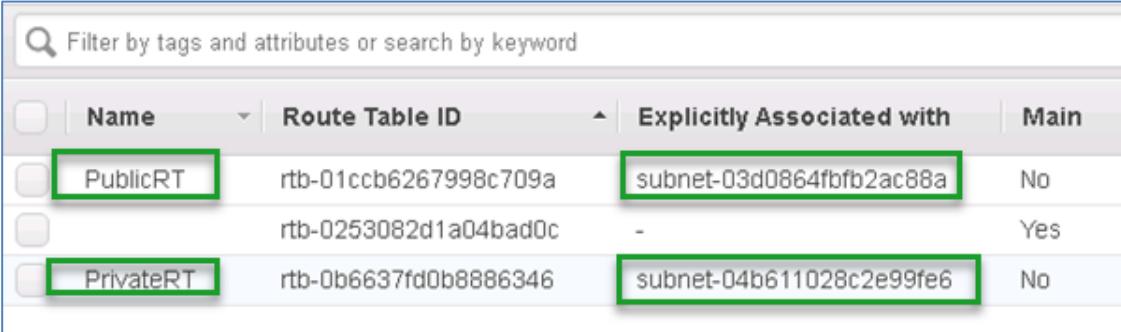
Step	Action																		
3-4	<p>In the VPC Dashboard menu, click Subnets.</p> 																		
3-5	<p>Verify that you see two subnets and verify that the Availability Zones are unique between the two subnets:</p> <p>Names: PublicSubnet and PrivateSubnet</p> <p>IPv4 CIDR: 10.221.16.0/20 for PublicSubnet and 10.221.0.0/20 for PrivateSubnet</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Subnet ID</th> <th>VPC</th> <th>IPv4 CIDR</th> <th>Available</th> <th>Availability Zone</th> </tr> </thead> <tbody> <tr> <td>PublicSubnet</td> <td>subnet-062826cd7...</td> <td>vpc-0662d46c68...</td> <td>10.221.16.0/20</td> <td>4089</td> <td>us-east-1a</td> </tr> <tr> <td>PrivateSubnet</td> <td>subnet-0ff5605cf...</td> <td>vpc-0662d46c68...</td> <td>10.221.0.0/20</td> <td>4090</td> <td>us-east-1b</td> </tr> </tbody> </table>	Name	Subnet ID	VPC	IPv4 CIDR	Available	Availability Zone	PublicSubnet	subnet-062826cd7...	vpc-0662d46c68...	10.221.16.0/20	4089	us-east-1a	PrivateSubnet	subnet-0ff5605cf...	vpc-0662d46c68...	10.221.0.0/20	4090	us-east-1b
Name	Subnet ID	VPC	IPv4 CIDR	Available	Availability Zone														
PublicSubnet	subnet-062826cd7...	vpc-0662d46c68...	10.221.16.0/20	4089	us-east-1a														
PrivateSubnet	subnet-0ff5605cf...	vpc-0662d46c68...	10.221.0.0/20	4090	us-east-1b														

Step	Action										
3-6	<p>In the VPC Dashboard menu, click Internet Gateways.</p> 										
3-7	<p>Verify that you see an IGW attached to the PrimaryVPC.</p>  <table border="1"> <thead> <tr> <th></th> <th>Name</th> <th>ID</th> <th>State</th> <th>VPC</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>IGW</td> <td>igw-0b7bbd50589...</td> <td>attached</td> <td>vpc-0662d46c68fe1252f PrimaryVPC</td> </tr> </tbody> </table>		Name	ID	State	VPC	<input type="checkbox"/>	IGW	igw-0b7bbd50589...	attached	vpc-0662d46c68fe1252f PrimaryVPC
	Name	ID	State	VPC							
<input type="checkbox"/>	IGW	igw-0b7bbd50589...	attached	vpc-0662d46c68fe1252f PrimaryVPC							

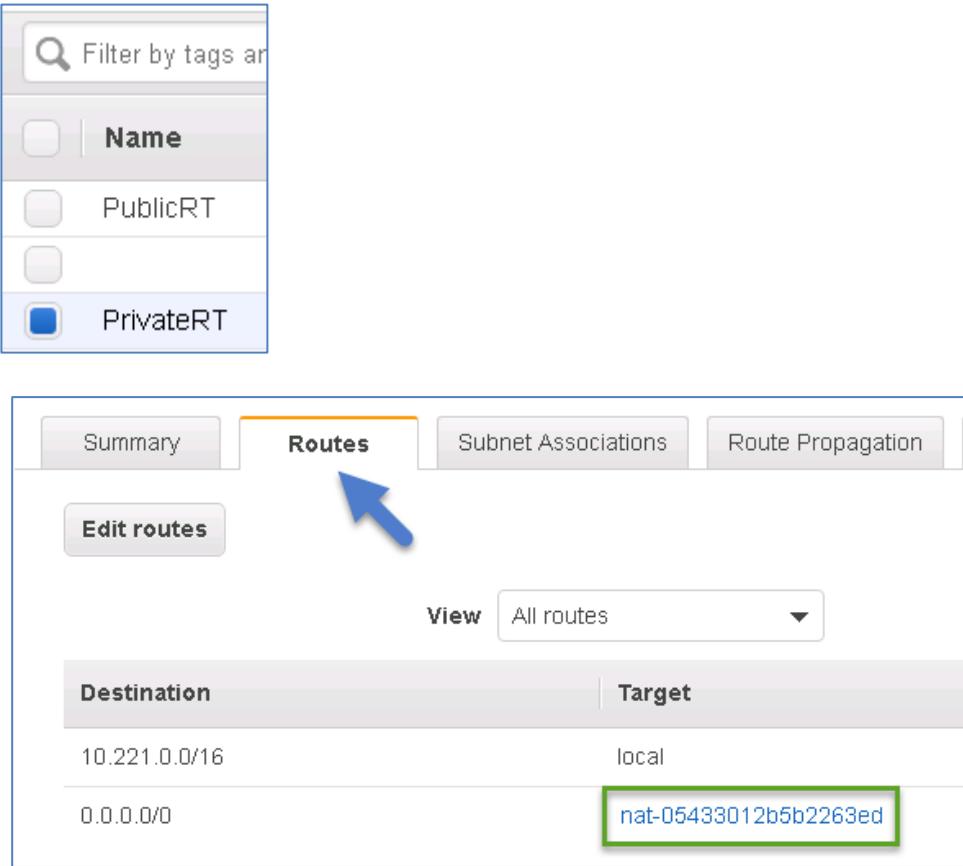
Step	Action
3-8	Click NAT Gateways
	
3-9	Verify that you see a NAT gateway that is created in the public subnet.
3-10	 The NAT gateway has a public IP (elastic IP address) that is externally available and a private IP address. It is created in the public subnet so that traffic from the private subnet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

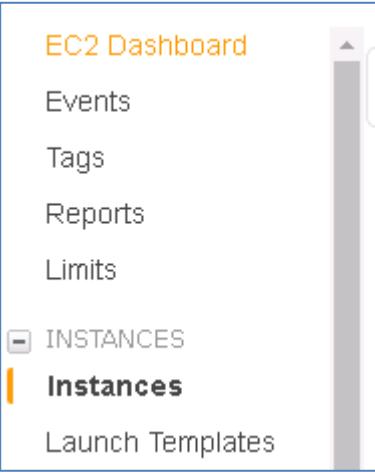
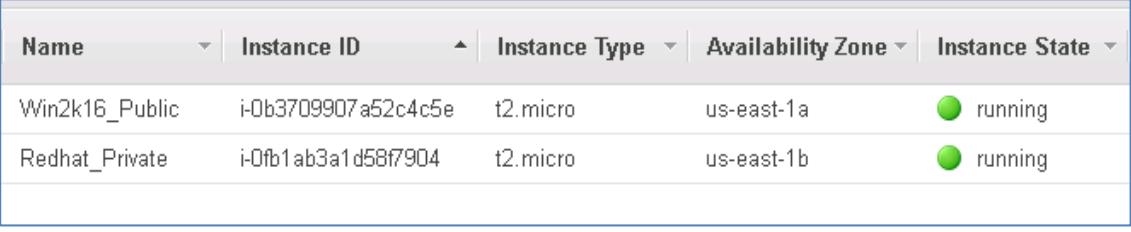
Step	Action																				
4-1	<p>In the VPC Dashboard, click Route Tables.</p> 																				
4-2	<p>Verify that you see a PublicRT and PrivateRT and that they are explicitly associated with subnets. (You can check the subnets to which they are associated in a later step.)</p>  <table border="1"><thead><tr><th></th><th>Name</th><th>Route Table ID</th><th>Explicitly Associated with</th><th>Main</th></tr></thead><tbody><tr><td></td><td>PublicRT</td><td>rtb-01ccb6267998c709a</td><td>subnet-03d0864fbfb2ac88a</td><td>No</td></tr><tr><td></td><td></td><td>rtb-0253082d1a04bad0c</td><td>-</td><td>Yes</td></tr><tr><td></td><td>PrivateRT</td><td>rtb-0b6637fd0b8886346</td><td>subnet-04b611028c2e99fe6</td><td>No</td></tr></tbody></table>		Name	Route Table ID	Explicitly Associated with	Main		PublicRT	rtb-01ccb6267998c709a	subnet-03d0864fbfb2ac88a	No			rtb-0253082d1a04bad0c	-	Yes		PrivateRT	rtb-0b6637fd0b8886346	subnet-04b611028c2e99fe6	No
	Name	Route Table ID	Explicitly Associated with	Main																	
	PublicRT	rtb-01ccb6267998c709a	subnet-03d0864fbfb2ac88a	No																	
		rtb-0253082d1a04bad0c	-	Yes																	
	PrivateRT	rtb-0b6637fd0b8886346	subnet-04b611028c2e99fe6	No																	

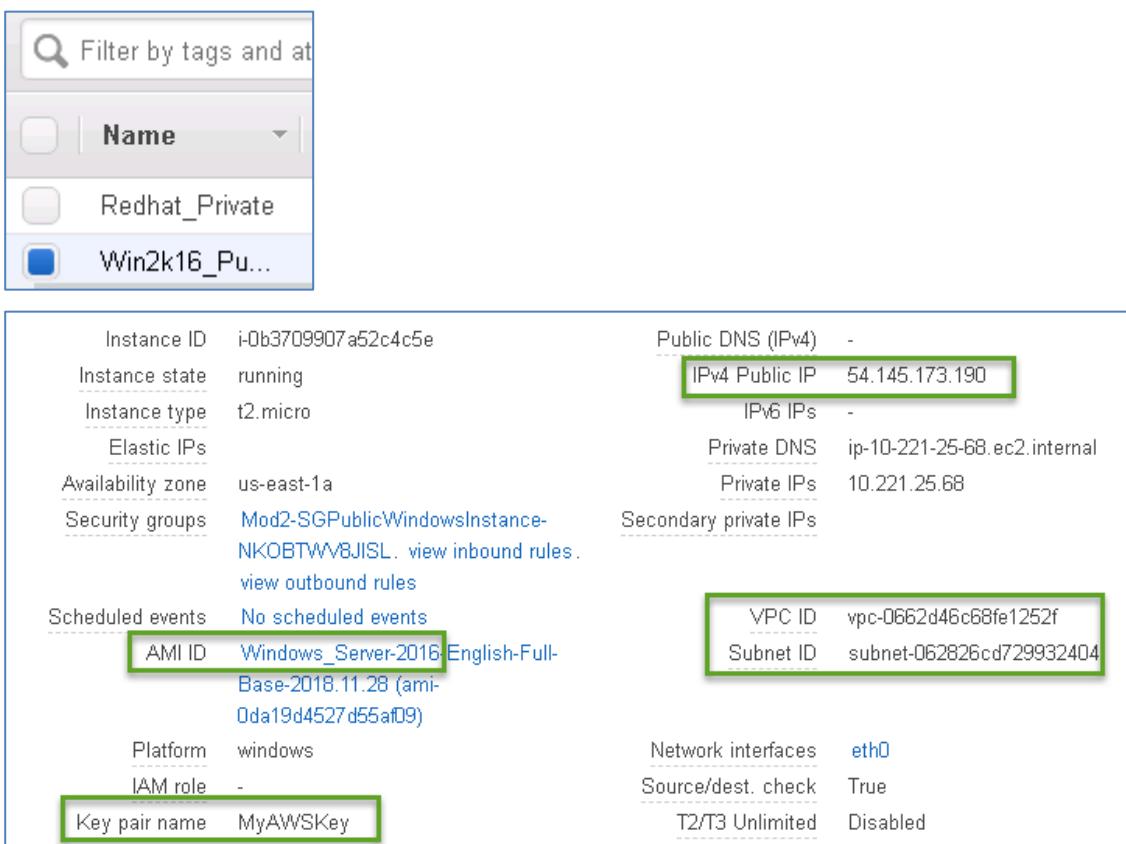
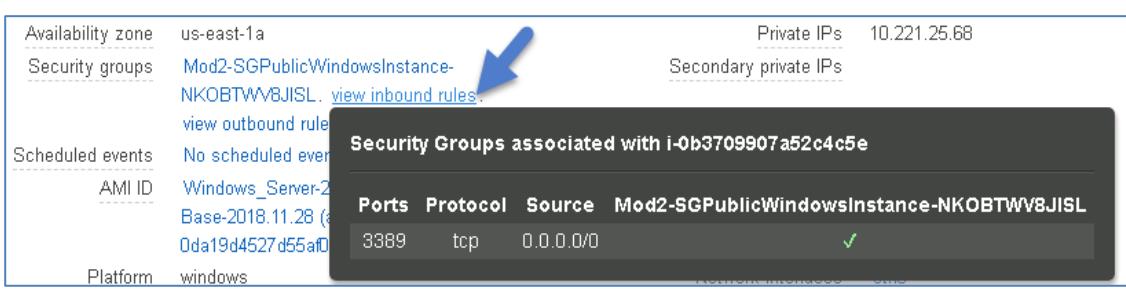
Step	Action						
4-3	<p>Select PublicRT and review the routes that are in the Routes tab.</p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> </tr> </thead> <tbody> <tr> <td>10.221.0.0/16</td> <td>local</td> </tr> <tr> <td>0.0.0.0/0</td> <td>igw-0b7bbd505892ea4d9</td> </tr> </tbody> </table>	Destination	Target	10.221.0.0/16	local	0.0.0.0/0	igw-0b7bbd505892ea4d9
Destination	Target						
10.221.0.0/16	local						
0.0.0.0/0	igw-0b7bbd505892ea4d9						
4-4	<p> 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.</p>						
4-5	<p>Review the Subnet Associations for the PublicRT.</p> <table border="1"> <thead> <tr> <th>Subnet ID</th> <th>IPv4 CIDR</th> <th>IPv6 CIDR</th> </tr> </thead> <tbody> <tr> <td>subnet-03d0864fbfb2ac88a PublicSubnet</td> <td>10.221.16.0/20</td> <td>-</td> </tr> </tbody> </table>	Subnet ID	IPv4 CIDR	IPv6 CIDR	subnet-03d0864fbfb2ac88a PublicSubnet	10.221.16.0/20	-
Subnet ID	IPv4 CIDR	IPv6 CIDR					
subnet-03d0864fbfb2ac88a PublicSubnet	10.221.16.0/20	-					
4-6	<p> This route table is explicitly associated with the public subnet to route traffic locally and to the internet</p>						

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

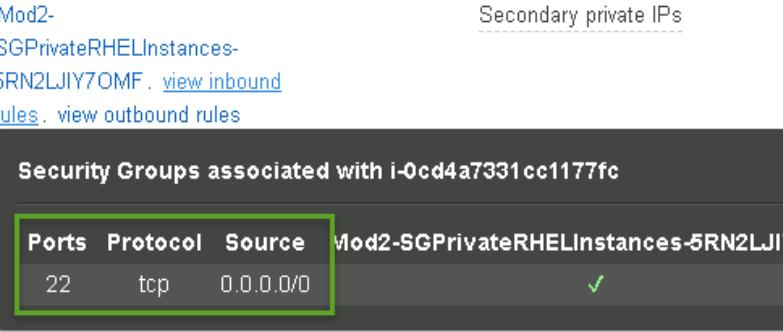
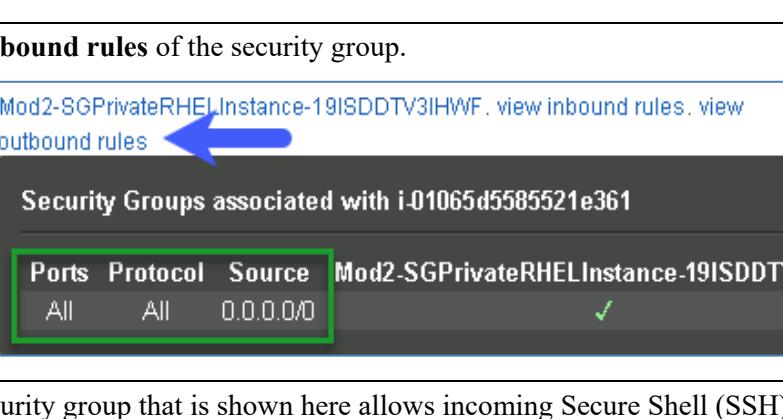
Task 5: Review Public and Private Amazon EC2 Instances That Are Created and the Security Groups with Which They Are Associated

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.  <p>The screenshot shows the AWS Services menu with a search bar at the top. Below it, there are three main categories: Compute (with EC2, Lightsail, ECS, EKS, Lambda), Blockchain (with Amazon Managed Blockchain), and Satellite (with Ground Station).</p>															
5-2	In the EC2 Dashboard, click Instances .  <p>The screenshot shows the EC2 Dashboard sidebar. The 'INSTANCES' section is expanded, and the 'Instances' option is selected, indicated by an orange vertical bar on the left.</p>															
5-3	Verify that you see the following instances and that the Instance State is running.  <p>The screenshot shows the EC2 Instances table with the following data:</p> <table border="1"><thead><tr><th>Name</th><th>Instance ID</th><th>Instance Type</th><th>Availability Zone</th><th>Instance State</th></tr></thead><tbody><tr><td>Win2k16_Public</td><td>i-0b3709907a52c4c5e</td><td>t2.micro</td><td>us-east-1a</td><td>● running</td></tr><tr><td>Redhat_Private</td><td>i-0fb1ab3a1d58f7904</td><td>t2.micro</td><td>us-east-1b</td><td>● running</td></tr></tbody></table>	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
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												

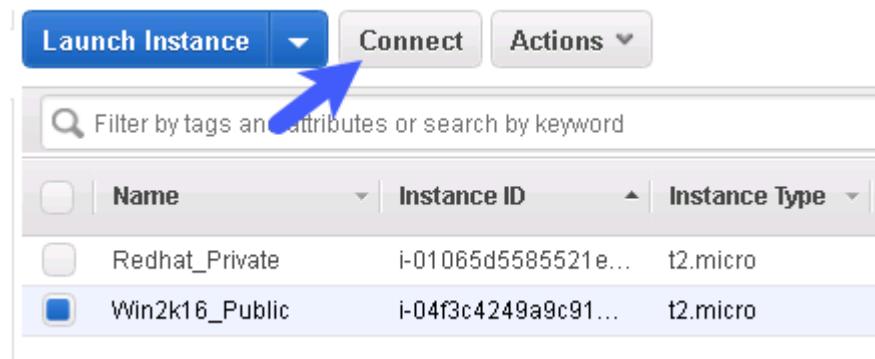
Step	Action
5-4	<p>Select Win2k16_Public, and review the details in the bottom of the window:</p> <ol style="list-style-type: none"> Verify that the instance is running the AMI Windows_Server-2016-Base-2018.11.28 (ami-Oda19d4527d55af09). Verify that VPC is PrimaryVPC and the subnet is Public Subnet by matching the IDs in the VPC Dashboard. Verify that the instance has a public IP. (The Public IP that you see might be different from what you see in the example.) Verify that the instance was deployed with the key pair MyAWSKey.pem 
5-5	<p>Click view inbound rules of the security group.</p> 

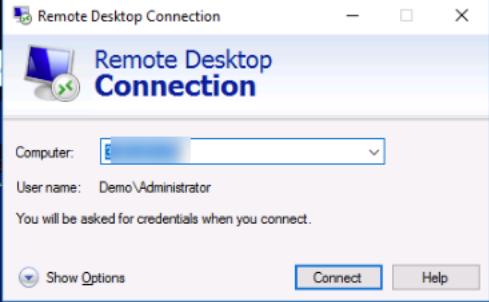
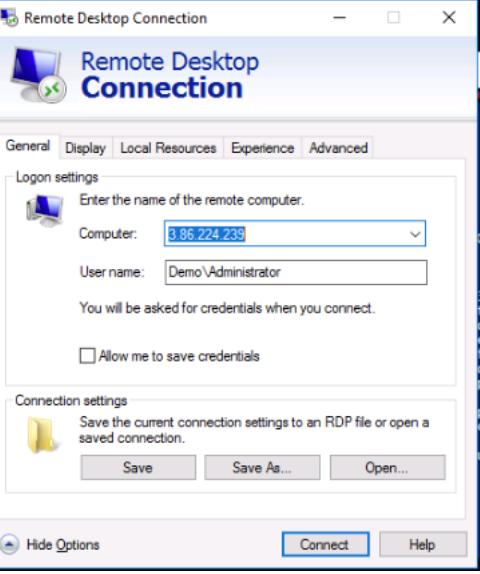
Step	Action
5-6	<p>Click view outbound rules of the security group.</p>
5-7	<p> The security groups act as a firewall for the instances that are associated with them. The security group that is shown here allows incoming Remote Desktop Protocol (RDP) traffic on port 3389 from any source to the Windows instance. You use RDP to log in to this instance in the next task.</p> <p>In the outbound direction from the Amazon EC2 instance, the security group allows all protocol traffic.</p>
5-8	<p>Select Redhat_Private, and review the details in the bottom of the window:</p> <ol style="list-style-type: none"> Verify that the instance is running the AMI RHEL-7.6_HVM*. Verify that VPC is PrimaryVPC and the subnet is PrivateSubnet by matching the IDs in the VPC Dashboard. There is no Public IP. Make a note of the following information: Private IP: _____ Verify that the instance was deployed with the key pair MyAWSKey.pem

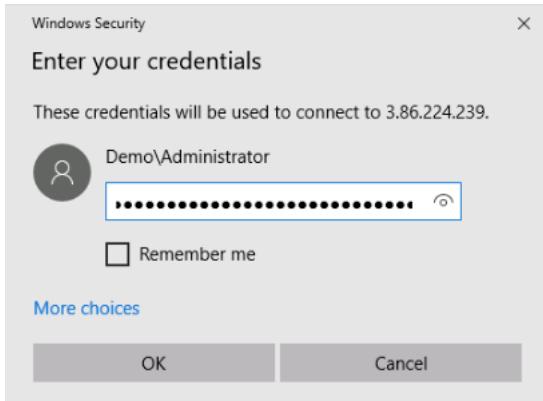
Step	Action						
5-9	<p>Click the view inbound rules of the security group.</p>  <table border="1"> <thead> <tr> <th>Ports</th> <th>Protocol</th> <th>Source</th> </tr> </thead> <tbody> <tr> <td>22</td> <td>tcp</td> <td>0.0.0.0/0</td> </tr> </tbody> </table>	Ports	Protocol	Source	22	tcp	0.0.0.0/0
Ports	Protocol	Source					
22	tcp	0.0.0.0/0					
5-10	<p>Click the view outbound rules of the security group.</p>  <table border="1"> <thead> <tr> <th>Ports</th> <th>Protocol</th> <th>Source</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>All</td> <td>0.0.0.0/0</td> </tr> </tbody> </table>	Ports	Protocol	Source	All	All	0.0.0.0/0
Ports	Protocol	Source					
All	All	0.0.0.0/0					
5-11	<p>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.</p>						

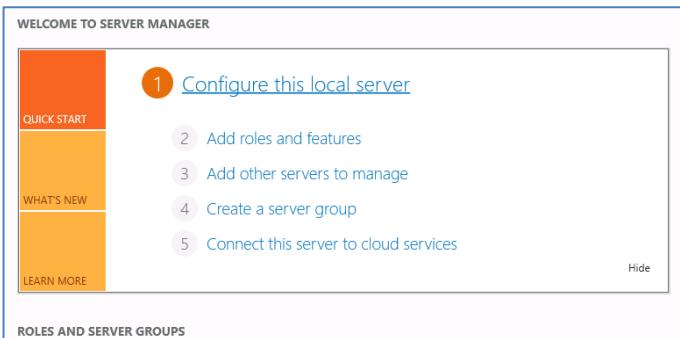
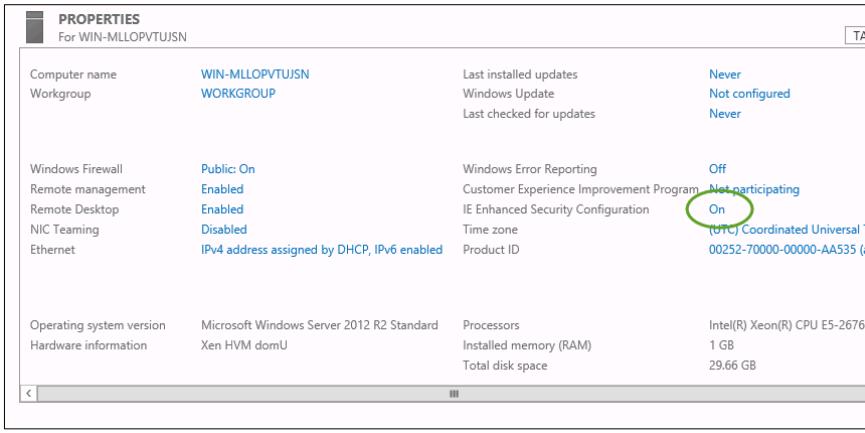
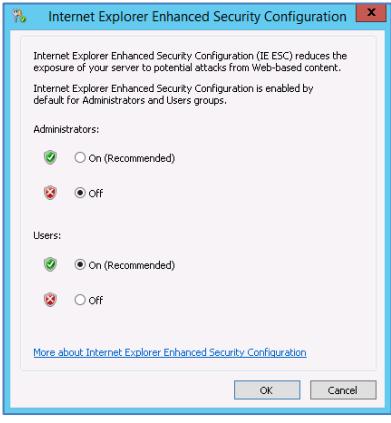
Task 6: Log In to the Windows Server Amazon EC2 Instances in Public Subnet

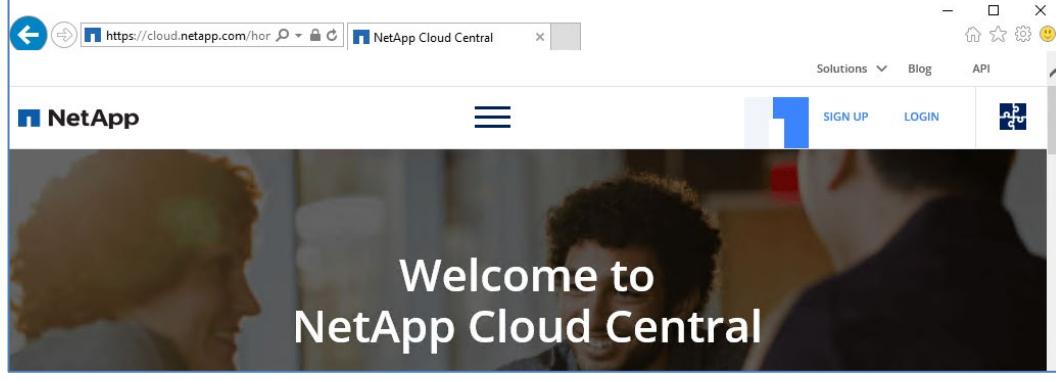
In this task, you connect to the Windows instance in the public subnet through RDP and verify access to the internet from this instance.

Step	Action
6-1	<p>On the Instances dashboard, complete the following actions:</p> <ol style="list-style-type: none">Select the Win2k16_Public instance.Click Connect. 
6-2	<p>In the Connect To Your Instance window, click Get Password.</p> 
6-3	<p>In the Connect To Your Instance > Get Password window, next to Key Pair Path, click Choose File.</p>
6-4	<p>Select the MyAWSKey.pem file that you saved in the CourseFiles folder, and then click Open.</p>
6-5	<p>Click Decrypt Password.</p>

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

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

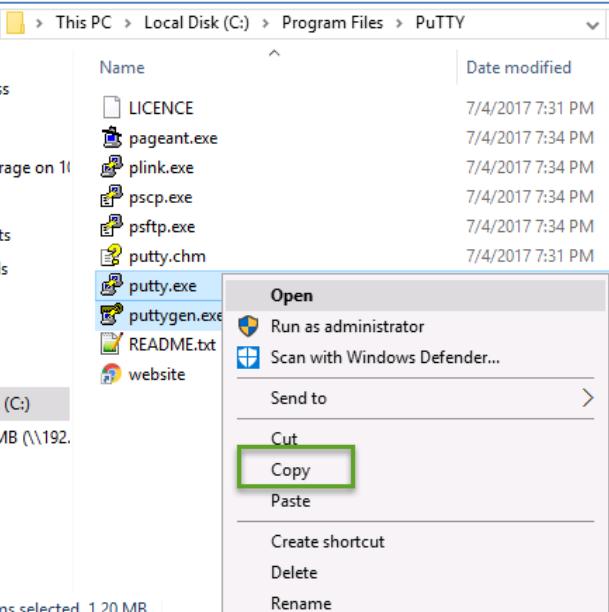
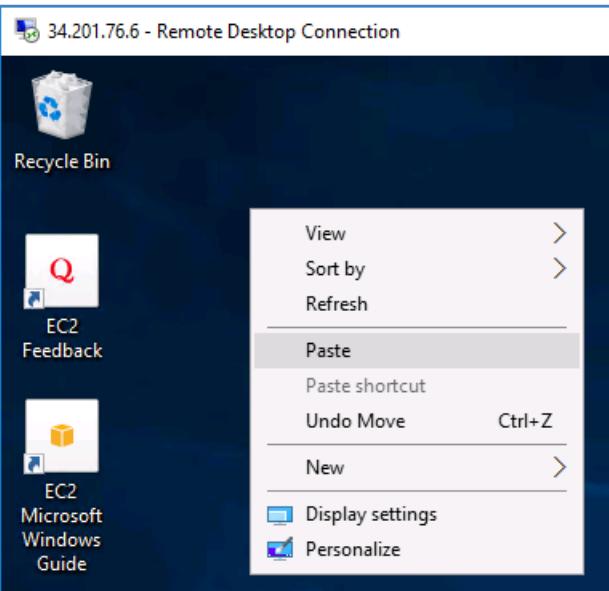
Step	Action
6-15	<p>Click Configure this local server.</p> 
6-16	<p>In the Properties section, to the right of IE Enhanced Security Configuration, click On.</p> 
6-17	<p>In the Internet Explorer Enhanced Security Configuration window, complete the following actions to turn off Internet Explorer Enhanced Security Confirmation:</p> <ol style="list-style-type: none"> a. Under Administrators, select Off. b. Click OK. 

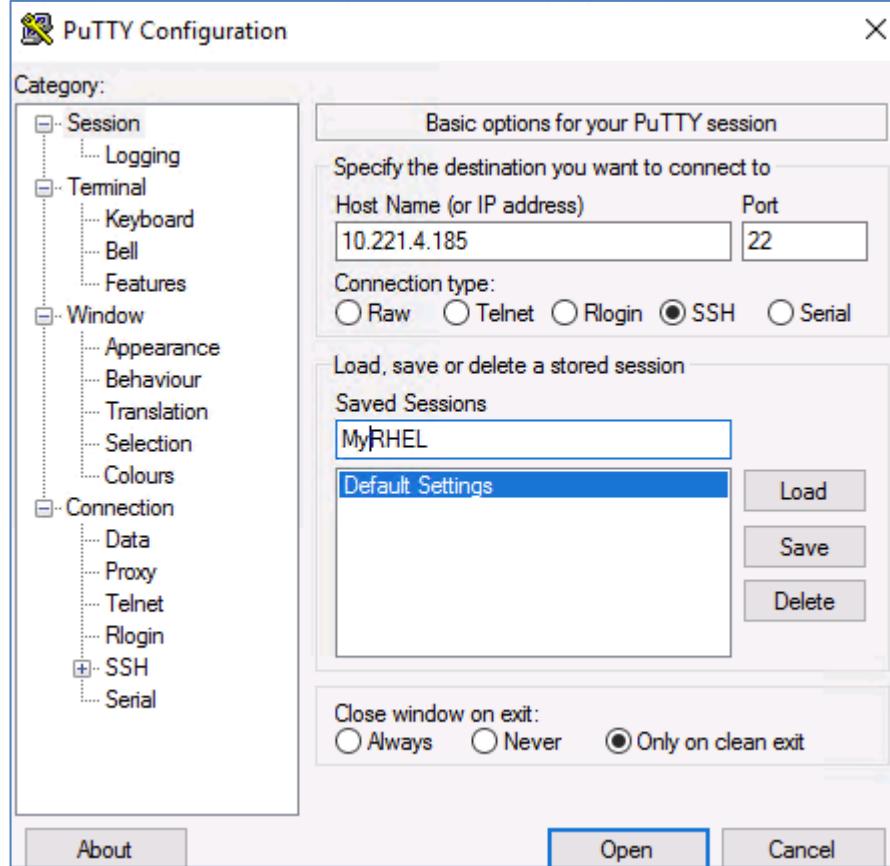
Step	Action
6-18	Click the Start menu.
	
6-19	Click Internet Explorer .
6-20	In Internet Explorer, enter the URL http://cloud.netapp.com to verify that this Windows Server, which is in the public subnet, can reach the internet through the internet gateway.
6-21	Verify that the NetApp Cloud Central page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

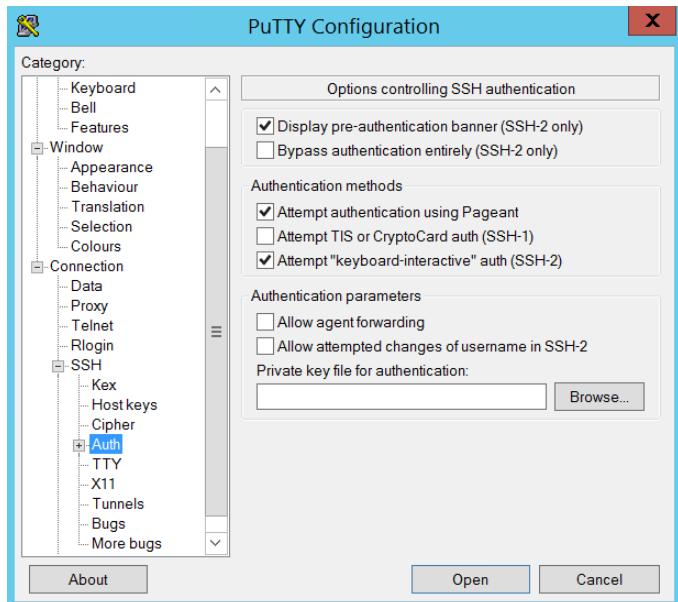
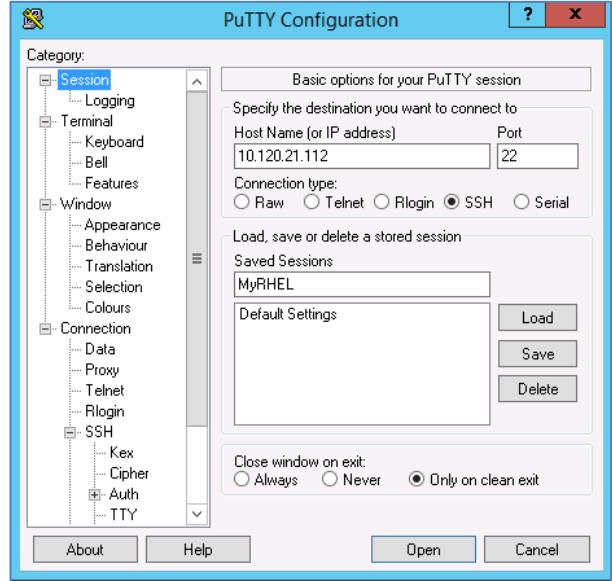
Task 7: Log In to the Linux Server Amazon EC2 Instances in Private Subnet

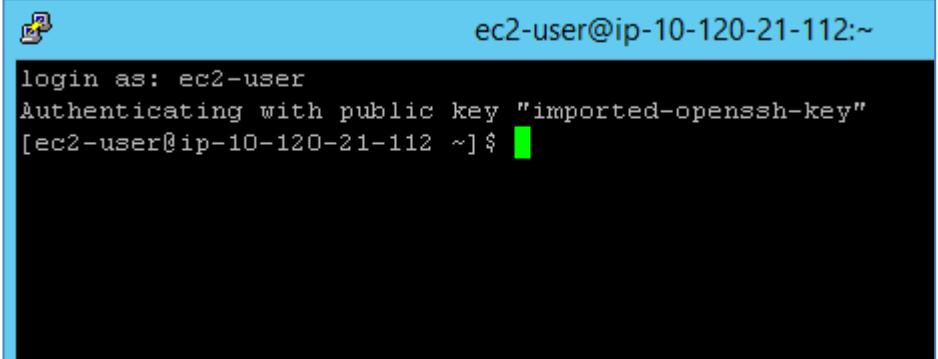
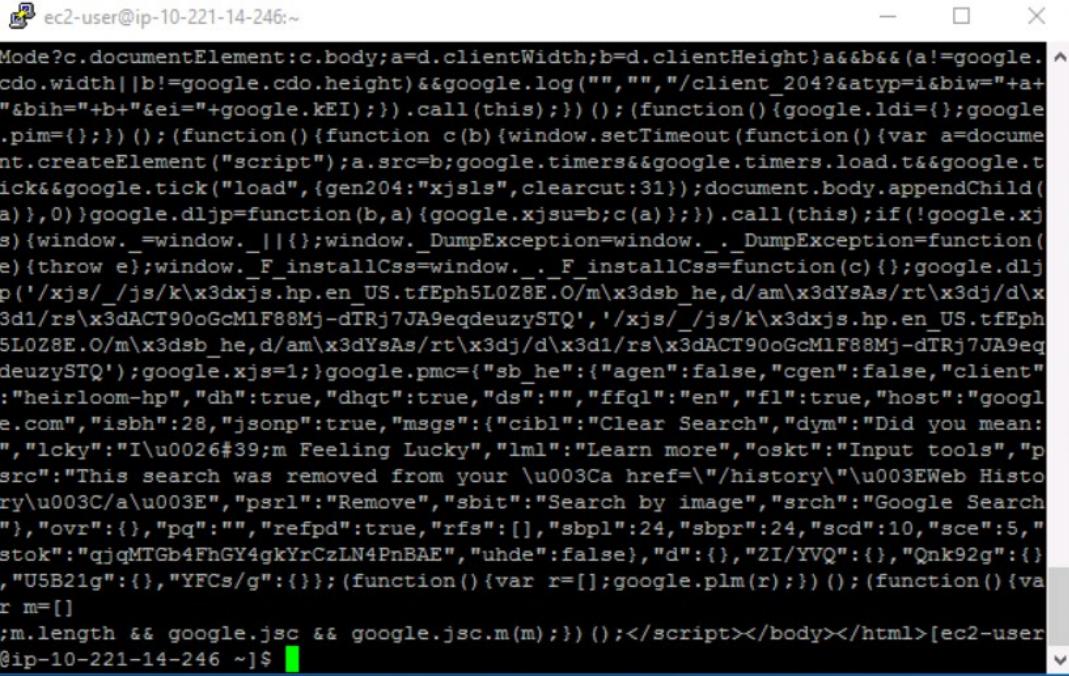
Use SSH to access the Linux instance from the Windows Server instance and verify access to the internet from this Linux Server instance.

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	<p>Copy the putty.exe and puttygen.exe files from your jump host C:\Program Files\PuTTY to the Public_W2K16 desktop. (Note on the jump host desktop the putty and puttygen are just links, so you cannot copy directly from the desktop.)</p>  
7-5	<p>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.</p>
7-6	<p>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</p> <p>Note: You must ensure that your key size is at least 2048 bits when you generate the key.</p>

Step	Action
7-7	Double-click the PuTTY icon. 
7-8	Use the following settings: <ul style="list-style-type: none"> • 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

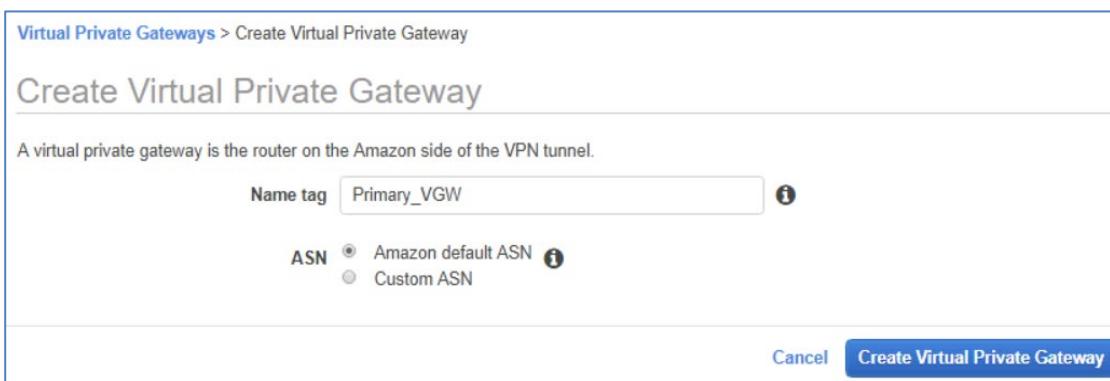
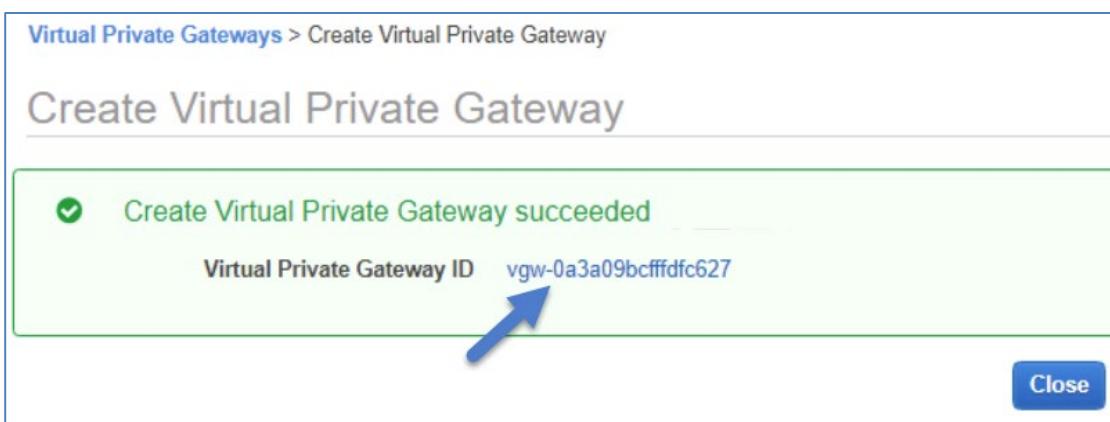
This exercise focuses on enabling you to do the following:

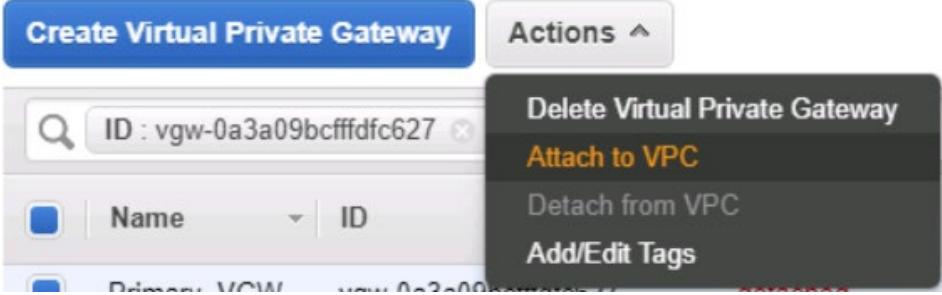
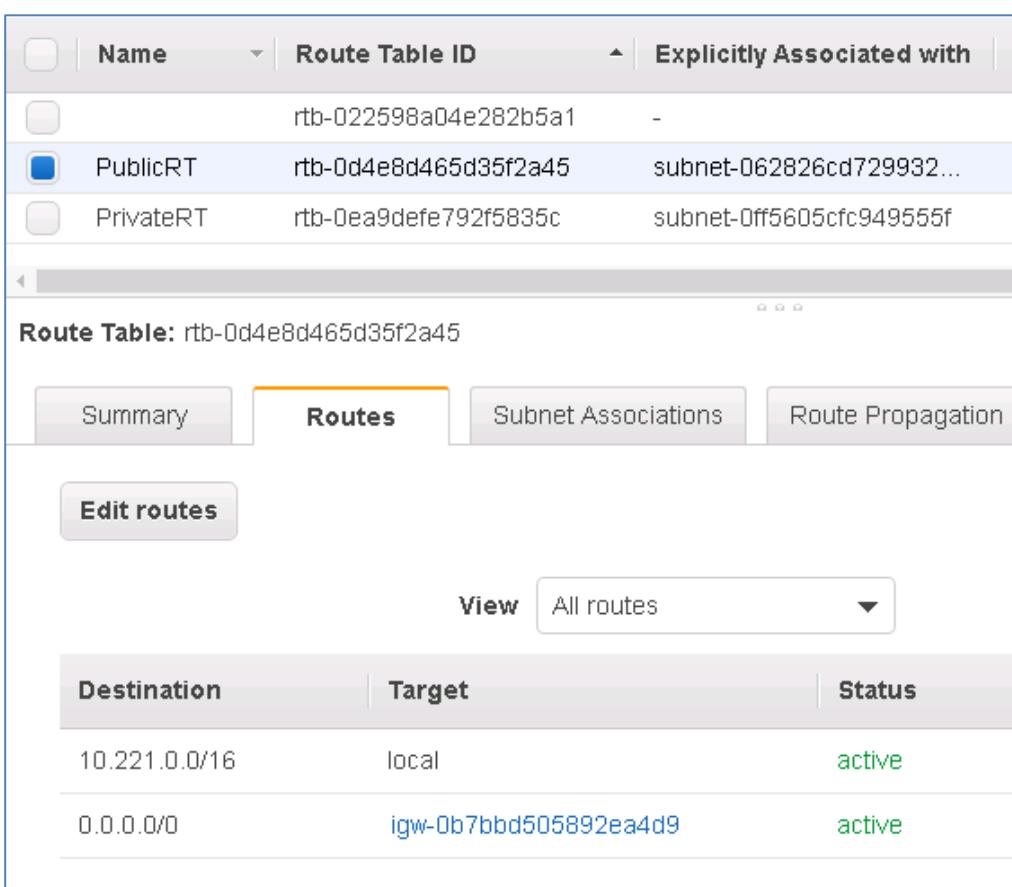
- Create a virtual private gateway for access from your VPC to the private network with the on-premises data center
- Create a customer gateway and establish a VPN IPsec connection to an on-premises data center
- Join an AWS virtual machine to the on-premises Active Directory service

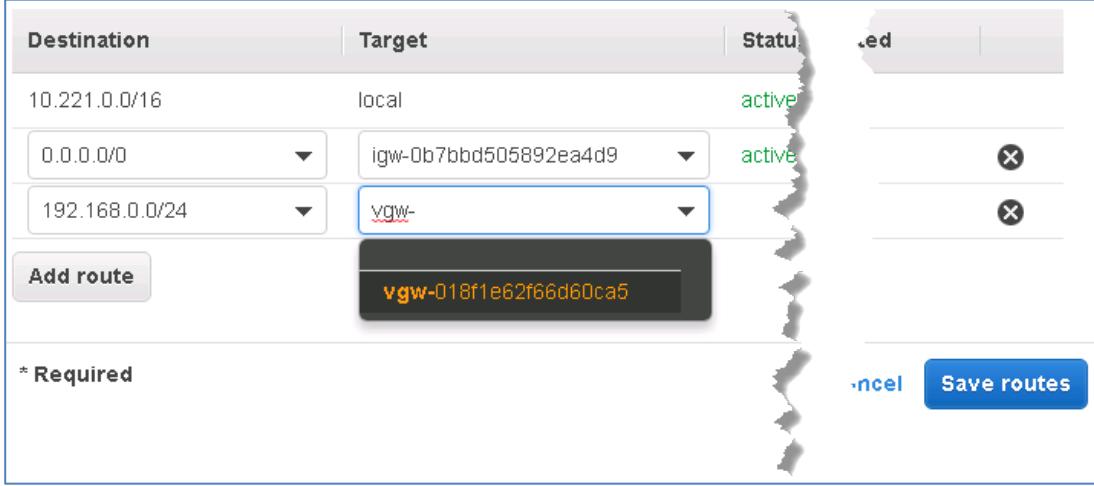
Task 1: Create a Virtual Private Gateway

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	<p>On the Create Virtual Private Gateway window, do the following:</p> <ol style="list-style-type: none"> Enter the name tag Primary_VGW. For the ASN, select Amazon default ASN. Click Create Virtual Private Gateway. 
1-5	<p>Click the Virtual Private Gateway ID.</p> 
1-6	<p>Verify that the Primary_VGW was created and is detached.</p> 

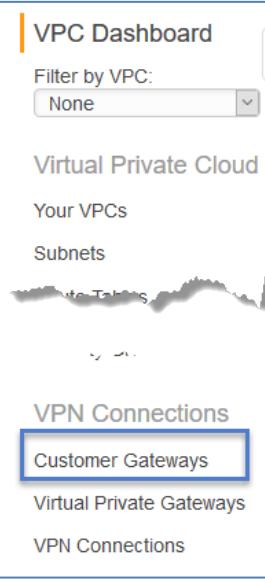
Step	Action
1-7	Select Primary_VGW , and then select Actions > Attach to VPC . 
1-8	In the Attach to VPC window, select PrimaryVPC , and then click Yes, Attach .
1-9	On the VPC Dashboard, select Route Tables , and then select PublicRT . 
1-10	Click the Routes tab, and then click Edit routes .
1-11	Click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

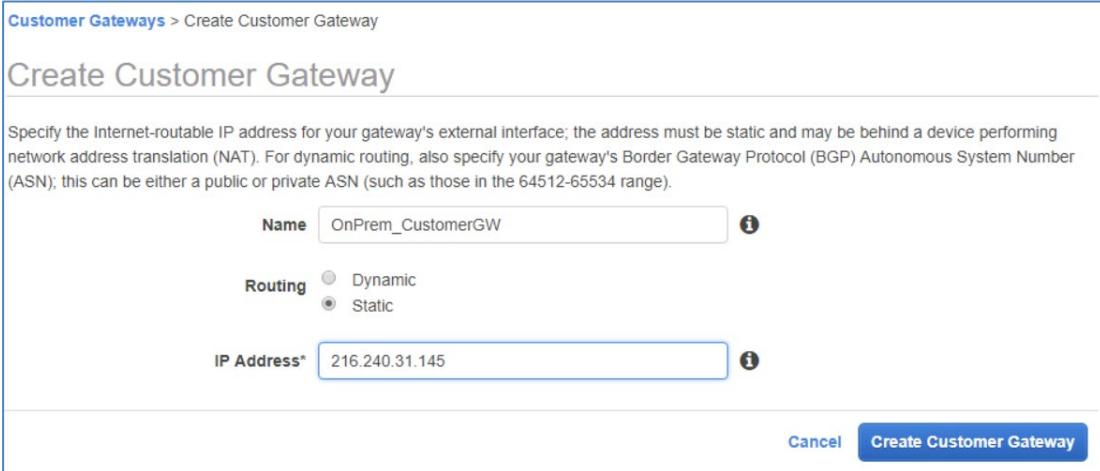
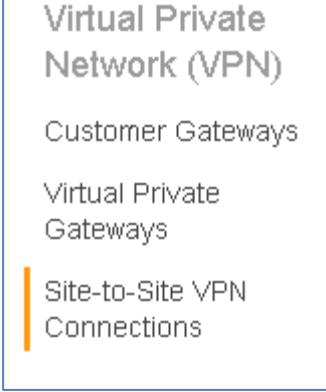
Step	Action
1-12	<p>Enter the following values:</p> <ul style="list-style-type: none"> Destination: 192.168.0.0/24 Target: Select Virtual Private Gateway, and then select your virtual private gateway ID. 
1-13	Click Save routes .
1-14	Click Close .
1-15	Click the Route Propagation tab.
1-16	Click Edit 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 .

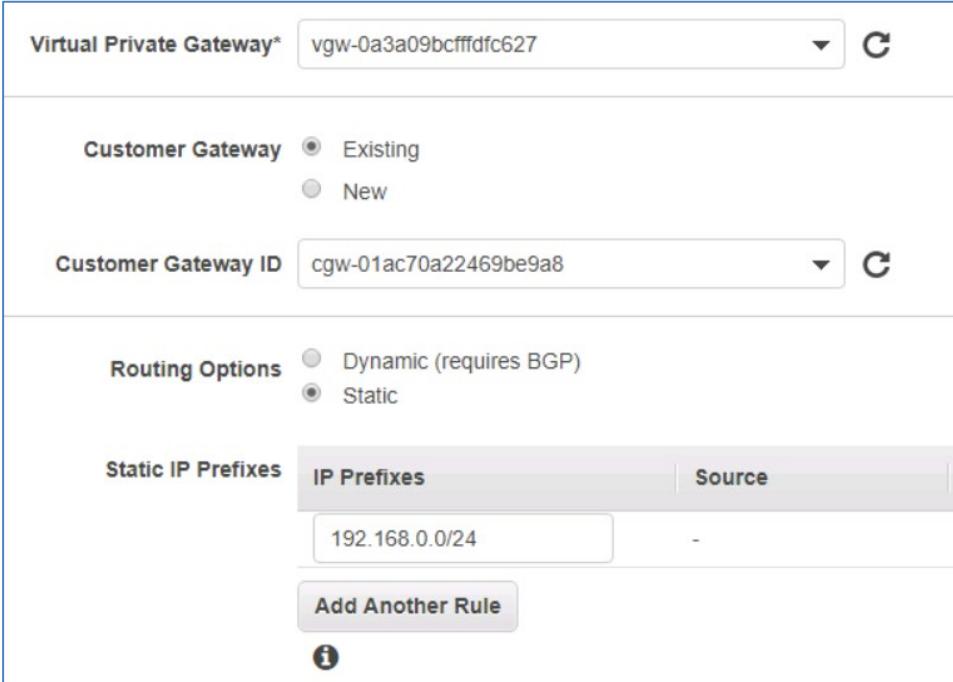
Step	Action
1-23	<p>In the rule row, use the following settings:</p> <ul style="list-style-type: none"> Type: All traffic Protocol: All Port Range: All Source: Custom 192.168.0.0/24 Description: Allow traffic from On-prem <p>Note: These settings enable your on-premises data center traffic to reach all AWS instances that use this security group.</p> 
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 <i>both</i> the private and public subnets!

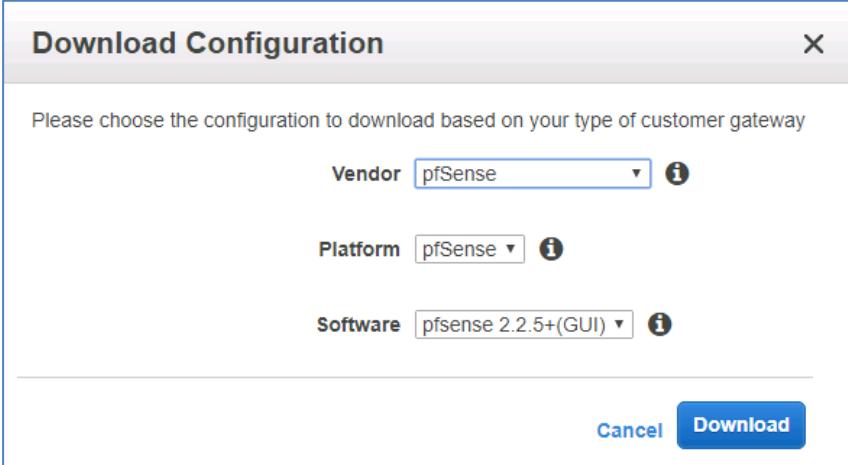
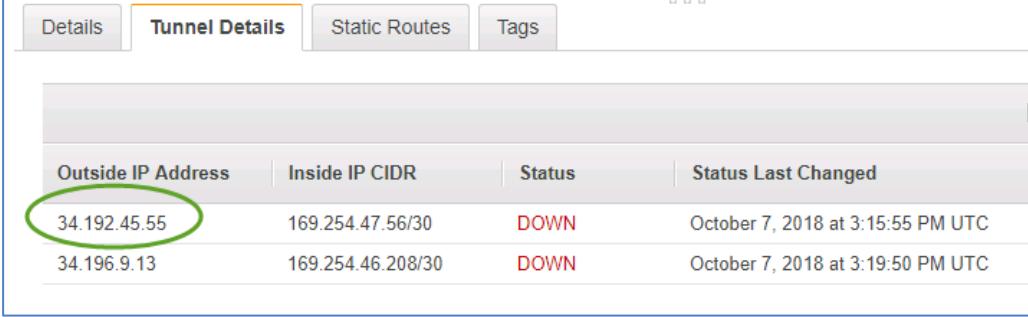
Task 2: Configure an AWS VPN and Customer Gateway

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 .

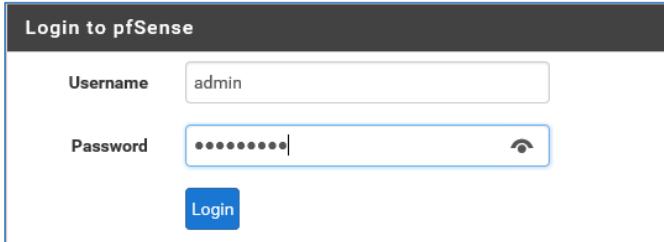
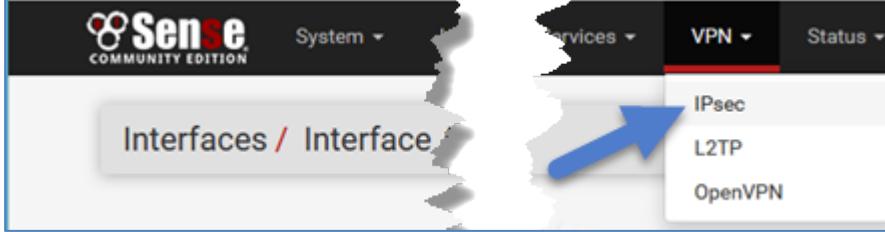
Step	Action
2-4	<p>In the Create Customer Gateway window, enter the following values:</p> <ul style="list-style-type: none"> • Name tag: OnPrem_CustomerGW • Routing: Static • IP address: <Customer gateway address that is provided by your instructor> (Your IP Address may differ from the image below) 
2-5	Click Create Customer Gateway .
2-6	Click Close .
2-7	<p>On the VPC Dashboard, click Site-to-Site VPN Connections.</p> 
2-8	Click Create VPN Connection .

Step	Action
2-9	<p>In the Create VPN Connection window, use the following settings:</p> <ul style="list-style-type: none"> • Name tag: To_OnPrem_VPN • Virtual Private Gateway: Select the virtual private gateway ID for your primary VPC. • Customer Gateway: <ul style="list-style-type: none"> ◦ 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	<p>Wait for the VPN state to become available.</p>  <p>Note: The process might take up to five minutes.</p>
2-13	Click Download Configuration .

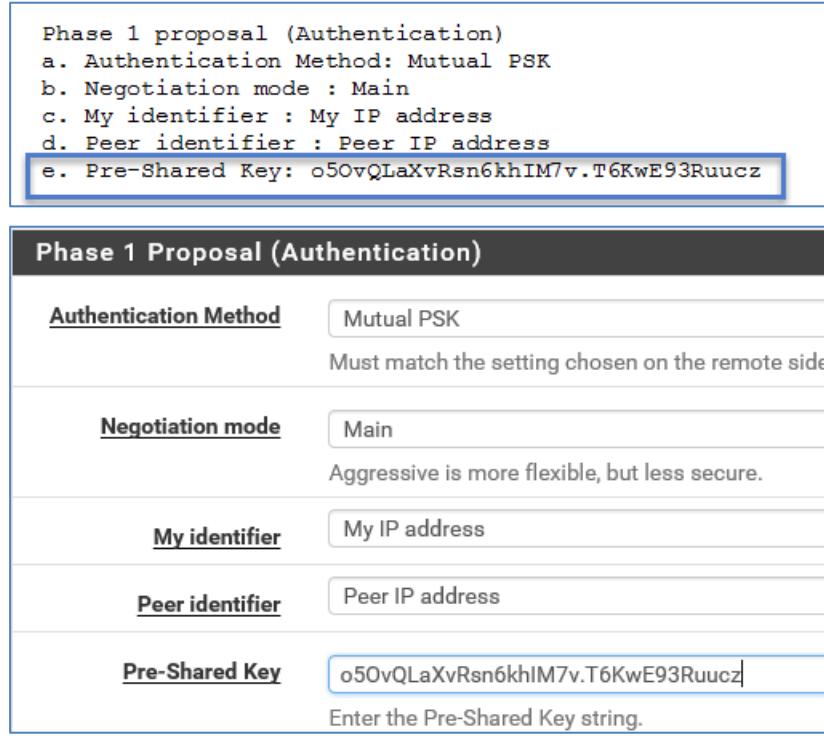
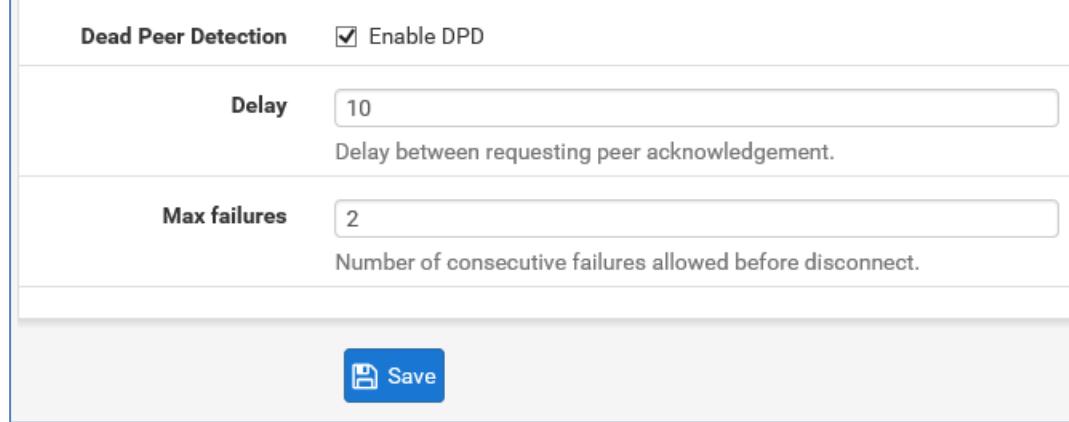
Step	Action												
2-14	<p>In the Download Configuration window, select the following values:</p> <ul style="list-style-type: none"> Vendor: pfSense Platform: pfSense Software: pfSense 2.2.5+ (GUI)  <p>(You are using pfSense in your on-premises environment as your secure gateway and router into the on-premises environment.)</p>												
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	<p>Record the IP address of the Outside IP Address of Tunnel 1: _____</p>  <table border="1"> <thead> <tr> <th>Outside IP Address</th> <th>Inside IP CIDR</th> <th>Status</th> <th>Status Last Changed</th> </tr> </thead> <tbody> <tr> <td>34.192.45.55</td> <td>169.254.47.56/30</td> <td>DOWN</td> <td>October 7, 2018 at 3:15:55 PM UTC</td> </tr> <tr> <td>34.196.9.13</td> <td>169.254.46.208/30</td> <td>DOWN</td> <td>October 7, 2018 at 3:19:50 PM UTC</td> </tr> </tbody> </table> <p>Although there are two tunnels for this course, you configure only one. In a production environment, you configure both tunnels for redundancy.</p>	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	34.192.45.55	169.254.47.56/30	DOWN	October 7, 2018 at 3:15:55 PM UTC	34.196.9.13	169.254.46.208/30	DOWN	October 7, 2018 at 3:19:50 PM UTC
Outside IP Address	Inside IP CIDR	Status	Status Last Changed										
34.192.45.55	169.254.47.56/30	DOWN	October 7, 2018 at 3:15:55 PM UTC										
34.196.9.13	169.254.46.208/30	DOWN	October 7, 2018 at 3:19:50 PM UTC										

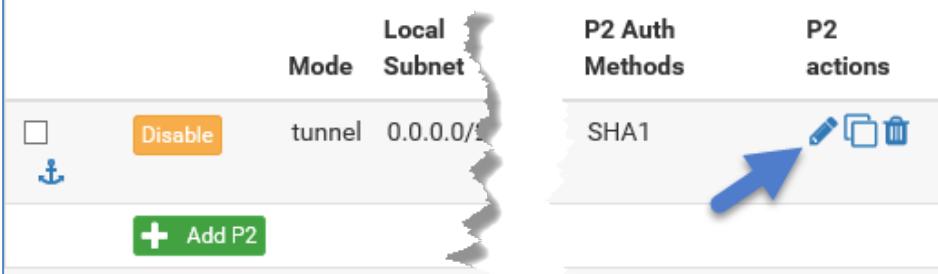
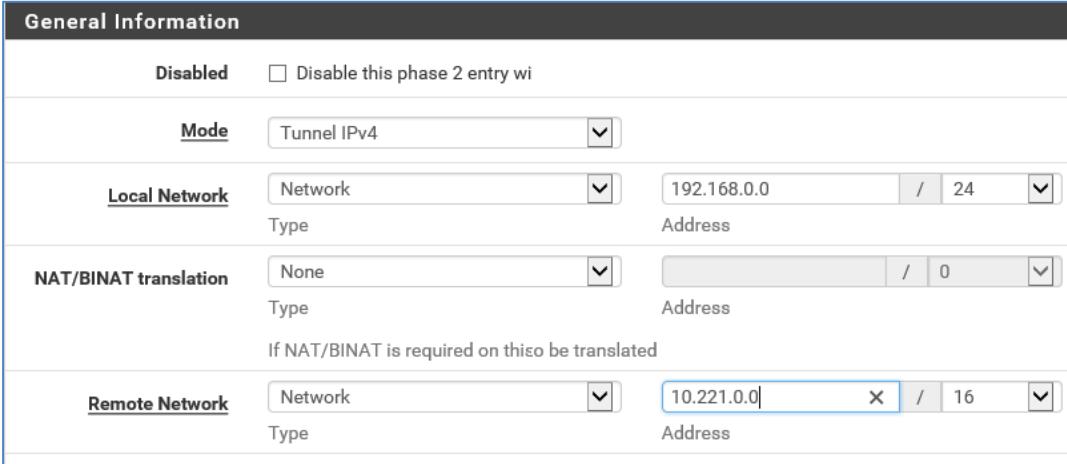
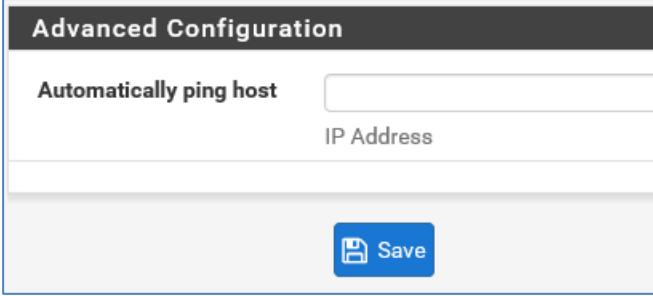
Task 3: Configure VPN IPsec Tunnels

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.

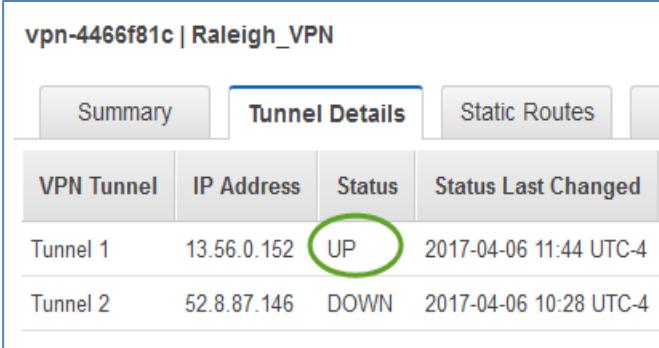
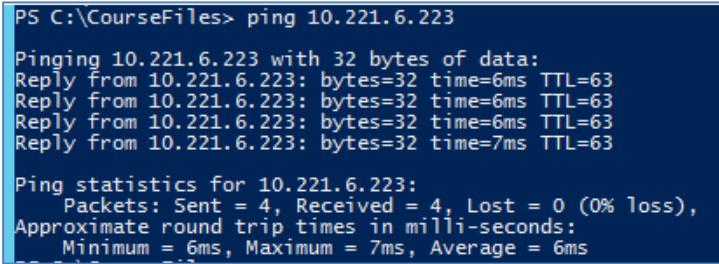
Step	Action
3-1	On your Windows Server jump host, double click the pfSense shortcut. 
3-2	If a security warning appears, click Advanced and then click Proceed to 192.168.0.1 (unsafe) .
3-3	Enter the following credentials: Username: admin Password: Netapp1! 
3-4	Click Login .
3-5	Select VPN > IPsec .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

Step	Action
3-7	<p>In the General Information section, replace the Remote Gateway value with the Tunnel 1 IP address that you recorded in Step 2-19.</p> <p>General Information</p> <p>Disabled <input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.</p> <p>Key Exchange version IKEv1 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 IKEv2 as responder.</p> <p>Internet Protocol IPv4 Select the Internet Protocol family.</p> <p>Interface LAN Select the interface for the local endpoint of this phase1 entry.</p> <p>Remote Gateway Enter the public IP address or host name of the remote gateway.</p> <p>Description AWS VPC Tunnel A description may be entered here for administrative reference (not parsed).</p>
3-8	Open the file vpn-xxxx.txt.

Step	Action
3-9	<p>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.</p> <pre> 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: o50vQLaXvRsn6khIM7v.T6KwE93Ruucz </pre> 
3-10	 <p>Be sure to copy the Pre-Shared Key value for Tunnel 1, not Tunnel 2. Both values exist in the vpn-xxxx.txt file.</p>
3-11	<p>Accept the default values for all the other settings, scroll to the bottom of the page, and then click Save.</p> 
3-12	<p>Click Apply Changes.</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #fff;"> <p>The IPsec tunnel configuration has been changed. The changes must be applied for them to take effect.</p> <div style="text-align: right; margin-top: -10px;"> ✓ Apply Changes </div> </div>

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: <ol style="list-style-type: none"> Replace the Local Network IP address with 192.168.0.0/24. 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 .
	

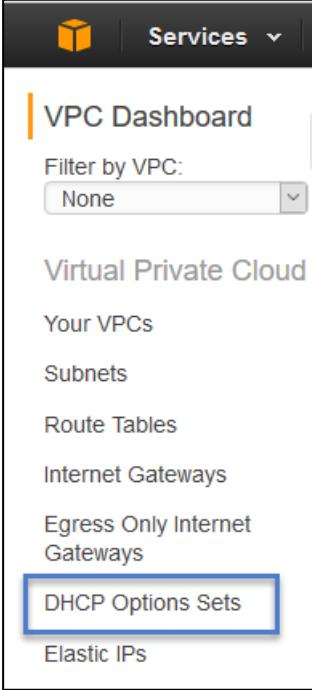
Step	Action
3-17	Click Apply Changes .
	<p>The IPsec tunnel configuration has been changed. The changes must be applied for them to take effect.</p> <div style="text-align: right; border: 1px solid green; padding: 2px;"> Apply Changes</div>
3-18	From the pfSense menu, select Status > IPsec .
	<p>The screenshot shows the pfSense Status menu with several options: Captive Portal, CARP (failover), Dashboard, Firewall Rules, Gateways, Interfaces, and IPsec. The IPsec option is highlighted with a blue box.</p>
3-19	For AWS VPC Tunnel, click Connect VPN .
	<p>The screenshot shows the IPsec Status page for the AWS VPC Tunnel. It lists the tunnel details: Local ID (192.168.0.2), Local IP (192.168.0.2), Remote ID (52.9.67.252), Remote IP (52.9.67.252), and Status (Disconnected). A green button labeled "Connect VPN" is visible.</p>
3-20	Verify that the session status is Established.
	<p>The screenshot shows the Status page for the AWS VPC Tunnel. It displays the session status as "ESTABLISHED" in green text, along with the time "61 seconds (00:01:01) ago". A red "Disconnect" button is also present.</p>

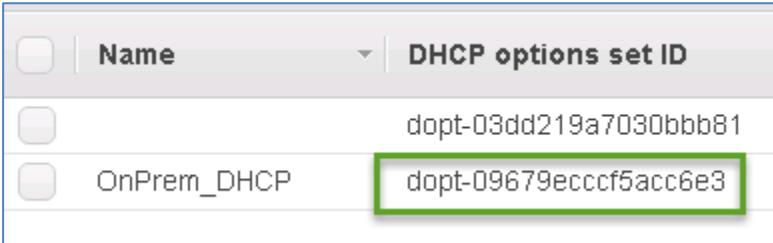
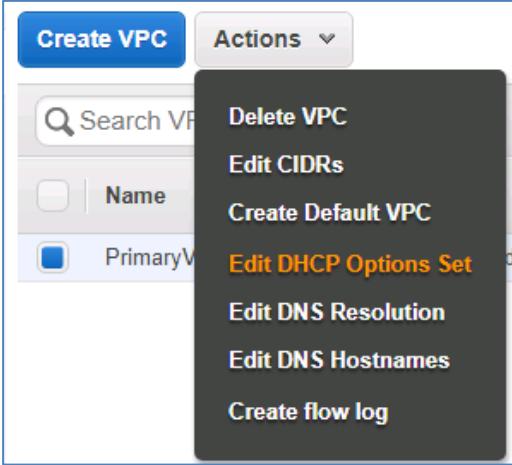
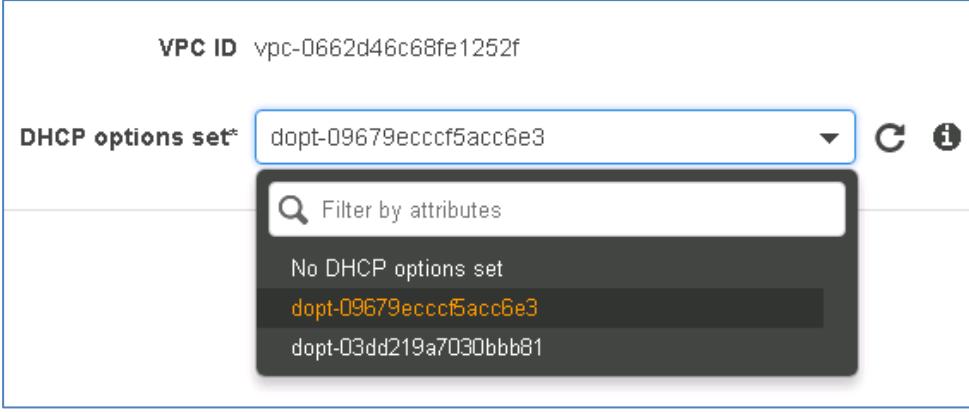
Step	Action
3-21	<p>Return to the AWS Console, select VPC > Site-to-Site VPN Connections, and then verify that the tunnel status is UP. Note: It might take up to 10 minutes for the Status to appear as UP.</p> 
3-22	<p> The following steps are used to verify that you have connectivity from your on-premises 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.</p>
3-23	<p>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.</p> 
3-24	<p>Instantiate a Remote Desktop Connection from the jump host by using the private IP address of the Win2k16_Public Amazon EC2 instance in AWS.</p> <p>Note: You might need to decrypt the password again by using the MyAWSKey.pem file</p> 

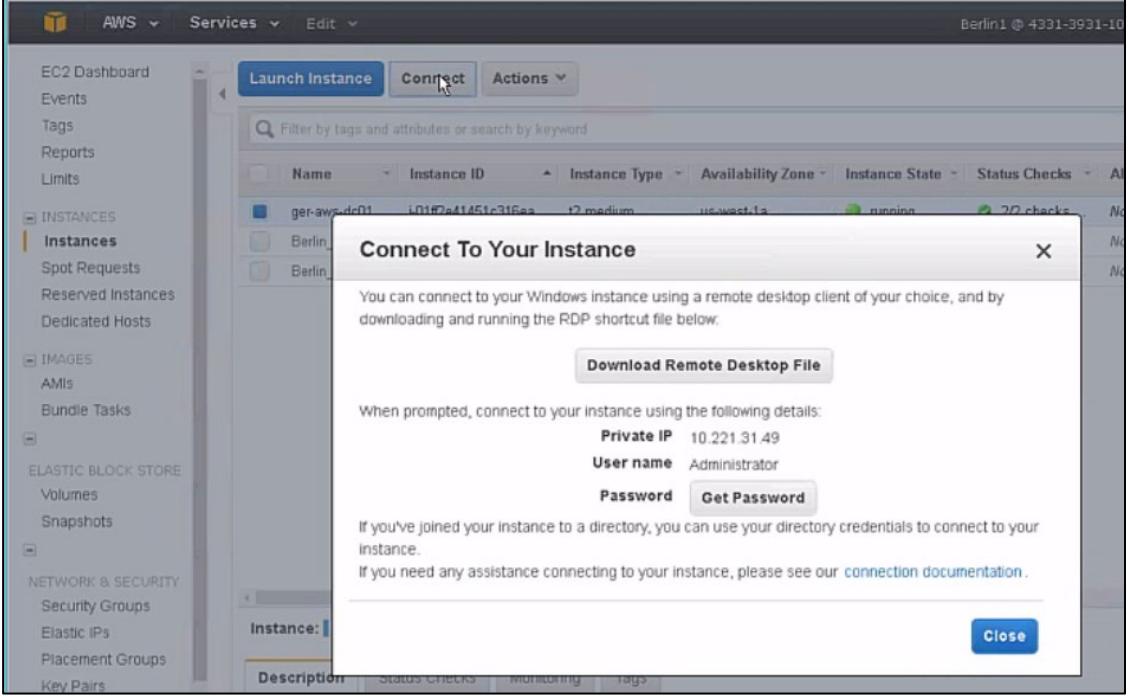
Step	Action
3-25	<p>Open a PowerShell window from the Win2k16_Public desktop, and then verify that you can ping the domain controller:</p> <pre>C:>ping 192.168.0.253 PS C:\Users\Administrator> ping 192.168.0.253 Pinging 192.168.0.253 with 32 bytes of data: Reply from 192.168.0.253: bytes=32 time=9ms TTL=127 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</pre>

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: <ul style="list-style-type: none">Name tag: OnPrem_DHCPDomain name: demo.netapp.comDomain name servers: 192.168.0.253NTP servers: 192.168.0.253NetBIOS name servers: Leave blank.NetBIOS node type: Leave blank.
4-6	Click Create DHCP options set .
4-7	Click Close .

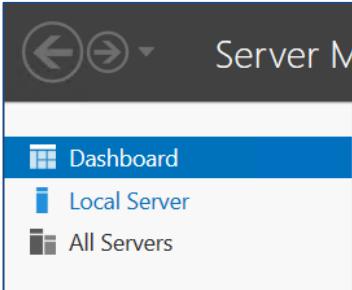
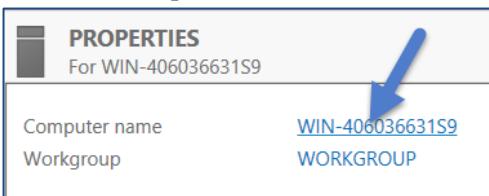
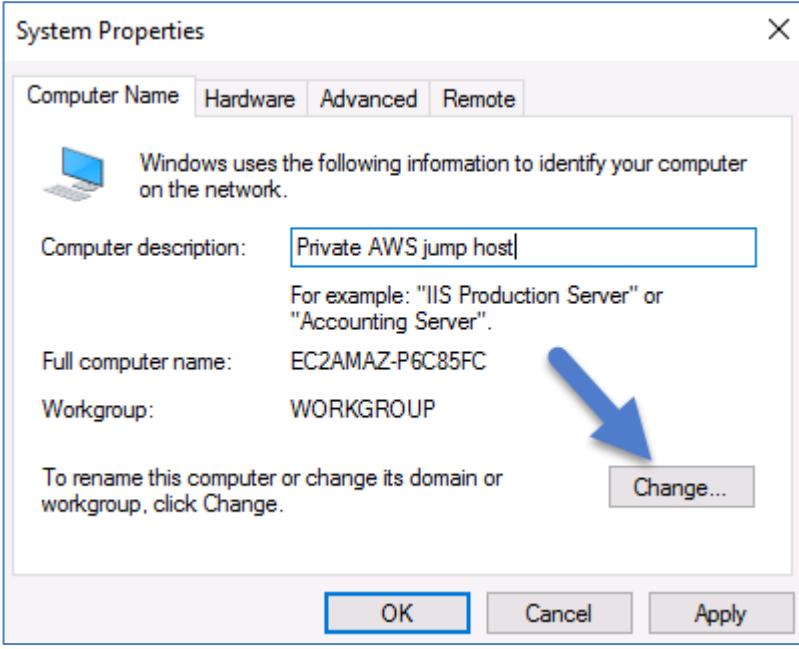
Step	Action
4-8	Record the DHCP options set ID for the OnPrem_DHCP.
	
4-9	On the VPC Dashboard, click Your VPCs .
4-10	Select the PrimaryVPC checkbox.
4-11	Select Actions > Edit DHCP Options Set .
	
4-12	In the Edit DHCP Options Set window, select the DHCP options set ID for the OnPrem_DHCP, and then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

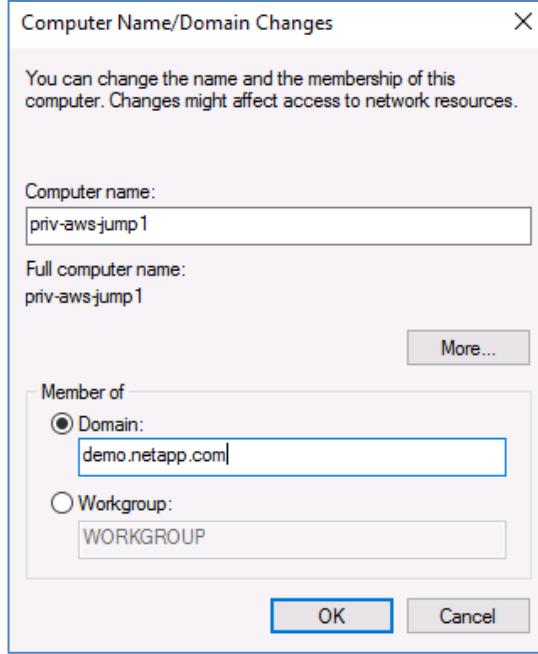
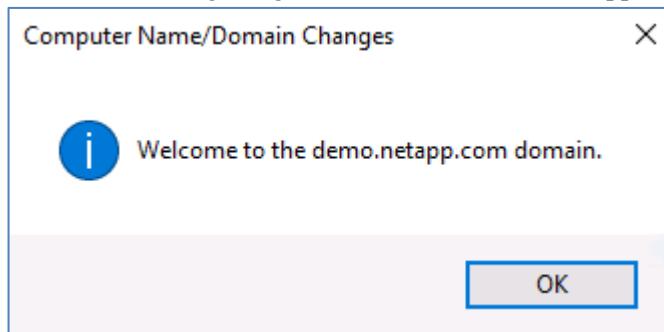
Step	Action
4-14	<p>Verify that you see OnPrem_DHCP as the option set for PrimaryVPC.</p> 
4-15	<p>Create an Amazon EC2 for Windows Server instance (Microsoft Windows Server 2016) in the private subnet by using the following key data:</p> <ul style="list-style-type: none"> AMI: Microsoft Windows Server 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: <ol style="list-style-type: none"> Name: SGPrivateWindowsInstances Rule: allow Remote Desktop Protocol (RDP) from within the VPC (10.221.0.0/16) Rule: allow all traffic from 192.168.0.0/24 On launch choose key pair: MyAWSKey <p>Note: This Windows Server is now assigned the DNS servers in the on-premises data center.</p>
4-16	<p>After the instance finishes booting, click the Connect button to log in to the instance.</p> 

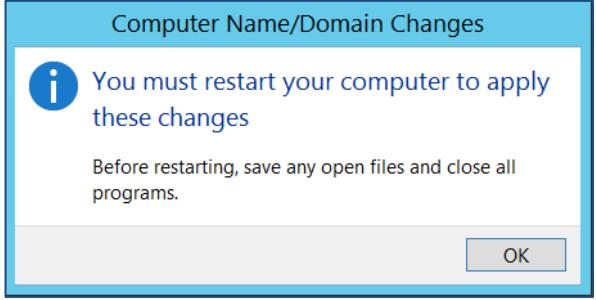
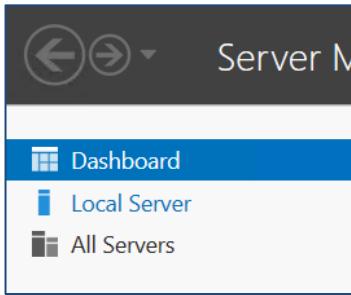
Step	Action
4-17	<p>In the Connect To Your Instance window, use the following settings:</p> <ol style="list-style-type: none"> Click Get Password. Select the key file in your CourseFiles folder. Click Decrypt password. Copy the private IP, user account name and password to a text file that is named Win2k16_Private_Login.txt.
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	<p>From the private Window Server Amazon EC2 instance, open a PowerShell (or CLI) window, and then ping the DNS servers.</p> <pre>C:> ping 192.168.0.253 Administrator: Windows PowerShell 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=10ms 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 = 10ms, Average = 9ms PS C:\Users\Administrator></pre>

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	<p>Select the Domain option button, and then enter demo.netapp.com.</p> 
5-7	Click OK .
5-8	<p>In the Windows Security window, enter the following values:</p> <ul style="list-style-type: none"> User name: Demo\Administrator Password: Netapp1!
5-9	Click OK .
5-10	<p>Verify that a Welcome to the domain message appears.</p> <p>Note: The message might take several minutes to appear.</p> 
5-11	Click OK .

Step	Action
5-12	<p>When the “You must restart your computer to apply these changes” message appears, click OK.</p> 
5-13	<p>In the System Properties window, click Close.</p>
5-14	<p>Click Restart Now.</p>
5-15	<p>After the RDP session closes, wait a few minutes for the Private_W2K16 instance to restart.</p>
5-16	<p>Open a Remote Desktop Connection from your jump host to this Amazon EC2 instance by using the following credentials:</p> <ul style="list-style-type: none"> • User name: Demo\Administrator • Password: Netapp1!
5-17	 <p>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.</p>
5-18	<p>Open Server Manager by clicking the icon to the right of the Start icon.</p> 
5-19	<p>On the Dashboard, click Local Server.</p> 
5-20	<p>Verify that the computer is a member of the demo.netapp.com domain.</p> 

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.

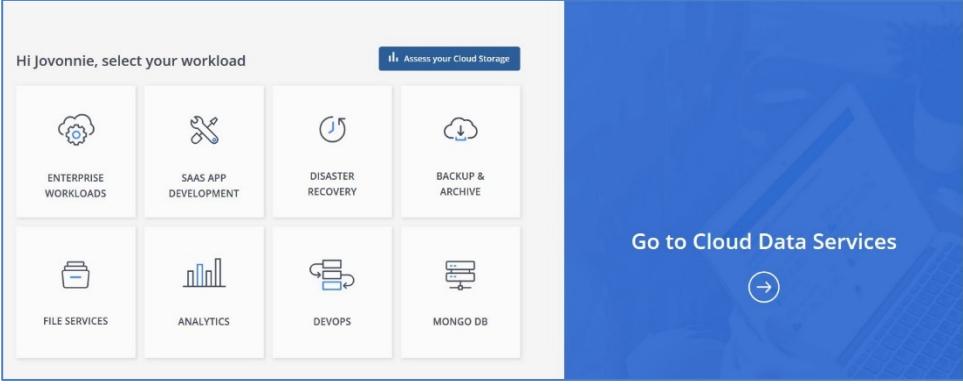
Objectives

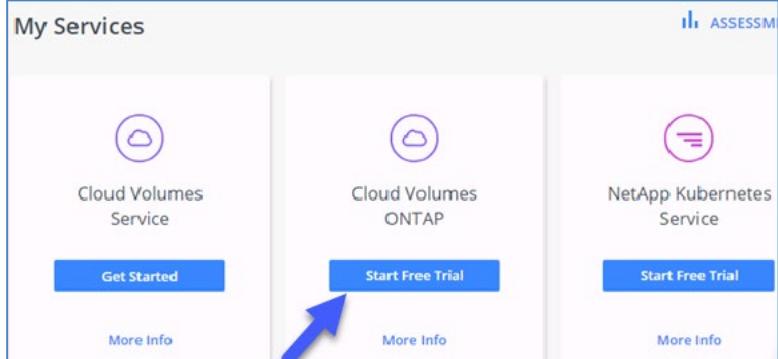
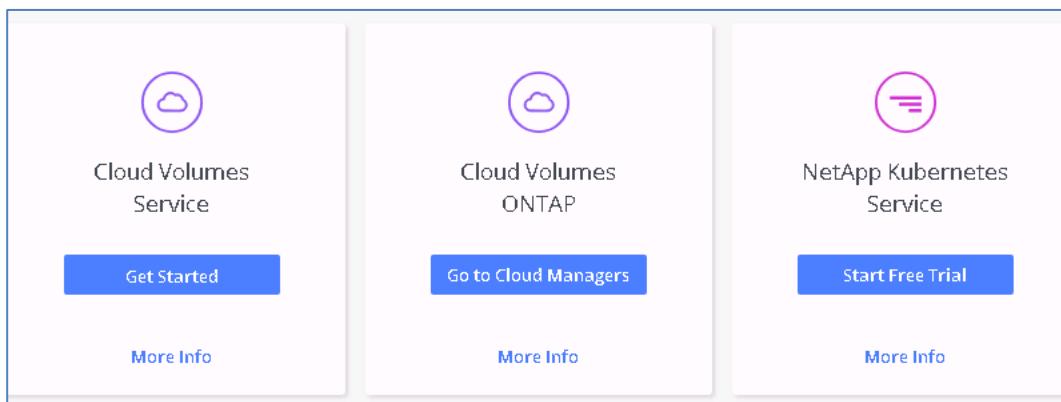
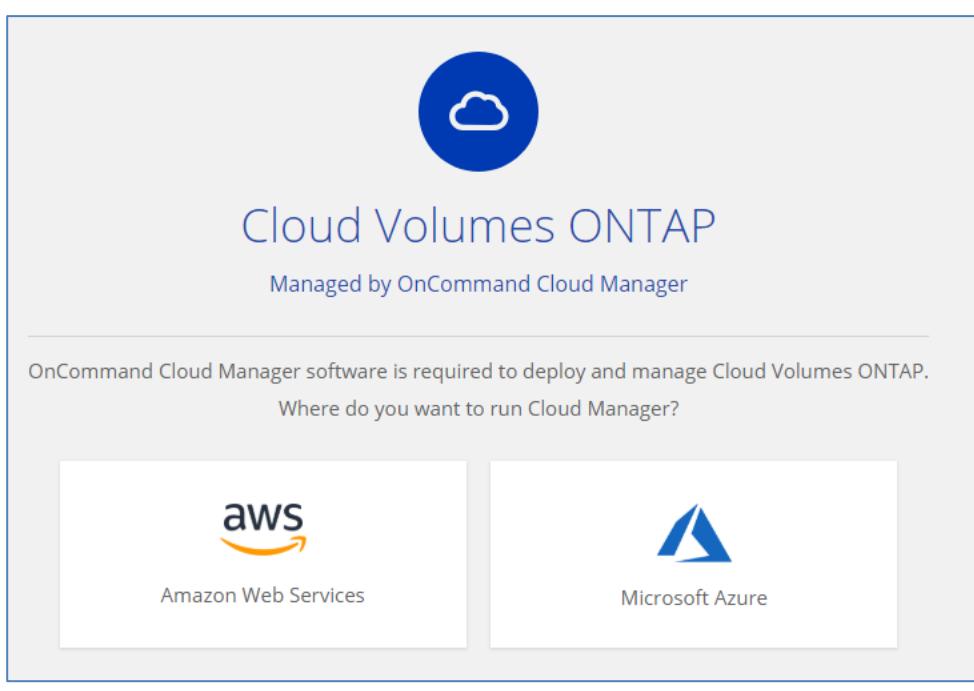
This exercise focuses on enabling you to do the following:

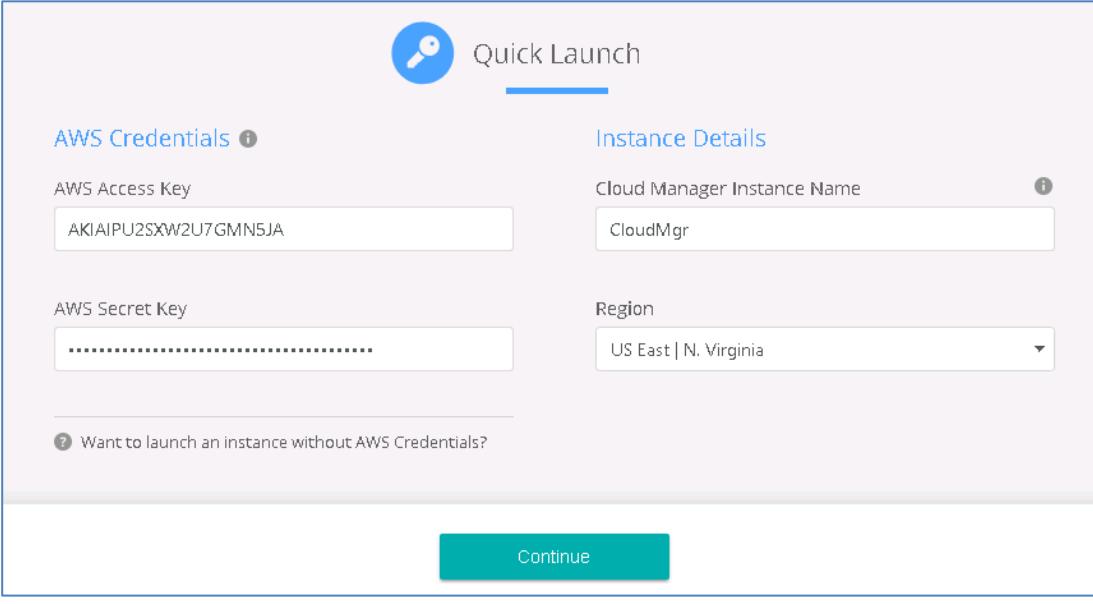
- Deploy Cloud Manager
- Configure Amazon Web Services (AWS) Identity and Access Management (IAM) permissions for Cloud Manager
- Deploy Cloud Volumes ONTAP instances by using Cloud Manager
- Create volumes and prepare the CIFS protocol for a Cloud Volumes ONTAP instance

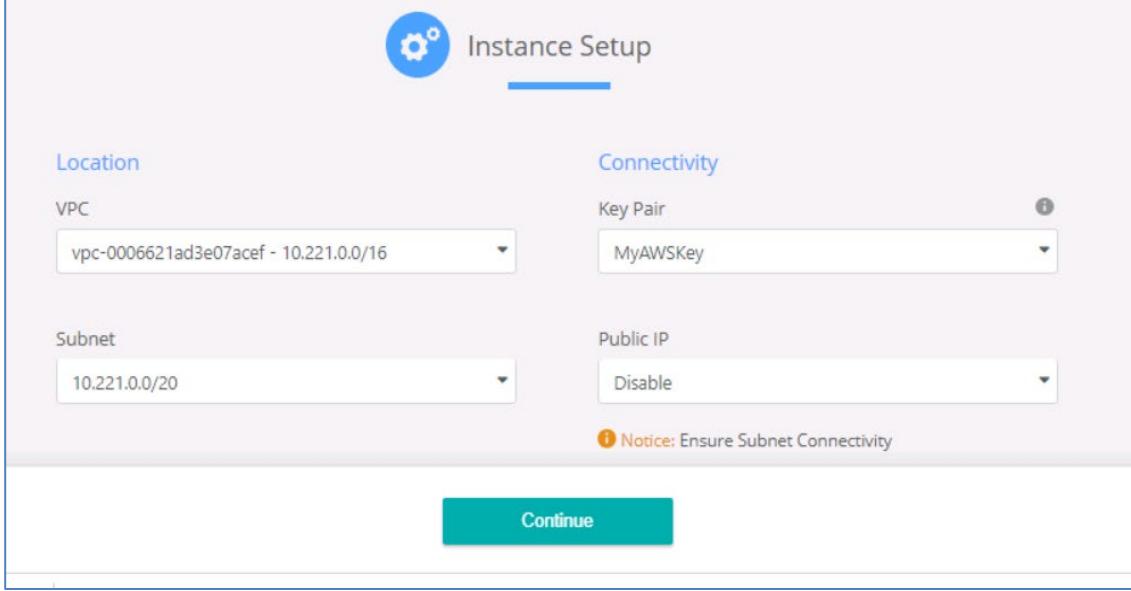
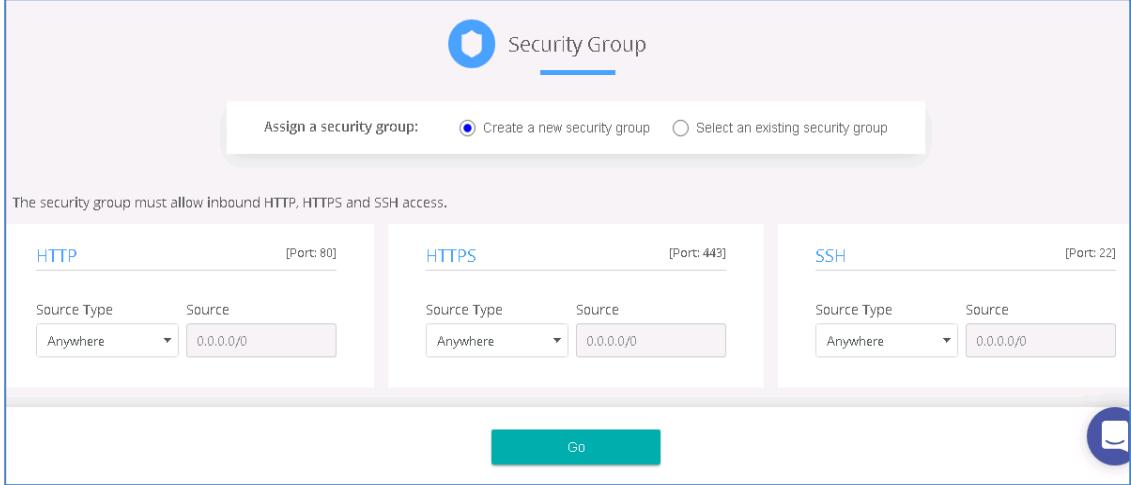
Task 1: Deploy and Configure Cloud Manager

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

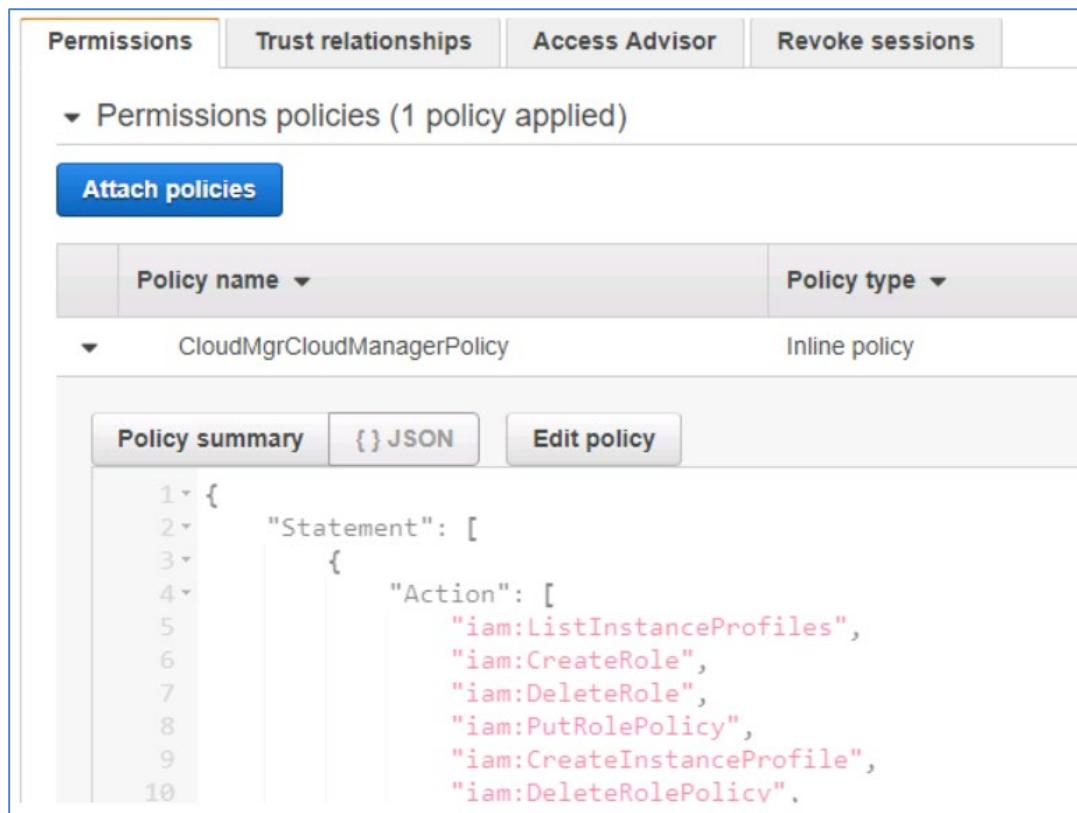
Step	Action
1-1	Log in to the on-premises jump host (Windows Server).
1-2	Navigate to cloud.netapp.com . (Note it runs best in Chrome so you might want to download Chrome to your Windows Server.)
1-3	Click LOGIN .
1-4	On the LOGIN page, enter the following: <ul style="list-style-type: none">• Email: <<i>your user name in the awslogin.txt file</i>>@demo.netapp.com• Password: Netapp1!
1-5	Click LOGIN .
1-6	On the right of the window, click Go to Cloud Data Services . 

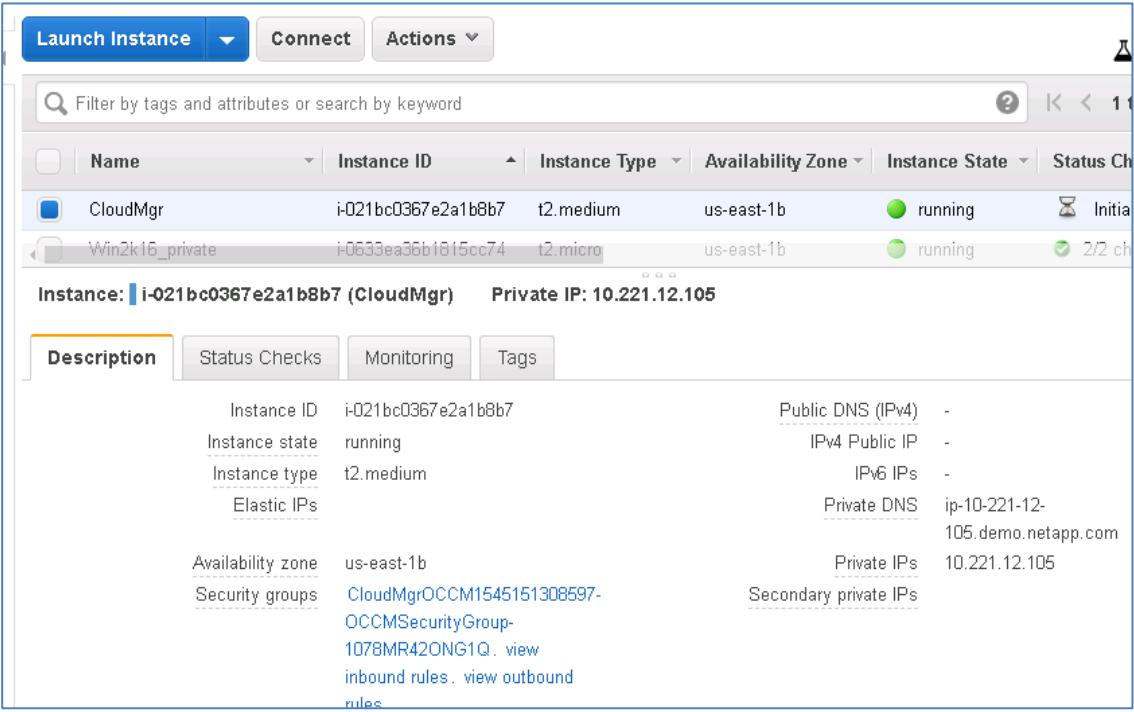
Step	Action
1-7	<p>Click the Start Free Trial button under Cloud Volumes ONTAP</p> 
1-8	<p>If you have previously created Cloud Manager from Cloud Central, you see Go to Cloud Managers instead of Create Cloud Manager.</p> 
1-9	<p>Click the Amazon Web Services tile to deploy Cloud Manager in AWS.</p> 

Step	Action
1-10	<p>Complete the Quick Launch form by entering the appropriate information in the AWS Credentials and Instance Details fields:</p> <ul style="list-style-type: none"> • AWS Access Key ID: <found in awslogin.txt file on the desktop of your jump host> • AWS Secret Access Key: <found in awslogin.txt file on the desktop of your jump host> • Cloud Manager Instance Name: CloudMgr • Region: Select US East N. Virginia  <p>The screenshot shows the 'Quick Launch' interface. It has two main sections: 'AWS Credentials' and 'Instance Details'. In the 'AWS Credentials' section, there is a 'AWS Access Key' field containing 'AKIAIPU2SXW2U7GMNSJA' and an 'AWS Secret Key' field with several dots. In the 'Instance Details' section, there is a 'Cloud Manager Instance Name' field containing 'CloudMgr' and a 'Region' dropdown menu set to 'US East N. Virginia'. At the bottom left, there is a note: 'Want to launch an instance without AWS Credentials?' followed by a question mark icon. A large teal 'Continue' button is at the bottom right.</p>
1-11	Click Continue .

Step	Action
1-12	<p>In the Instance Setup page, select the following elements from the lists:</p> <ul style="list-style-type: none"> • VPC: Select PrimaryVPC. • Key Pair: Select MyAWSKey. • Subnet: Select the PrivateSubnet. • Public IP: Select Disable. • Click Continue. 
1-13	<p>In the Security Group page, configure the Cloud Manager security group.</p> <ul style="list-style-type: none"> • 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 .

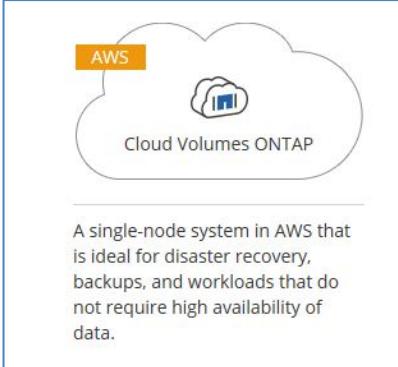
Step	Action
1-15	<p>Verify that Cloud Manager starts to deploy. Do not wait for Cloud Manager to deploy, go on to the next step in this guide.</p>
1-16	 Cloud Manager automatically deploys in about seven minutes. Your web browser directs you to the Cloud Manager interface in which you can deploy Cloud 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.

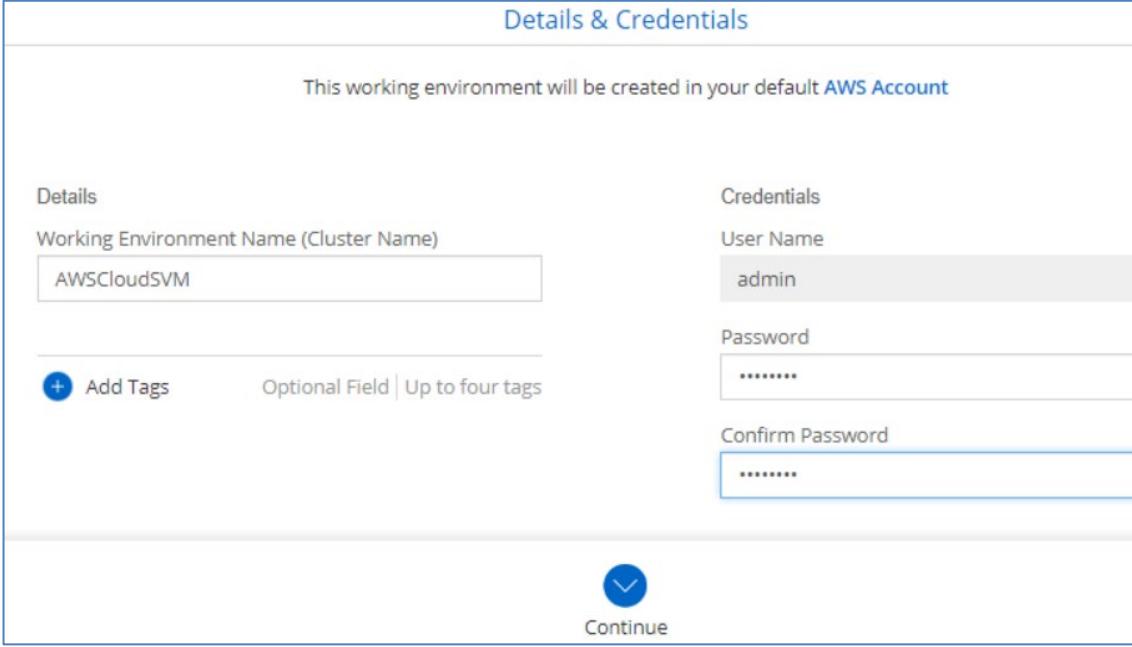
Step	Action
1-20	<p>Expand the policy and then click the JSON tab.</p>  <pre> 1 { 2 "Statement": [3 { 4 "Action": [5 "iam>ListInstanceProfiles", 6 "iam>CreateRole", 7 "iam>DeleteRole", 8 "iam>PutRolePolicy", 9 "iam>CreateInstanceProfile", 10 "iam>DeleteRolePolicy" 11] 12 } 13 } 14 }</pre>
1-21	 <p>These 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.</p>

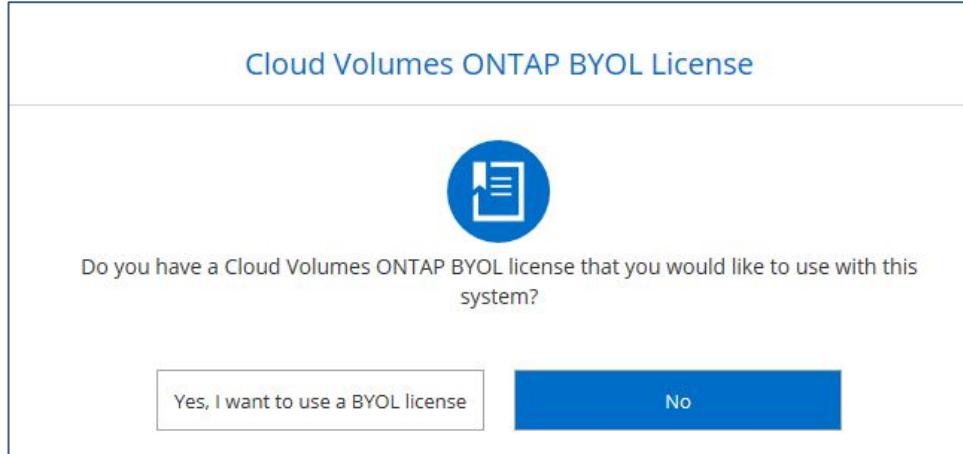
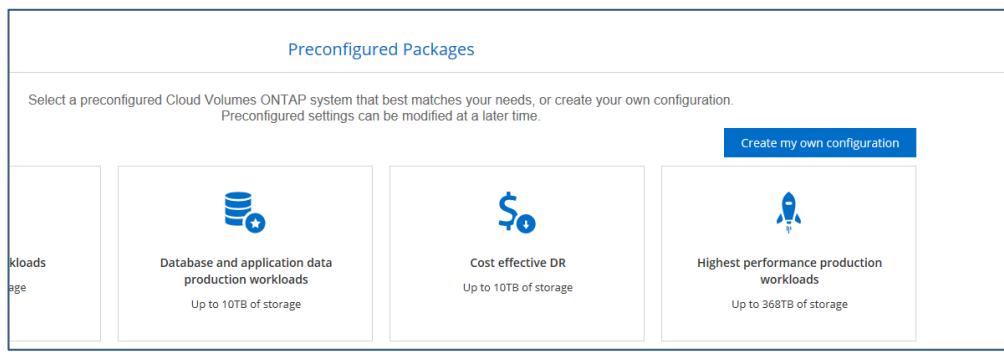
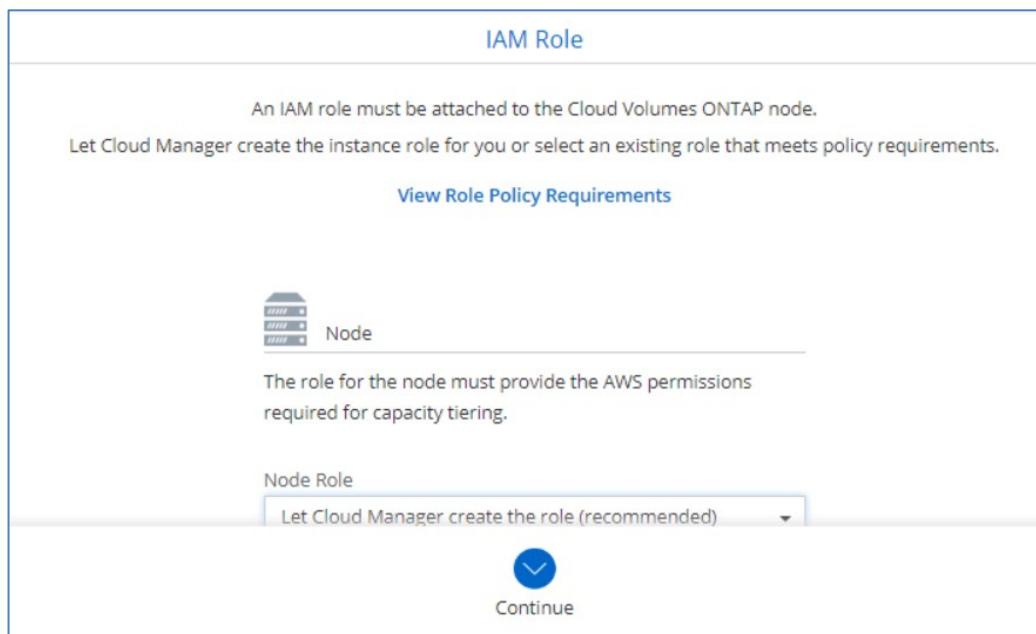
Step	Action																																										
1-22	<p>Select Services > EC2 and note that an Amazon Elastic Compute Cloud (Amazon EC2) instance with the name CloudMgr is deployed, with an instance type of t2.medium. It is deployed in the private subnet and is associated with the security group that you configured in the Cloud Manager wizard.</p>  <p>The screenshot shows the AWS EC2 Instances page. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below is a search bar and a table header with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status. Two instances are listed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Instance ID</th> <th>Instance Type</th> <th>Availability Zone</th> <th>Instance State</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>CloudMgr</td> <td>i-021bc0367e2a1b8b7</td> <td>t2.medium</td> <td>us-east-1b</td> <td>running</td> <td>Initial</td> </tr> <tr> <td>Win2k16_private</td> <td>i-0633ea36b1815cc74</td> <td>t2.micro</td> <td>us-east-1b</td> <td>running</td> <td>2/2 ch</td> </tr> </tbody> </table> <p>Below the table, it says 'Instance: i-021bc0367e2a1b8b7 (CloudMgr) Private IP: 10.221.12.105'. A tab bar at the bottom includes 'Description' (selected), Status Checks, Monitoring, and Tags. Under 'Description', detailed information is shown:</p> <table border="1"> <tbody> <tr> <td>Instance ID</td> <td>i-021bc0367e2a1b8b7</td> <td>Public DNS (IPv4)</td> <td>-</td> </tr> <tr> <td>Instance state</td> <td>running</td> <td>IPv4 Public IP</td> <td>-</td> </tr> <tr> <td>Instance type</td> <td>t2.medium</td> <td>IPv6 IPs</td> <td>-</td> </tr> <tr> <td>Elastic IPs</td> <td></td> <td>Private DNS</td> <td>ip-10-221-12-105.demo.netapp.com</td> </tr> <tr> <td>Availability zone</td> <td>us-east-1b</td> <td>Private IPs</td> <td>10.221.12.105</td> </tr> <tr> <td>Security groups</td> <td>CloudMgrOCCM1545151308597-OCCMSecurityGroup-1078MR42ONG1Q, view inbound rules, view outbound rules</td> <td>Secondary private IPs</td> <td></td> </tr> </tbody> </table>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status	CloudMgr	i-021bc0367e2a1b8b7	t2.medium	us-east-1b	running	Initial	Win2k16_private	i-0633ea36b1815cc74	t2.micro	us-east-1b	running	2/2 ch	Instance ID	i-021bc0367e2a1b8b7	Public DNS (IPv4)	-	Instance state	running	IPv4 Public IP	-	Instance type	t2.medium	IPv6 IPs	-	Elastic IPs		Private DNS	ip-10-221-12-105.demo.netapp.com	Availability zone	us-east-1b	Private IPs	10.221.12.105	Security groups	CloudMgrOCCM1545151308597-OCCMSecurityGroup-1078MR42ONG1Q, view inbound rules, view outbound rules	Secondary private IPs	
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status																																						
CloudMgr	i-021bc0367e2a1b8b7	t2.medium	us-east-1b	running	Initial																																						
Win2k16_private	i-0633ea36b1815cc74	t2.micro	us-east-1b	running	2/2 ch																																						
Instance ID	i-021bc0367e2a1b8b7	Public DNS (IPv4)	-																																								
Instance state	running	IPv4 Public IP	-																																								
Instance type	t2.medium	IPv6 IPs	-																																								
Elastic IPs		Private DNS	ip-10-221-12-105.demo.netapp.com																																								
Availability zone	us-east-1b	Private IPs	10.221.12.105																																								
Security groups	CloudMgrOCCM1545151308597-OCCMSecurityGroup-1078MR42ONG1Q, view inbound rules, view outbound rules	Secondary private IPs																																									
1-23	Return to Cloud Central and wait for Cloud Manager to finish deploying.																																										

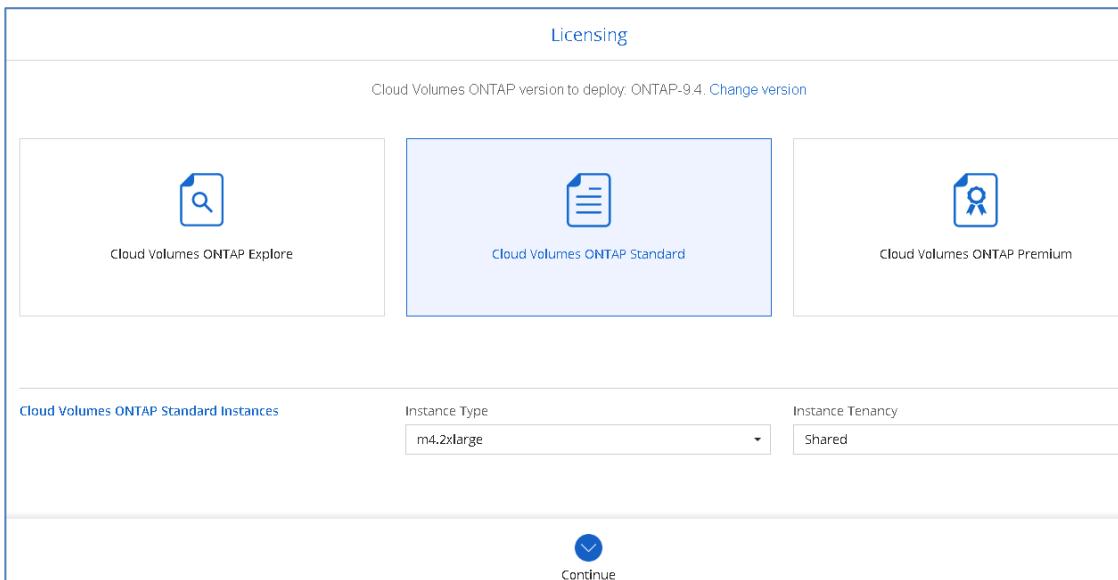
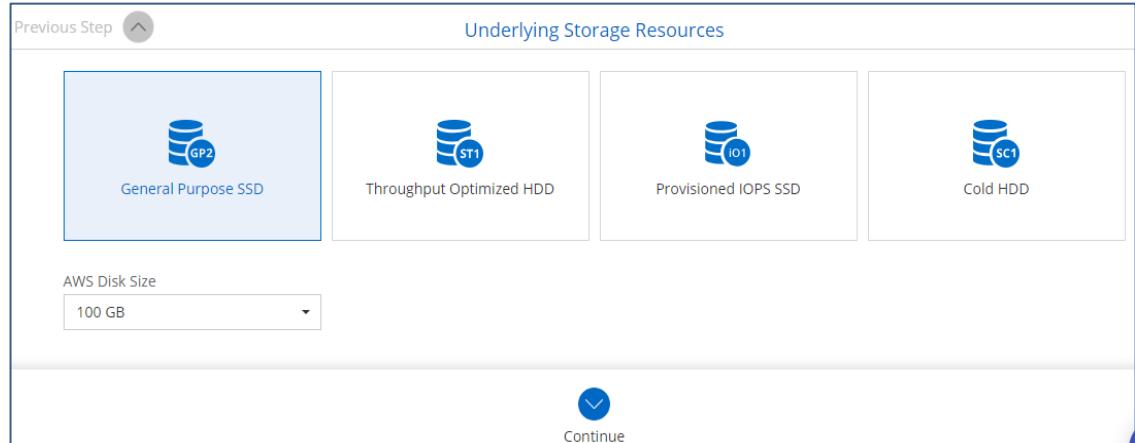
Task 2: Deploy Cloud Volumes ONTAP

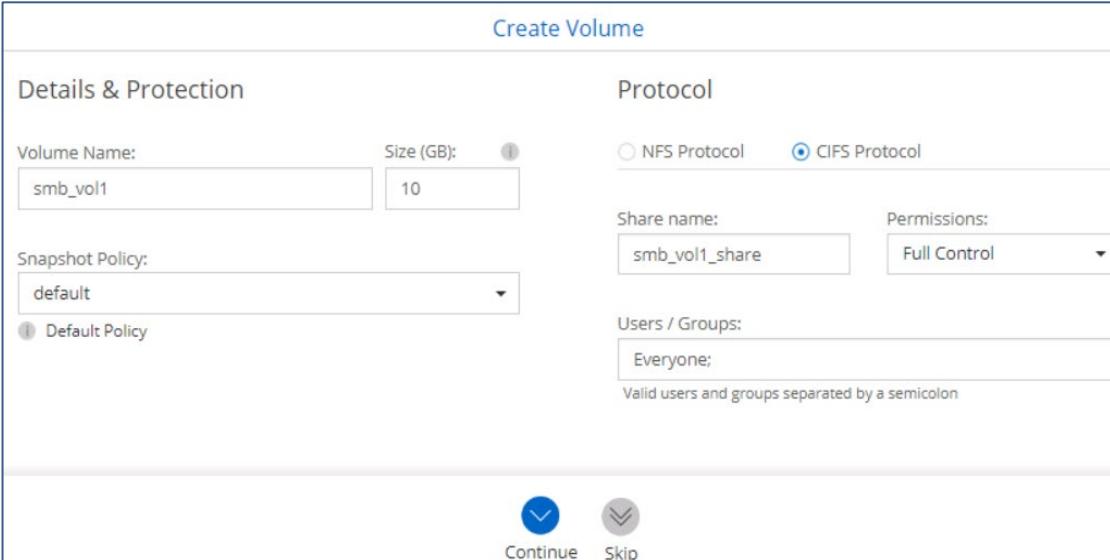
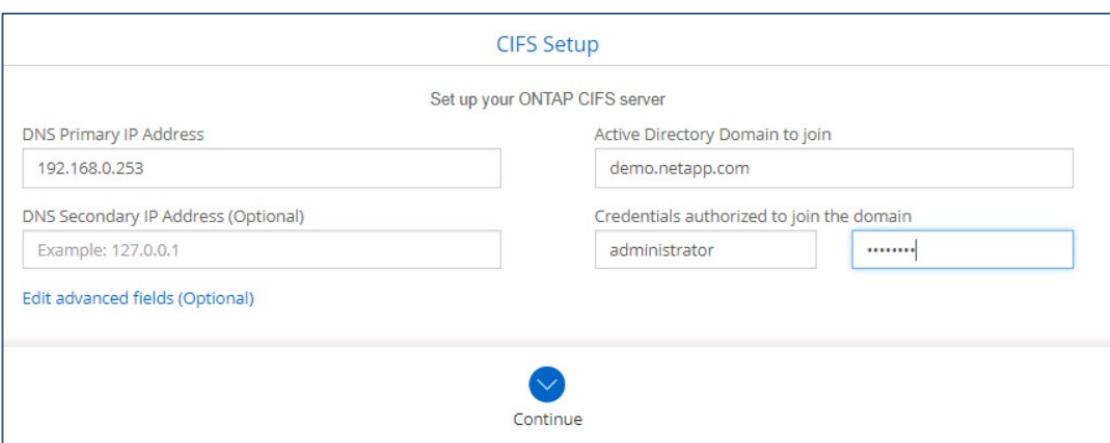
In this task, you deploy your first Cloud Volumes ONTAP instance.

Step	Action
2-1	<p>In Cloud Manager, click Create.</p> 
2-2	<p>Select Cloud Volumes ONTAP.</p>  <p>A single-node system in AWS that is ideal for disaster recovery, backups, and workloads that do not require high availability of data.</p>
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	<p>On the Details & Credentials page, enter the following values:</p> <ul style="list-style-type: none"> Working Environment Name: AWSCloudSVM Password: Netapp1! Confirm Password: Netapp1! 
2-5	Click Continue .
2-6	<p>On the Location page, select the following values:</p> <ul style="list-style-type: none"> 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	<p>On the Data Encryption page, click None.</p> 
2-9	Click Continue .

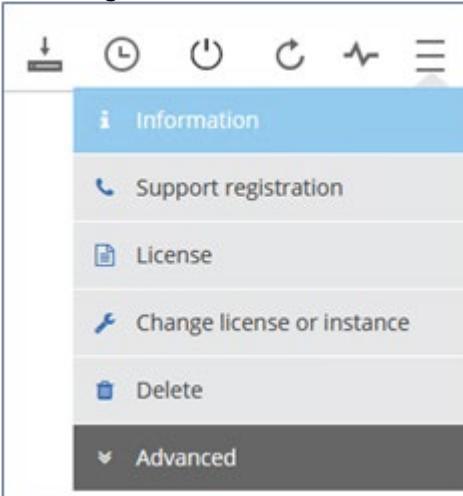
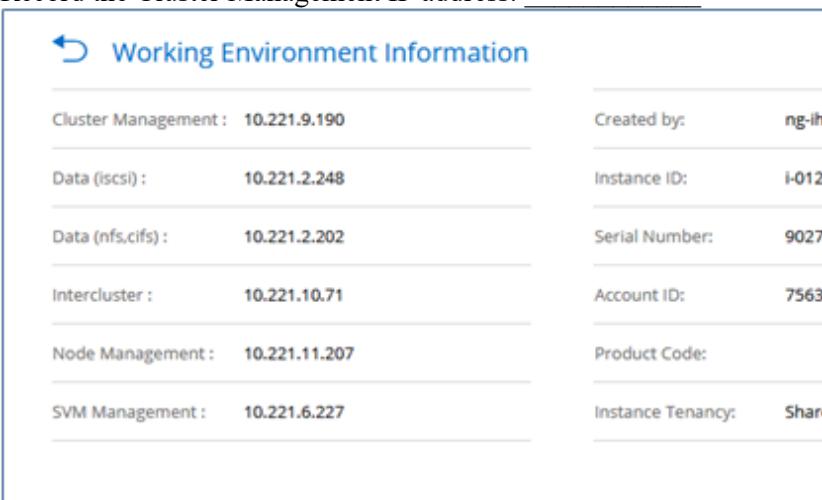
Step	Action
2-10	<p>On the Cloud Volumes ONTAP BYOL License page, click No.</p> 
2-11	<p>On the Preconfigured Packages page, click Create my own configuration.</p> 
2-12	<p>On the IAM Role page, accept the recommendation Let Cloud Manager create the role.</p> 
2-13	<p>Click Continue.</p>

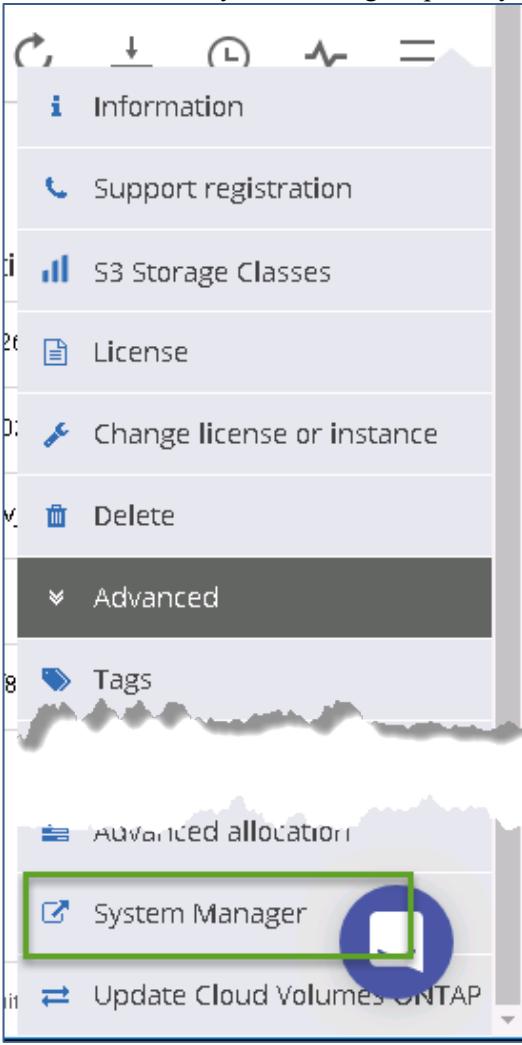
Step	Action
2-14	<p>On the Licensing page, configure the following information:</p> <ol style="list-style-type: none"> Click Change Version, and select ONTAP-9.5 from the list. Click Cloud Volumes ONTAP Standard. Select instance type m4.2xlarge 
2-15	Click Continue .
2-16	On the NetApp Support site credentials page, leave all the fields blank.
2-17	Click Continue .
2-18	<p>On the Underlying Storage Resources page, select General Purpose SSD and AWS Disk Size as 100 GB.</p> 
2-19	Click Continue .

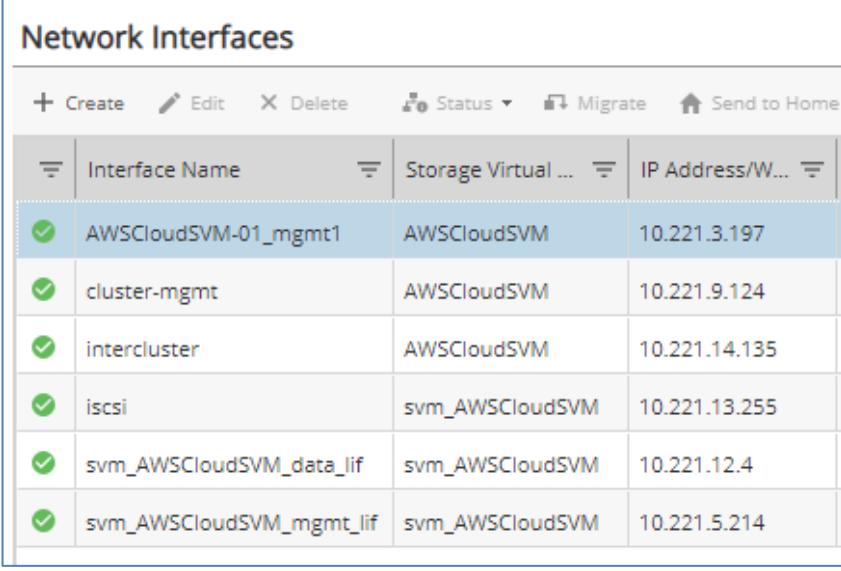
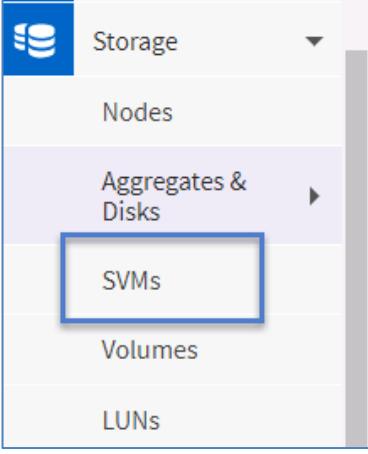
Step	Action
2-20	Complete the Write Speed & WORM page with the following: <ul style="list-style-type: none"> For the Write Speed, select Normal. For the WORM, select Disable Worm.
2-21	Click Continue .
2-22	On the Create Volume page, configure the following: <ul style="list-style-type: none"> Volume 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: <ul style="list-style-type: none"> 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! 

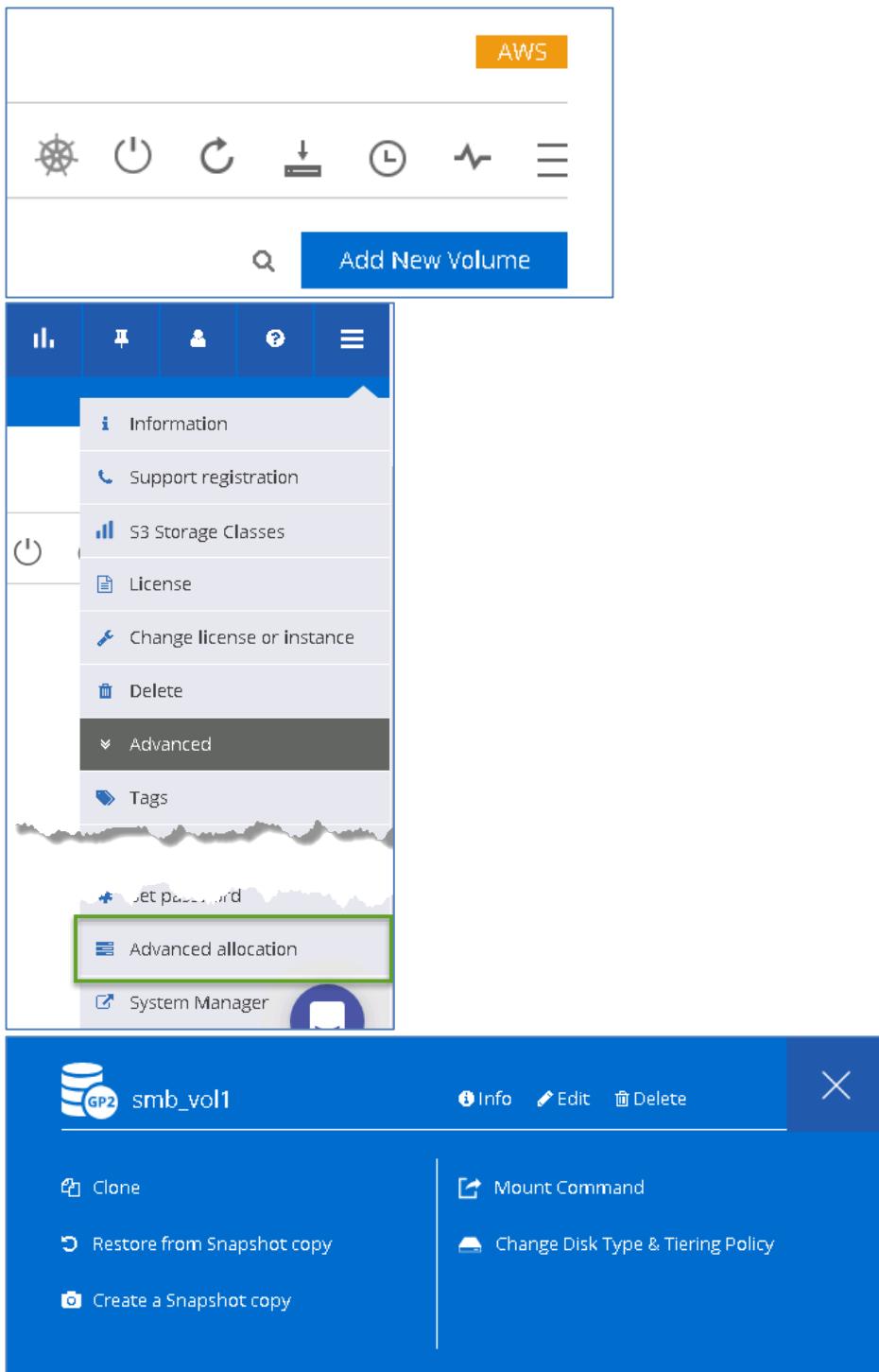
Step	Action								
2-25	Click Continue .								
2-26	On the Create Volume – Usage Profile, Disk Type & Tiering Policy page, select the Volume Tiering Policy menu and then select None . <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <input checked="" type="radio"/> Storage Efficiency Enable thin provisioning, deduplication, and compression <input type="radio"/> No Storage Efficiency Use fully provisioned capacity </div> <div style="margin-top: 20px;">  General Purpose SSD </div> <p>Cloud Manager will create the volume using the disk type that you previously selected. You can use different disk types with future volumes.</p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;">  Tiering data to object storage ^ </div> <div style="margin-top: 10px;"> i Volume Tiering Policy <div style="margin-top: 10px;"> <input type="radio"/> Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage. <input type="radio"/> Snapshot Only - Tiers cold Snapshot copies to object storage <input checked="" type="radio"/> None - Data tiering is disabled. </div> </div> </div>								
2-27	Click Continue .								
2-28	On the Review & Approve page, review the information, and then complete the following actions: <ol style="list-style-type: none"> Select the checkbox that is labeled I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. Select the checkbox that is labeled I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. Next to the “I understand that Cloud Manager ...” text, click More information. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> Previous Step Review & Approve </div> <div style="margin-top: 20px;"> <p>AWSCloudSVM us-east-1 AWS</p> <p><input checked="" type="checkbox"/> I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. More information ></p> <p><input checked="" type="checkbox"/> I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. More information ></p> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 20px;"> Overview Networking Storage ↗ </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 20px;"> <tr> <td style="padding: 5px;">Storage System:</td> <td style="padding: 5px;">Cloud Volumes ONTAP</td> <td style="padding: 5px;">Instance Tenancy:</td> <td style="padding: 5px;">Shared</td> </tr> <tr> <td style="padding: 5px;">License Type:</td> <td style="padding: 5px;">Cloud Volumes ONTAP Explore</td> <td style="padding: 5px;">Encryption:</td> <td style="padding: 5px;">None</td> </tr> </table> <div style="text-align: center; margin-top: 20px;"> GO </div> </div> </div>	Storage System:	Cloud Volumes ONTAP	Instance Tenancy:	Shared	License Type:	Cloud Volumes ONTAP Explore	Encryption:	None
Storage System:	Cloud Volumes ONTAP	Instance Tenancy:	Shared						
License Type:	Cloud Volumes ONTAP Explore	Encryption:	None						

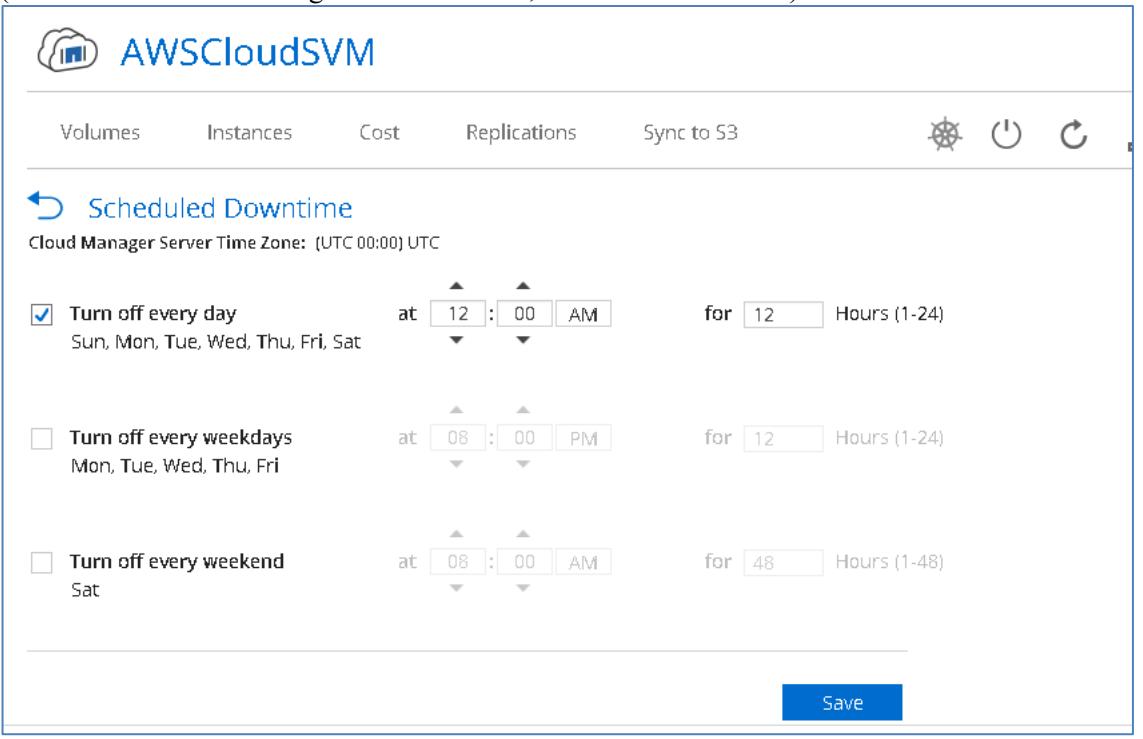
Step	Action
2-29	<p>Review the AWS resources that are allocated, and click Close.</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Cloud Manager allocates the following resources for each Cloud Volumes ONTAP working environment:</p> <ul style="list-style-type: none"> • Two EBS Disks: <ul style="list-style-type: none"> ◦ Cloud Volumes ONTAP Boot volume - 45 GB / 1250 PIOPS ◦ Cloud Volumes ONTAP Root volume - 140 GB / AWS General Purpose (SSD) • Up to six 100 GB disks to support required data capacity • Two AWS snapshots (replicating Cloud Volumes ONTAP Boot & Root disks) • EC2 instance for Cloud Volumes ONTAP (m4.xlarge) • S3 Bucket <hr/> <div style="text-align: center; background-color: #0070C0; color: white; padding: 5px 0;"> Close </div> </div>
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	<p>On the working environment page, click the menu icon, and then select Information to show the configuration details.</p> 																											
2-35	<p>Record the Cluster Management IP address: _____</p>  <table border="1"> <thead> <tr> <th colspan="3">Working Environment Information</th> </tr> </thead> <tbody> <tr> <td>Cluster Management :</td> <td>10.221.9.190</td> <td>Created by:</td> <td>ng-ih</td> </tr> <tr> <td>Data (iscsi) :</td> <td>10.221.2.248</td> <td>Instance ID:</td> <td>I-012</td> </tr> <tr> <td>Data (nfs,cifs) :</td> <td>10.221.2.202</td> <td>Serial Number:</td> <td>9027</td> </tr> <tr> <td>Intercluster :</td> <td>10.221.10.71</td> <td>Account ID:</td> <td>7563</td> </tr> <tr> <td>Node Management:</td> <td>10.221.11.207</td> <td>Product Code:</td> <td></td> </tr> <tr> <td>SVM Management :</td> <td>10.221.6.227</td> <td>Instance Tenancy:</td> <td>Shared</td> </tr> </tbody> </table>	Working Environment Information			Cluster Management :	10.221.9.190	Created by:	ng-ih	Data (iscsi) :	10.221.2.248	Instance ID:	I-012	Data (nfs,cifs) :	10.221.2.202	Serial Number:	9027	Intercluster :	10.221.10.71	Account ID:	7563	Node Management:	10.221.11.207	Product Code:		SVM Management :	10.221.6.227	Instance Tenancy:	Shared
Working Environment Information																												
Cluster Management :	10.221.9.190	Created by:	ng-ih																									
Data (iscsi) :	10.221.2.248	Instance ID:	I-012																									
Data (nfs,cifs) :	10.221.2.202	Serial Number:	9027																									
Intercluster :	10.221.10.71	Account ID:	7563																									
Node Management:	10.221.11.207	Product Code:																										
SVM Management :	10.221.6.227	Instance Tenancy:	Shared																									

Step	Action
2-36	<p>Click the working environment menu icon, and then select Advanced > System Manager.</p> <p>Note: To see the System Manager option, you need to expand the Advanced menu selection.</p> 
2-37	Click Launch .
2-38	<p>Log in to OnCommand System Manager with the following Cloud Volumes ONTAP credentials:</p> <ul style="list-style-type: none"> • User name: admin • Password: Netapp1!

Step	Action																					
2-39	<p>View the network interfaces for Cloud Volumes ONTAP, and in the System Manager toolbar, select Network > Network Interfaces.</p>  <table border="1"> <thead> <tr> <th>Interface Name</th> <th>Storage Virtual ...</th> <th>IP Address/W...</th> </tr> </thead> <tbody> <tr> <td>AWSCloudSVM-01_mgmt1</td> <td>AWSCloudSVM</td> <td>10.221.3.197</td> </tr> <tr> <td>cluster-mgmt</td> <td>AWSCloudSVM</td> <td>10.221.9.124</td> </tr> <tr> <td>intercluster</td> <td>AWSCloudSVM</td> <td>10.221.14.135</td> </tr> <tr> <td>iscsi</td> <td>svm_AWSCloudSVM</td> <td>10.221.13.255</td> </tr> <tr> <td>svm_AWSCloudSVM_data_lif</td> <td>svm_AWSCloudSVM</td> <td>10.221.12.4</td> </tr> <tr> <td>svm_AWSCloudSVM_mgmt_lif</td> <td>svm_AWSCloudSVM</td> <td>10.221.5.214</td> </tr> </tbody> </table>	Interface Name	Storage Virtual ...	IP Address/W...	AWSCloudSVM-01_mgmt1	AWSCloudSVM	10.221.3.197	cluster-mgmt	AWSCloudSVM	10.221.9.124	intercluster	AWSCloudSVM	10.221.14.135	iscsi	svm_AWSCloudSVM	10.221.13.255	svm_AWSCloudSVM_data_lif	svm_AWSCloudSVM	10.221.12.4	svm_AWSCloudSVM_mgmt_lif	svm_AWSCloudSVM	10.221.5.214
Interface Name	Storage Virtual ...	IP Address/W...																				
AWSCloudSVM-01_mgmt1	AWSCloudSVM	10.221.3.197																				
cluster-mgmt	AWSCloudSVM	10.221.9.124																				
intercluster	AWSCloudSVM	10.221.14.135																				
iscsi	svm_AWSCloudSVM	10.221.13.255																				
svm_AWSCloudSVM_data_lif	svm_AWSCloudSVM	10.221.12.4																				
svm_AWSCloudSVM_mgmt_lif	svm_AWSCloudSVM	10.221.5.214																				
2-40	<p>In the System Manager toolbar, select Storage > SVMs and explore the storage virtual machine (SVM) that was created.</p> 																					

Step	Action
2-41	<p>Return to Cloud Manager to explore the following features:</p> <ul style="list-style-type: none"> • Create an NFS volume. • Add disks to the Cloud Volumes ONTAP data aggregate. • Review the commands that are available on a volume.  <p>The screenshot shows the AWS Cloud Manager interface. At the top, there's a toolbar with icons for navigation and monitoring. Below it is a search bar and a blue button labeled 'Add New Volume'. The main area displays a list of volumes, with one volume named 'smb_vol1' selected. A context menu is open for this volume, listing options like 'Information', 'Support registration', 'S3 Storage Classes', 'License', 'Change license or instance', 'Delete', 'Advanced' (which is currently selected), and 'Tags'. At the bottom of the context menu, there's a section for 'Advanced allocation' with a green box around it. Another section below it contains 'System Manager' options.</p>
2-42	<p>In the Working Environment toolbar, click the clock icon.</p> 

Step	Action
2-43	<p>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.)</p> 

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.

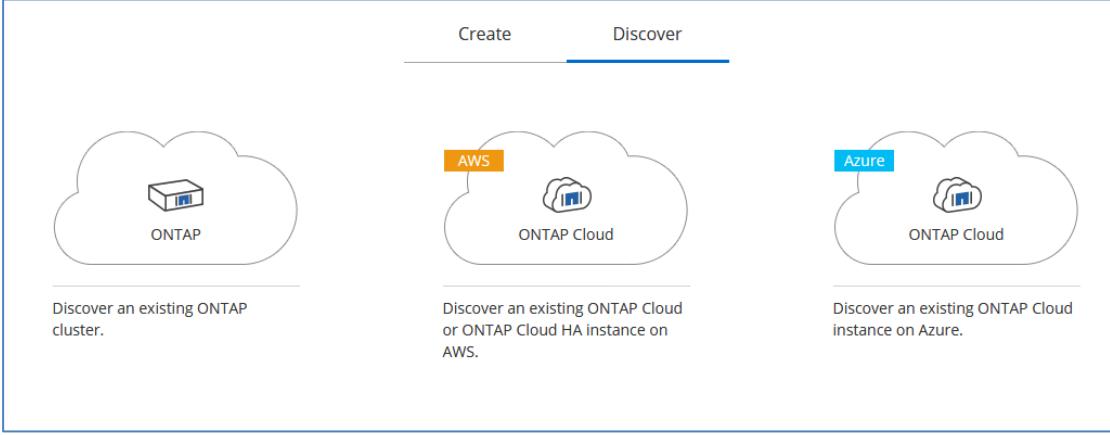
Objectives

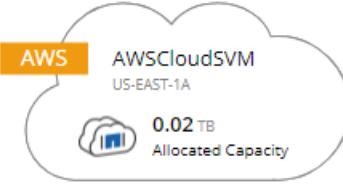
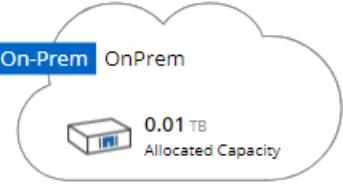
This exercise focuses on enabling you to do the following:

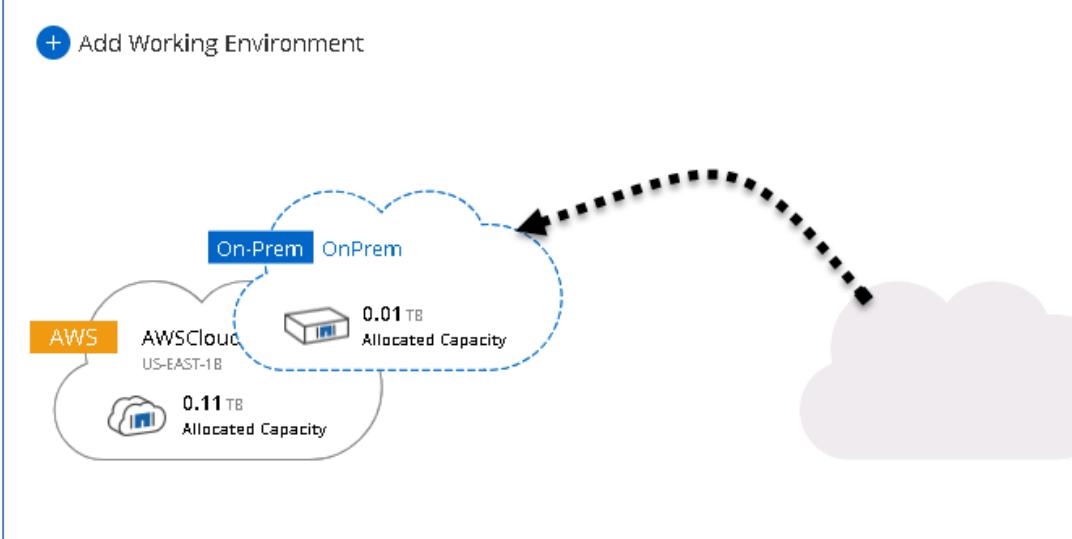
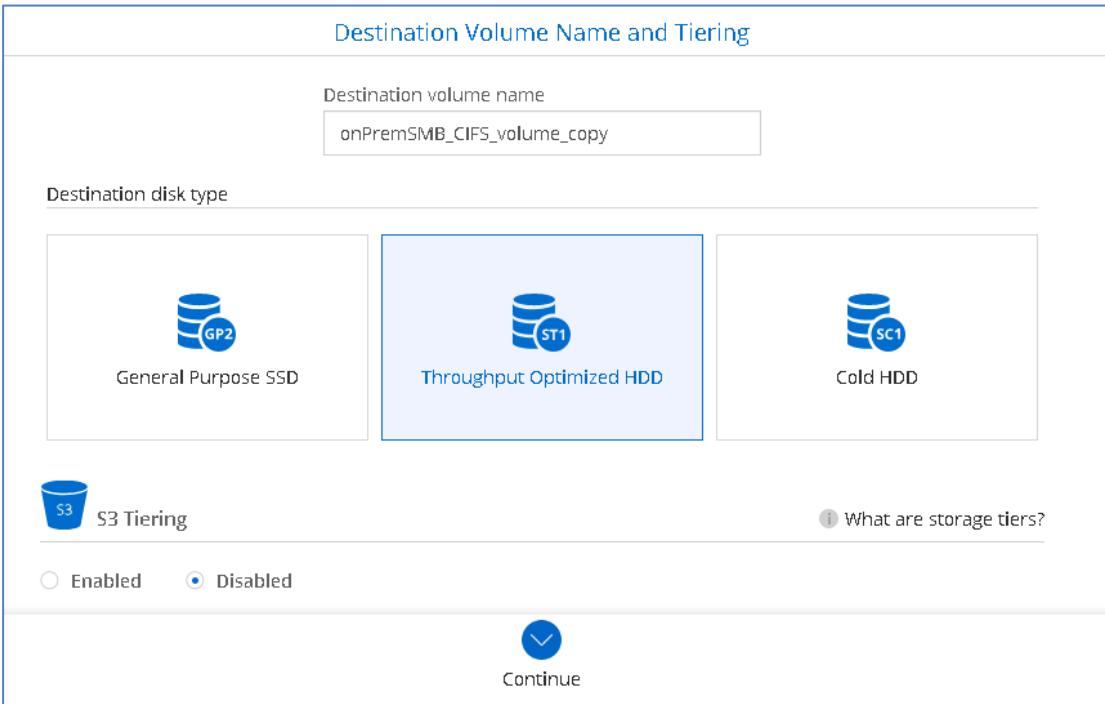
- Use Cloud Manager to implement hybrid-cloud SnapMirror relationships
- Perform a hybrid-cloud disaster recovery

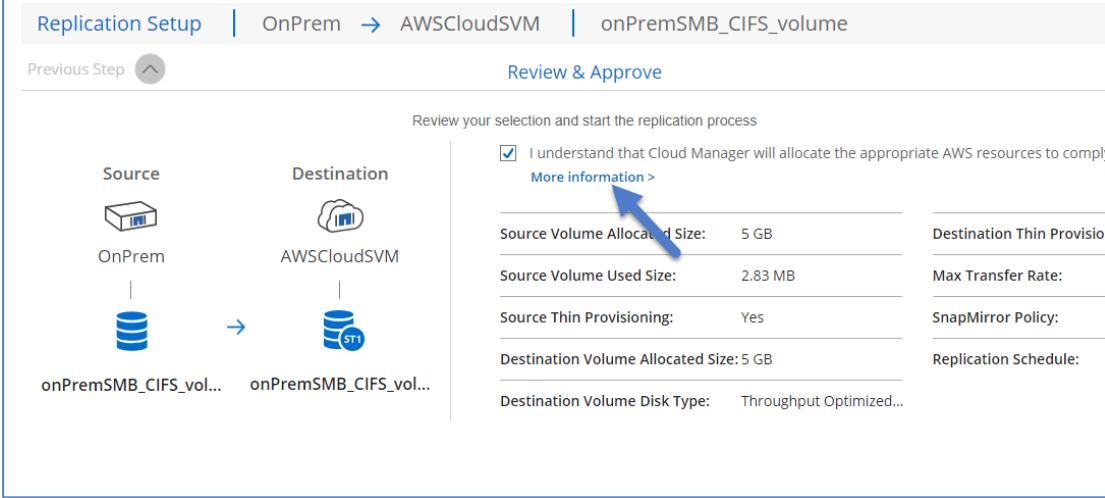
Task 1: Configure Replications Between On-Premises and Cloud

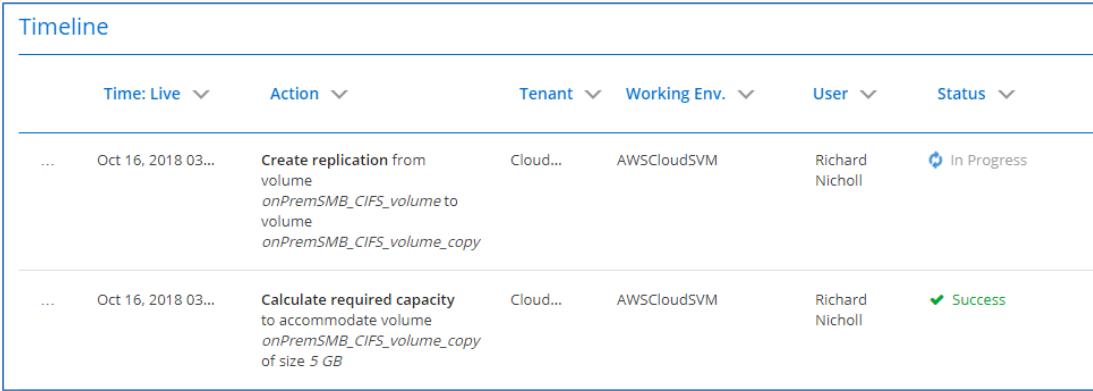
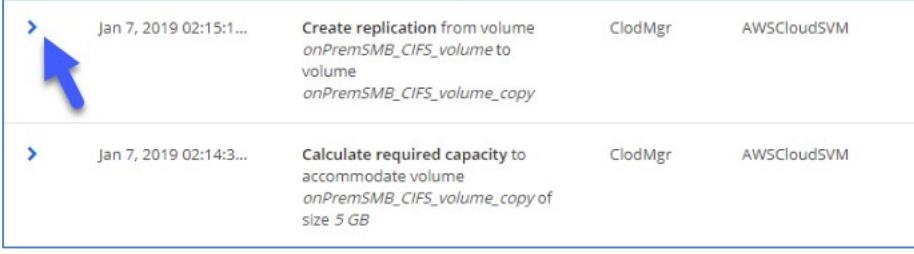
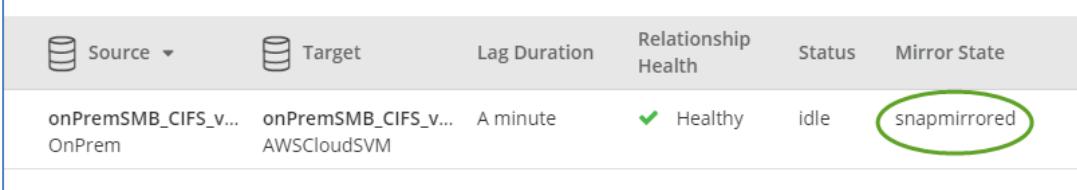
In this task, you use Cloud Manager to set up and manage SnapMirror relationships.

Step	Action
1-1	Copy files from the CourseFiles folder to the on-premises cluster: <ol style="list-style-type: none">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: <ul style="list-style-type: none">• Email Address: <<i>email account that you used for Cloud Central</i>> eg. rt###@demo.netapp.com• Password: <<i>password that you used for Cloud Central</i>>
1-4	Click + Add Working Environment.
1-5	Click the Discover tab.  <p>The screenshot shows the 'Discover' tab selected in the Cloud Manager interface. It displays three options for discovering cloud storage: 'Discover an existing ONTAP cluster' (ONTAP icon), 'Discover an existing ONTAP Cloud or ONTAP Cloud HA instance on AWS' (AWS icon), and 'Discover an existing ONTAP Cloud instance on Azure' (Azure icon).</p>
1-6	Click ONTAP (Discover an existing ONTAP cluster.)

Step	Action
1-7	<p>On the ONTAP Cluster Details page, enter the following information:</p> <ul style="list-style-type: none"> 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	<p>Verify that you now have two working environments.</p> <div style="border: 1px solid #ccc; padding: 10px;"> <h3>Working Environments</h3> <p> Add Working Environment</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>AWS AWSCloudSVM US-EAST-1A  0.02 TB Allocated Capacity</p> </div> <div style="text-align: center;">  <p>On-Prem OnPrem  0.01 TB Allocated Capacity</p> </div> </div> </div>
1-12	<p>In the OnPrem cluster, use System Manager (or the CLI) to verify that no cluster peer relationships exist.</p> <p>CLI command: <code>cluster peer show</code></p>
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. <p>CLI command to verify the existence of intercluster LIF:</p> <pre>net int show -role intercluster</pre>

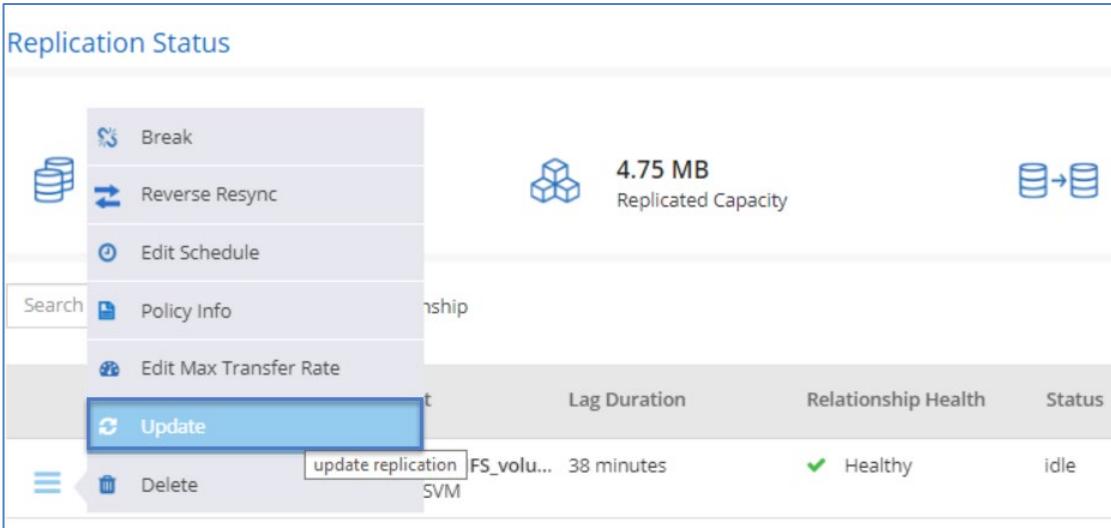
Step	Action
1-14	<p>Return to Cloud Manager, and then drag the OnPrem cloud to the AWSCloudSVM cloud.</p> 
1-15	<p>On the Source Volume Selection page, select onPremSMB_CIFS_volume, and then click Continue.</p>
1-16	<p>On the Destination Volume and Tiering page, do the following:</p> <ul style="list-style-type: none"> Leave the default Destination volume name. For the Destination Disk type, select Throughput Optimized HDD. For the S3 tiering, select Disabled. 
1-17	<p>Click Continue.</p>
1-18	<p>On the Max Transfer Rate page, leave the defaults and click Continue.</p>

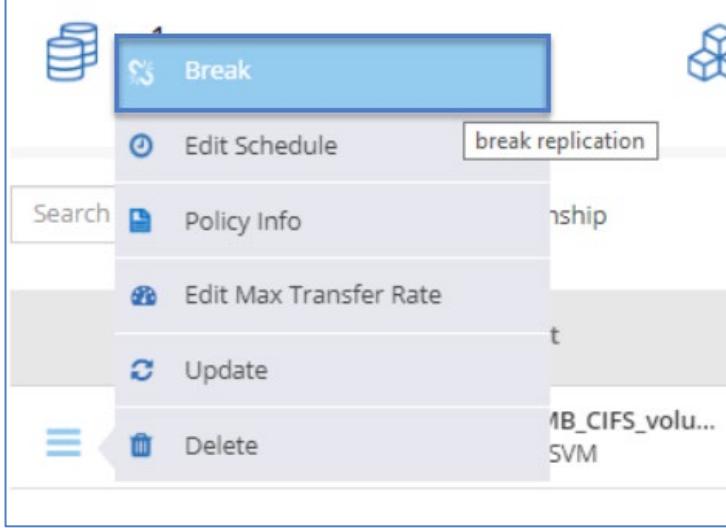
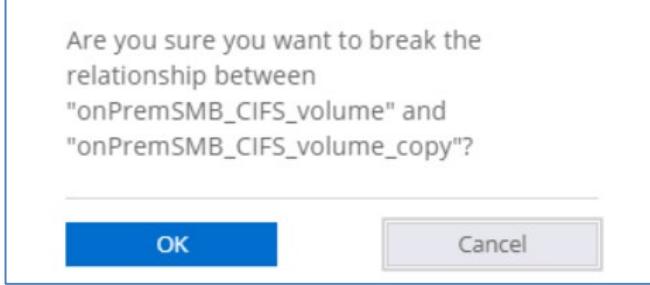
Step	Action
1-19	On the Replication Policy page, click Mirror .
1-20	On the Schedule page, click hourly .
1-21	On the Review page, review the information, and then do the following: <ol style="list-style-type: none"> Select the checkbox that is labeled I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. 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. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>No new AWS resources need to be purchased in order to complete this request.</p> <p>Volume onPremSMB_CIFS_volume_c... will be created on existing Aggregate aggr2.</p> <p style="text-align: center;">Close</p> </div>
1-23	Click Close .
1-24	Click Go .

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

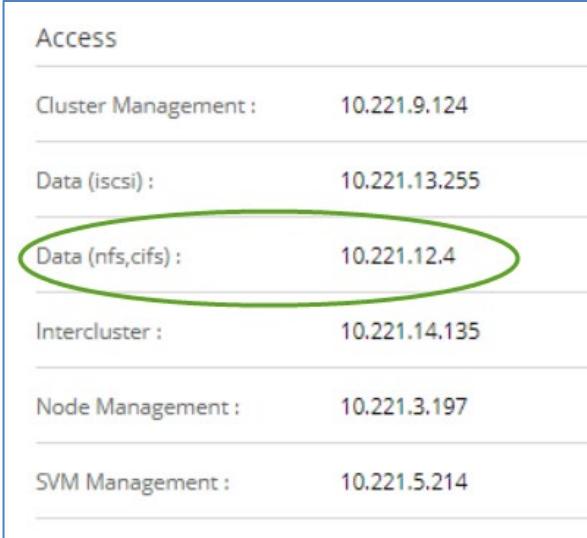
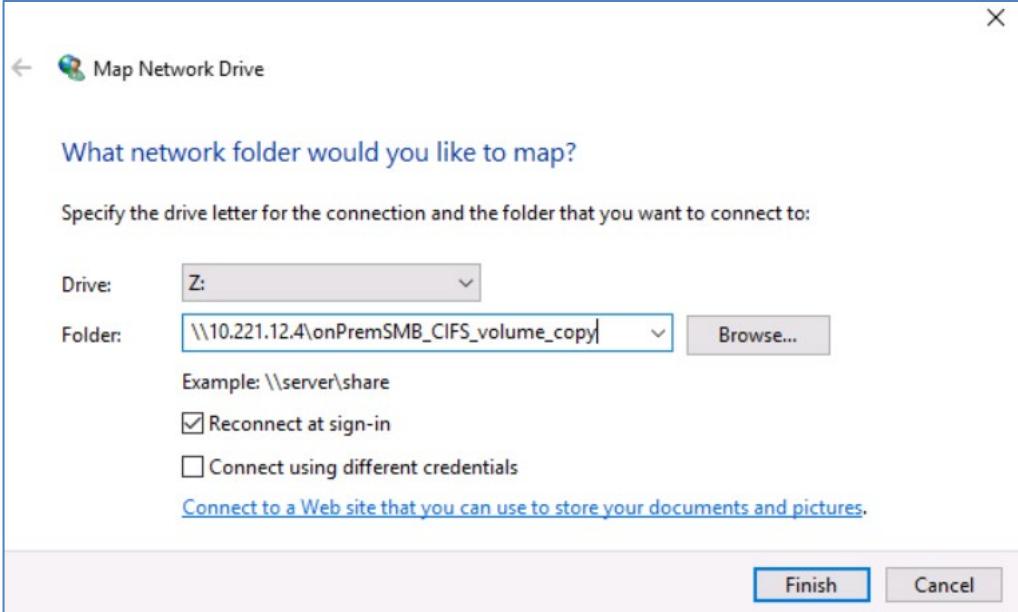
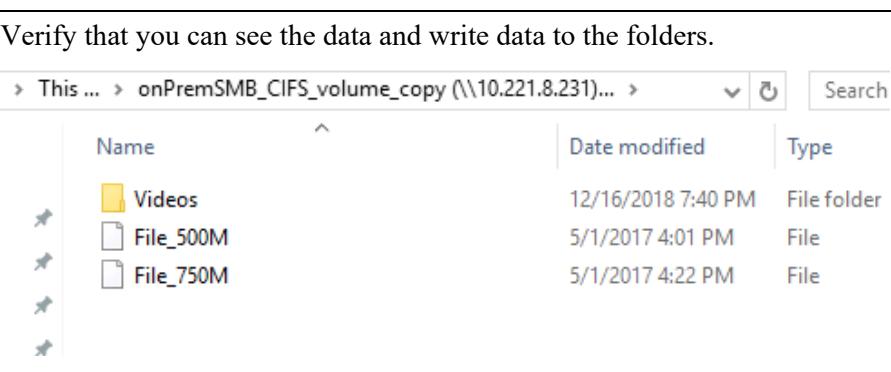
Task 2: Simulate Disaster Recovery

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	<p>Copy files from the CourseFiles folder to the on-premises cluster:</p> <ol style="list-style-type: none">On the jump host, open the CourseFiles folder.Copy the file File_750M and the Videos folder to the share onPremSMB (a shortcut is on the desktop).
2-2	<p>Use Cloud Manager to perform a manual update of the SnapMirror relationship.</p> 
2-3	<p>Wait for the Status to become Idle and the Mirror State to become snapmirrored.</p> 
2-4	 <p>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.</p>

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

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

Step	Action												
2-10	<p>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]).</p>  <p>The screenshot shows the 'Access' section of a configuration interface. It lists several network interfaces with their corresponding IP addresses:</p> <ul style="list-style-type: none"> Cluster Management : 10.221.9.124 Data (iscsi) : 10.221.13.255 Data (nfs,cifs) : 10.221.12.4 (This entry is circled in green) Intercluster : 10.221.14.135 Node Management : 10.221.3.197 SVM Management : 10.221.5.214 												
2-11	 <p>The screenshot shows the 'Map Network Drive' dialog box. It asks 'What network folder would you like to map?'. Below it, it says 'Specify the drive letter for the connection and the folder that you want to connect to:'. The 'Drive:' dropdown is set to 'Z:'. The 'Folder:' dropdown contains '\\10.221.12.4\onPremSMB_CIFS_volume_copy'. There are checkboxes for 'Reconnect at sign-in' (checked) and 'Connect using different credentials' (unchecked). A link 'Connect to a Web site that you can use to store your documents and pictures.' is present. At the bottom are 'Finish' and 'Cancel' buttons.</p> <p>Verify that you can see the data and write data to the folders.</p>  <p>The screenshot shows a file explorer window with the path 'This ... > onPremSMB_CIFS_volume_copy (\\"10.221.8.231)...'. The contents of the folder are listed in a table:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Date modified</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>Videos</td> <td>12/16/2018 7:40 PM</td> <td>File folder</td> </tr> <tr> <td>File_500M</td> <td>5/1/2017 4:01 PM</td> <td>File</td> </tr> <tr> <td>File_750M</td> <td>5/1/2017 4:22 PM</td> <td>File</td> </tr> </tbody> </table>	Name	Date modified	Type	Videos	12/16/2018 7:40 PM	File folder	File_500M	5/1/2017 4:01 PM	File	File_750M	5/1/2017 4:22 PM	File
Name	Date modified	Type											
Videos	12/16/2018 7:40 PM	File folder											
File_500M	5/1/2017 4:01 PM	File											
File_750M	5/1/2017 4:22 PM	File											

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

Step	Action
2-16	Wait for the Status to become Idle and the Mirror State to become snapmirrored.
	<p>The screenshot shows a table with columns: Source, Target, Lag Duration, Relationship Health, Status, and Mirror State. The Source row contains 'onPremSMB_CIFS_volume_copy' and 'AWSCloudSVM'. The Target row contains 'onPremSMB_CIFS_volume' and 'OnPrem'. The Lag Duration is 'A few seconds'. The Relationship Health is 'Healthy' with a green checkmark. The Status is 'idle' and the Mirror State is 'snapmirrored'. The 'Status' and 'Mirror State' columns are highlighted with a green border.</p>
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

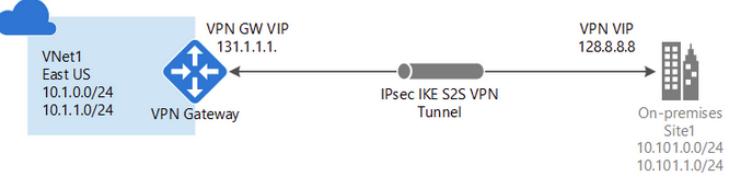
This exercise focuses on enabling you to do the following:

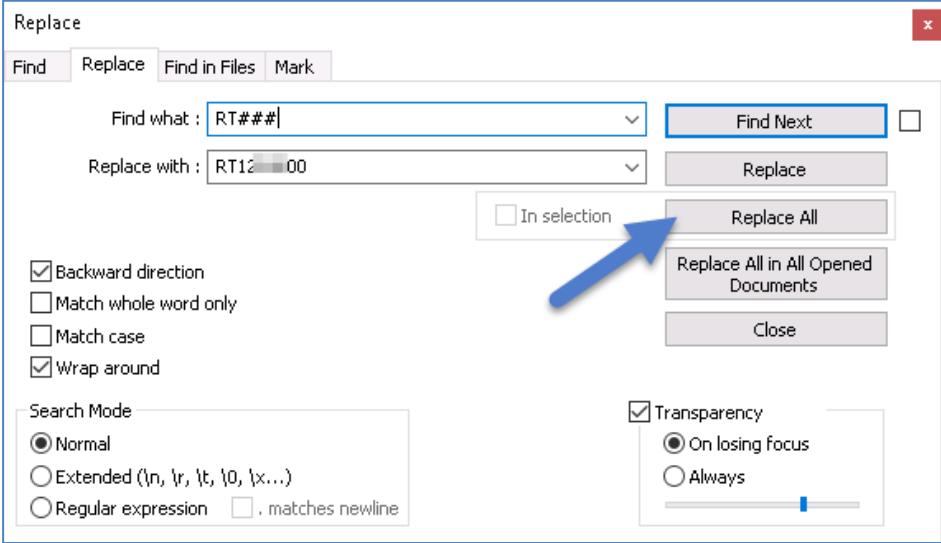
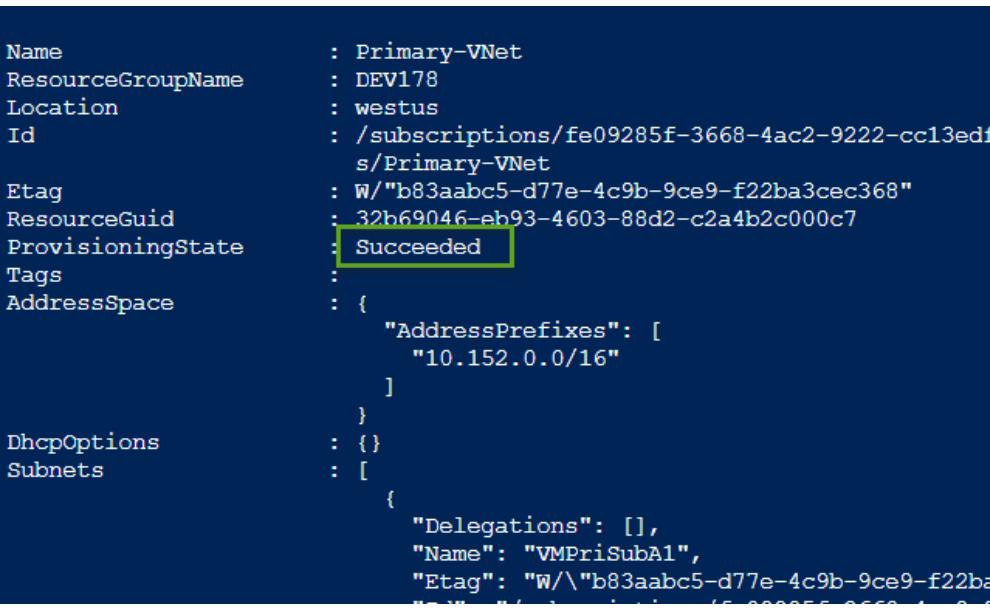
- Use Windows PowerShell to configure Azure resources
- Create and configure VNet resources
- Connect the VNet to a customer gateway through a VNet gateway

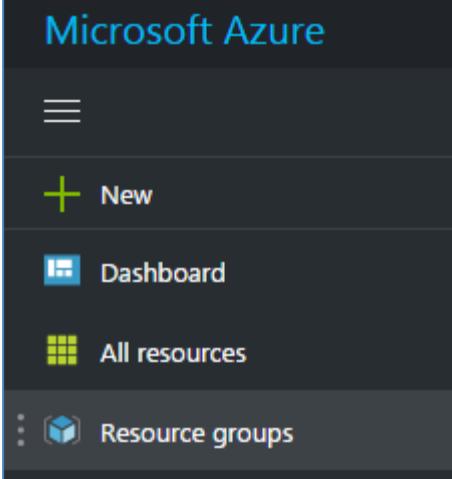
Task 1: Create VNet Resources

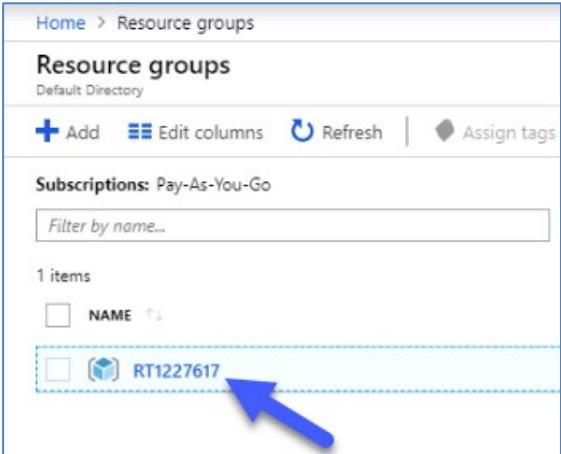
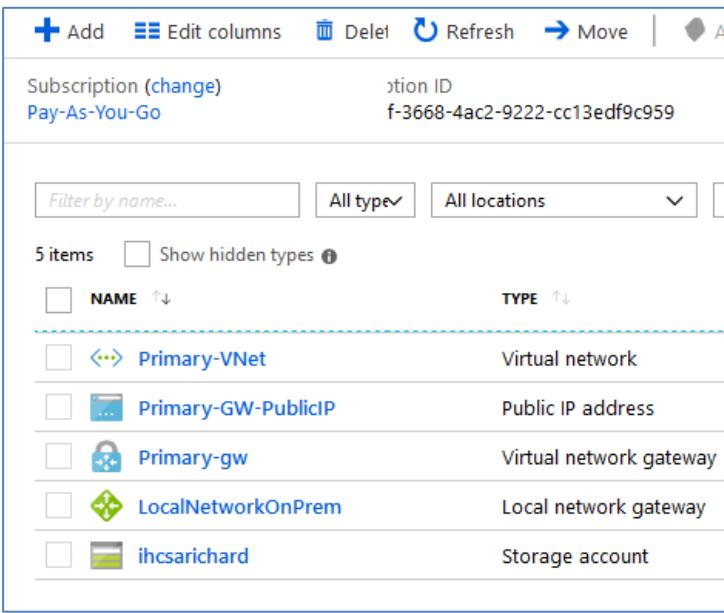
In this task, you create a VNet. You also create two subnets: one private subnet and one gateway subnet. The gateway subnet is a small network that Azure requires for use as a gateway zone for the VPN connection. You also create a local network gateway to connect to the customer gateway (the on-premises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

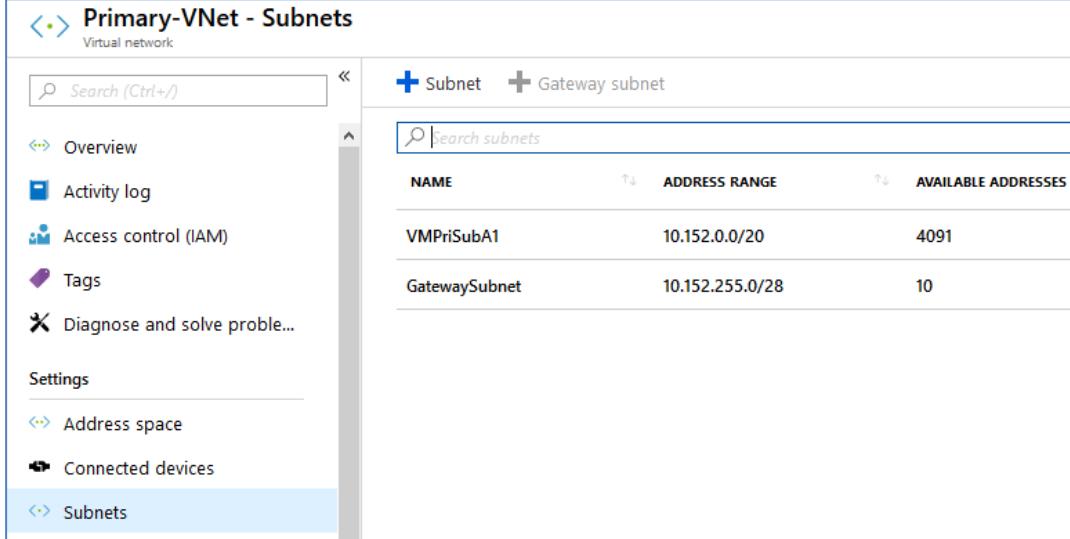
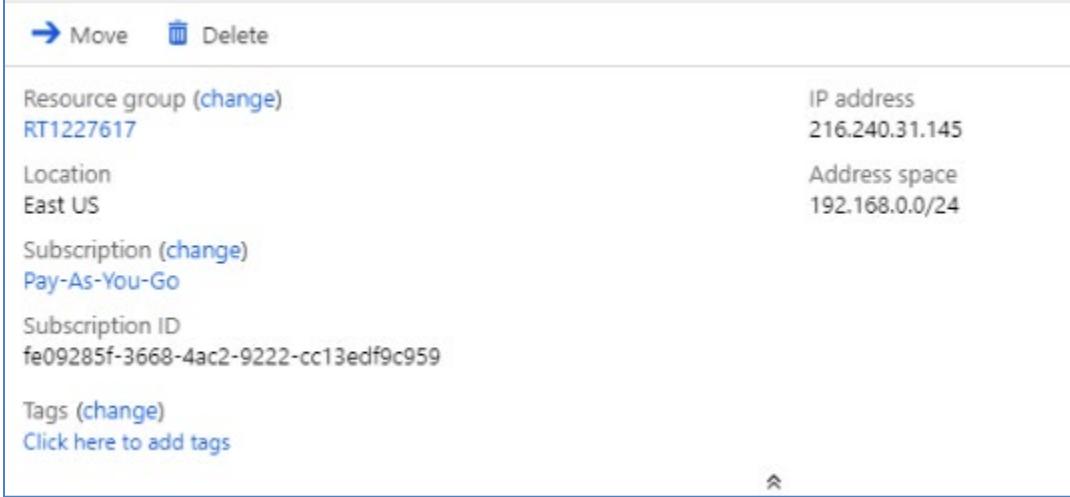
Step	Action
1-1	On your jump host, open a Windows PowerShell window.
1-2	<p>Log in to the Azure Resource Management account:</p> <ol style="list-style-type: none">a. Enter the Login-AzureRmAccount command.• For email, enter the Azure user name (email) from azurelogin.txt.• If you are asked for the account type, select Personal.• For password, enter the password that you created when you unlocked your Azure account. <p>Sample output:</p> <pre>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 :</pre>

Step	Action
1-3	<p>Get your Resource Group Name:</p> <pre>PS C:\Users\Administrator.DEMO> Get-AzureRmResourceGroup</pre> <p>Example Output:</p> <pre>ResourceGroupName : RT1224200 Location : eastus ProvisioningState : Succeeded Tags : ResourceId : /subscriptions/fe09285f-3668-4ac2-9222cc13edf9c959/resourceGroups/RT1224200</pre>
1-4	 <p>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:</p> <p>https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal</p> <div style="border: 1px solid #ccc; padding: 10px;"> <h2>Create a Site-to-Site connection in the Azure portal</h2> <p>10/17/2018 • 19 minutes to read • Contributors </p> <p>This article shows you how to use the Azure portal to create a Site-to-Site VPN gateway connection from your on-premises network to the VNet. The steps in this article apply to the Resource Manager deployment model. You can also create this configuration using a different deployment tool or deployment model by selecting a different option from the following list:</p> <p>Azure portal ▼</p> <p>A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. For more information about VPN gateways, see About VPN gateway.</p>  </div>
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	<p>In the Replace window, do the following:</p> <ul style="list-style-type: none"> Find what: RT### Replace with: <Your-RG-Name> Click Replace All. 
1-8	<p>Do another search to find and replace:</p> <ul style="list-style-type: none"> Find what: yourIP Replace with: the local network gateway IP address that your instructor gave you
1-9	<p>From section A. Create VNets and Subnets, copy and paste the commands into the Windows PowerShell.</p>
1-10	<p>Verify that the VNet creation succeeded.</p> <p>Note: The last command in section A should show an output like below.</p>  <pre> Name : Primary-VNet ResourceGroupName : DEV178 Location : westus Id : /subscriptions/fe09285f-3668-4ac2-9222-cc13edf s/Primary-VNet Etag : W/"b83aabc5-d77e-4c9b-9ce9-f22ba3cec368" ResourceGuid : 32b69046-eb93-4603-88d2-c2a4b2c000c7 ProvisioningState : Succeeded Tags : AddressSpace : { "AddressPrefixes": ["10.152.0.0/16"] } DhcpOptions : {} Subnets : [{ "Delegations": [], "Name": "VMPriSubA1", "Etag": "W/"b83aabc5-d77e-4c9b-9ce9-f22ba "Name": "VMPriSubA1" }] </pre>

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. <pre>Name : LocalNetworkOnPrem ResourceGroupName : DEV178 Location : eastus Id : /subscriptions/fe09285f-3668-4ac Gateways/LocalNetworkOnPrem Etag : W/"ele1e243-4ad6-4f90-ac10-87bda 141ce889-159b-4a28-8983-401cd7f7 ResourceGuid : 141ce889-159b-4a28-8983-401cd7f7 ProvisioningState : Succeeded Tags : GatewayIpAddress : 216.240.31.145 LocalNetworkAddressSpace : { "AddressPrefixes": ["192.168.0.0/24"] }</pre>
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	<p>Click RT###.</p> 
1-18	<p>Click Primary-VNet.</p> 

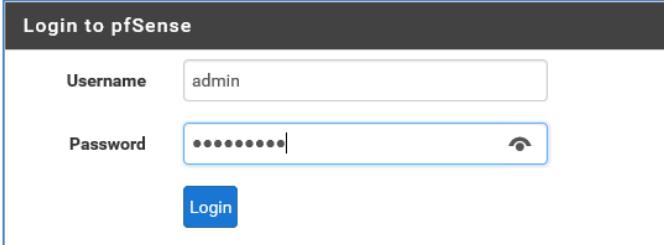
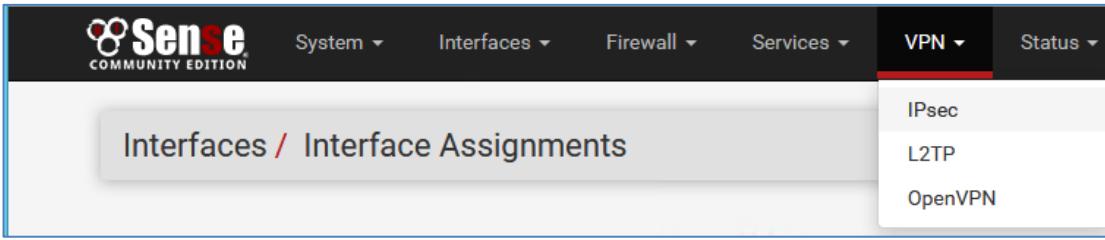
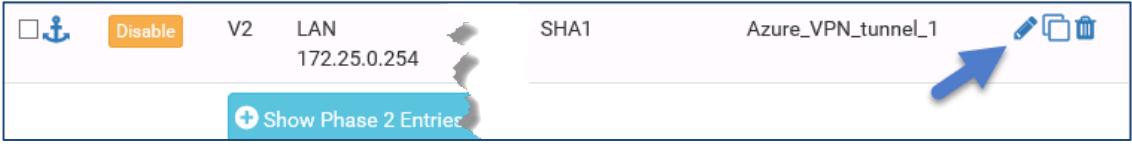
Step	Action																				
1-19	<p>In the Primary-VNet dashboard, click Subnets, and then view the subnets in the VNet.</p>  <table border="1"> <thead> <tr> <th>NAME</th> <th>ADDRESS RANGE</th> <th>AVAILABLE ADDRESSES</th> </tr> </thead> <tbody> <tr> <td>VMPriSubA1</td> <td>10.152.0.0/20</td> <td>4091</td> </tr> <tr> <td>GatewaySubnet</td> <td>10.152.255.0/28</td> <td>10</td> </tr> </tbody> </table>	NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	VMPriSubA1	10.152.0.0/20	4091	GatewaySubnet	10.152.255.0/28	10											
NAME	ADDRESS RANGE	AVAILABLE ADDRESSES																			
VMPriSubA1	10.152.0.0/20	4091																			
GatewaySubnet	10.152.255.0/28	10																			
1-20	<p>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.</p> <p>Sample output:</p>  <table border="1"> <thead> <tr> <th>Resource group (change)</th> <th>IP address</th> </tr> </thead> <tbody> <tr> <td>RT1227617</td> <td>216.240.31.145</td> </tr> <tr> <th>Location</th> <th>Address space</th> </tr> <tr> <td>East US</td> <td>192.168.0.0/24</td> </tr> <tr> <th>Subscription (change)</th> <th></th> </tr> <tr> <td>Pay-As-You-Go</td> <td></td> </tr> <tr> <th>Subscription ID</th> <td></td> </tr> <tr> <td>fe09285f-3668-4ac2-9222-cc13edf9c959</td> <td></td> </tr> <tr> <th>Tags (change)</th> <td></td> </tr> <tr> <td>Click here to add tags</td> <td></td> </tr> </tbody> </table>	Resource group (change)	IP address	RT1227617	216.240.31.145	Location	Address space	East US	192.168.0.0/24	Subscription (change)		Pay-As-You-Go		Subscription ID		fe09285f-3668-4ac2-9222-cc13edf9c959		Tags (change)		Click here to add tags	
Resource group (change)	IP address																				
RT1227617	216.240.31.145																				
Location	Address space																				
East US	192.168.0.0/24																				
Subscription (change)																					
Pay-As-You-Go																					
Subscription ID																					
fe09285f-3668-4ac2-9222-cc13edf9c959																					
Tags (change)																					
Click here to add tags																					

Task 2: Configure a VPN Connection

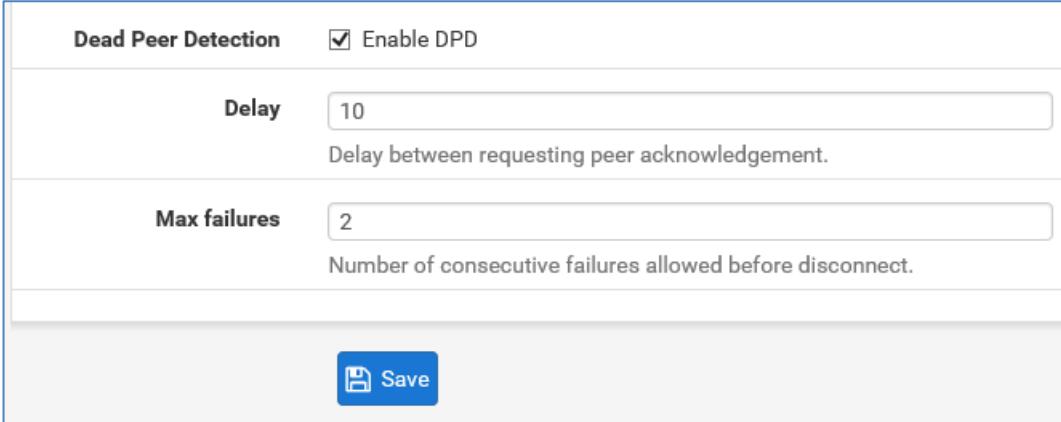
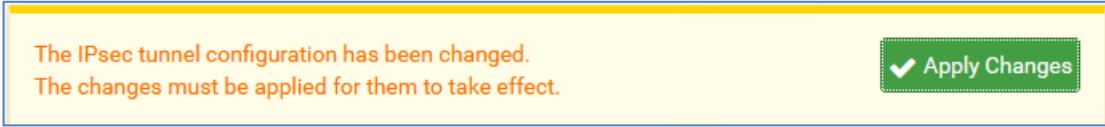
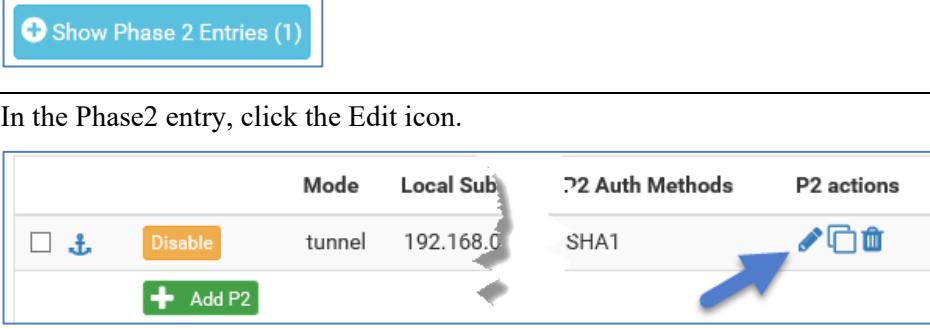
In this task, you set up a connection between Azure and the on-premises data center by using a VPN IPsec connection. You create and configure a VNet gateway, and then you create the VPN connection on the Azure side. Finally, you use pfSense in the on-premises data center to configure and initiate the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

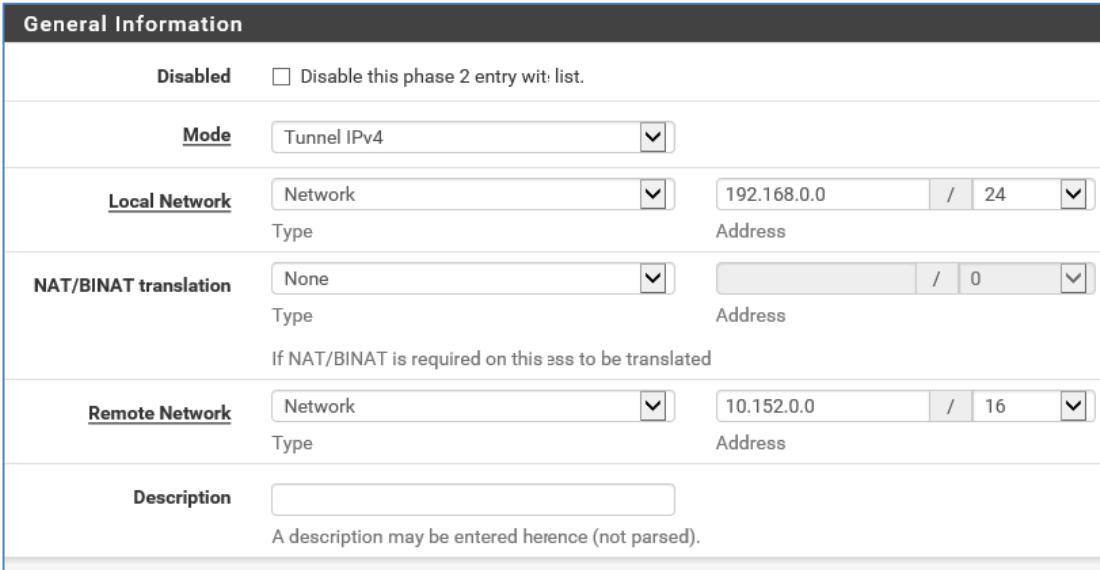
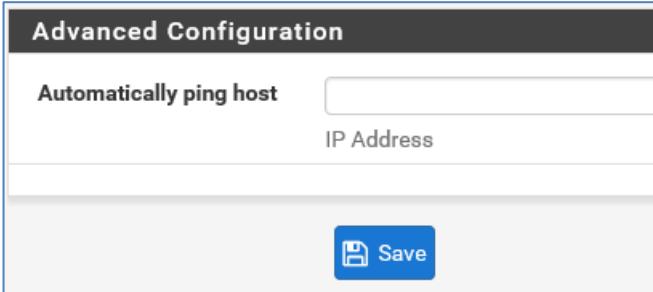
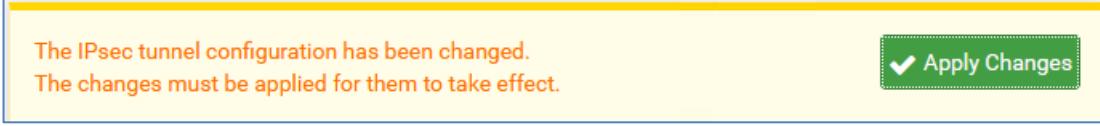
Step	Action
2-1	<p>From section C. Create VNet Gateway (VGW), copy and paste the commands into the Windows PowerShell.</p> <p>Note: The gateway-creation process might take up to 45 minutes. After the process is complete, you might need to press Enter in the Windows PowerShell window to see the results.</p> <p>Sample output:</p> <pre>Name : Primary-gw ResourceGroupName : DEV178 Location : eastus Id : /subscriptions/fe09285f-3668-4ac2-9222-cc13ed Gateways/Primary-gw Etag : W/"02ac54a8-82c9-47b8-b4b7-f9461db54b64" ResourceGuid : 2e543d80-32b5-4287-bdd6-0a9d7b392b77 ProvisioningState : Succeeded Tags : IpConfigurations : [{ "PrivateIpAllocationMethod": "Dynamic", "Subnet": { </pre> <p>If</p>
2-2	<p>Review the commands that you issued:</p> <ul style="list-style-type: none">• You used the <code>New-AzureRmPublicIpAddress</code> 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.

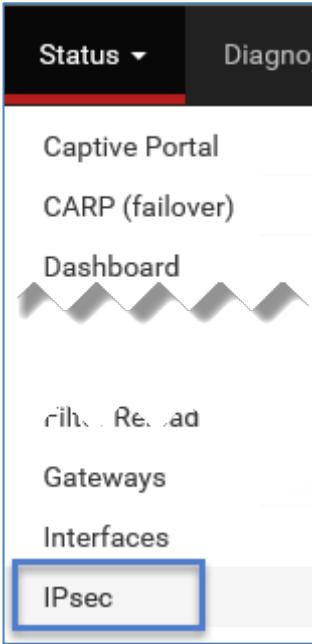
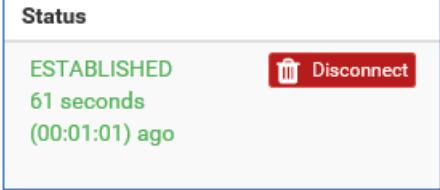
Step	Action
2-3	<p>Return to the Azure portal RT### resource group, and then look at the Primary-GW-PublicIP.</p>
2-4	<p>Record the public IP address, or save it in the Azure_connection_info.txt file in the CourseFiles folder:</p> <hr/>
2-5	<p>From section D. Create VPN Connection, copy and paste the commands into the Windows PowerShell.</p>
2-6	<p>Verify that the VPN Connection is created. (The ConnectionStatus is “Unknown” or “Connecting” until the pfSense on-premises configuration is complete.)</p> <pre>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 ErrorDetails : </pre>

Step	Action
2-7	 For Shared Key, the value must match the value that you will use for your local on-premises VPN device (“abc123xyz456” 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: <ul style="list-style-type: none"> User name: admin Password: Netapp1! 
2-11	Select VPN > IPsec . 
2-12	In the Azure VPN Tunnel 1 entry, click the Edit icon. 

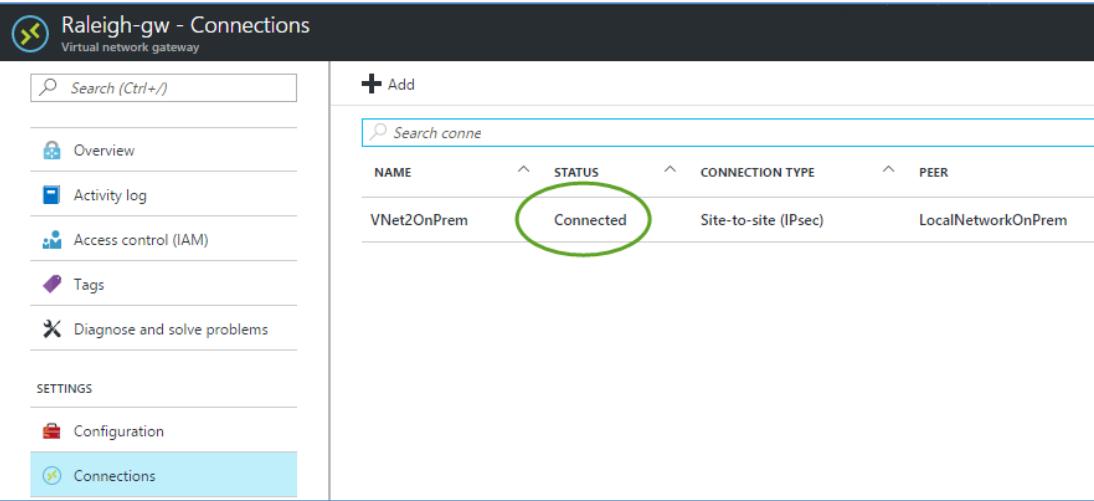
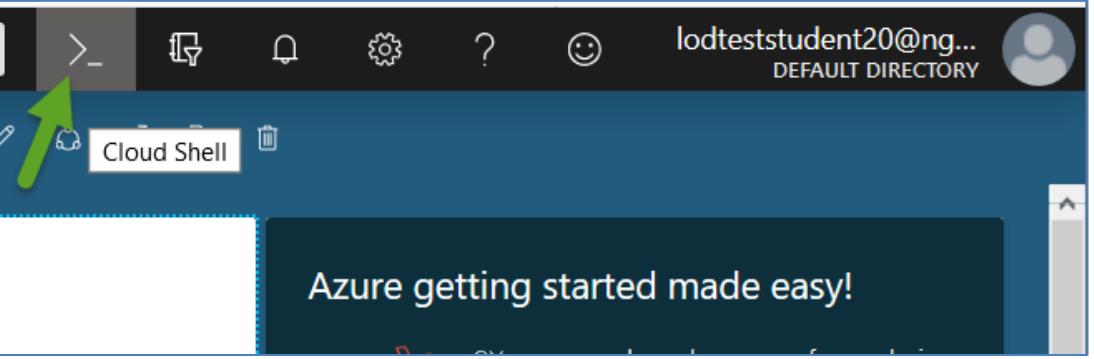
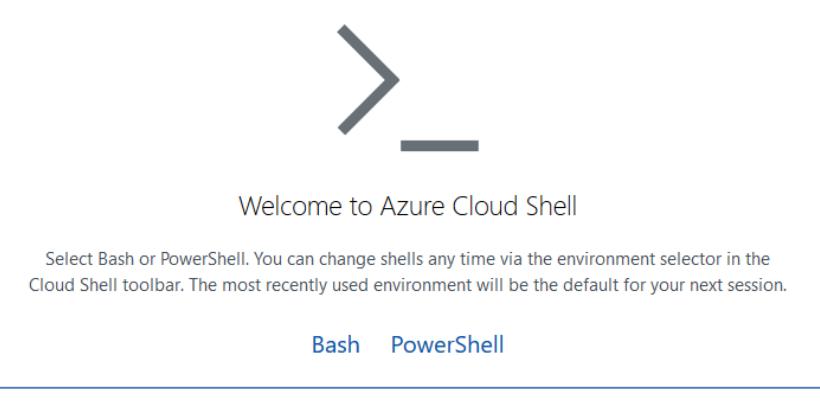
Step	Action
2-13	<p>In the General Information section, in the Remote Gateway field, overwrite the value with the IP address that you recorded in Step 2-4.</p> <p>General Information</p> <p>Disabled <input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.</p> <p>Key Exchange version IKEv2 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 with IKEv2 as responder.</p> <p>Internet Protocol IPv4 Select the Internet Protocol family.</p> <p>Interface LAN Select the interface for the local endpoint of this phase1 entry.</p> <p>Remote Gateway Enter the public IP address or host name of the remote gateway.</p> <p>Description Azure_VPN_tunnel_1 A description may be entered here for administrative reference (not parsed).</p>
2-14	<p>In the Phase 1 Proposal (Authentication) section, in the Pre-Shared Key field, overwrite the value with the value abc123xyz456.</p> <p>Phase 1 Proposal (Authentication)</p> <p>Authentication Method Mutual PSK Must match the setting chosen on the remote side.</p> <p>My identifier My IP address</p> <p>Peer identifier Peer IP address</p> <p>Pre-Shared Key abc123xyz456 Enter the Pre-Shared Key string.</p>

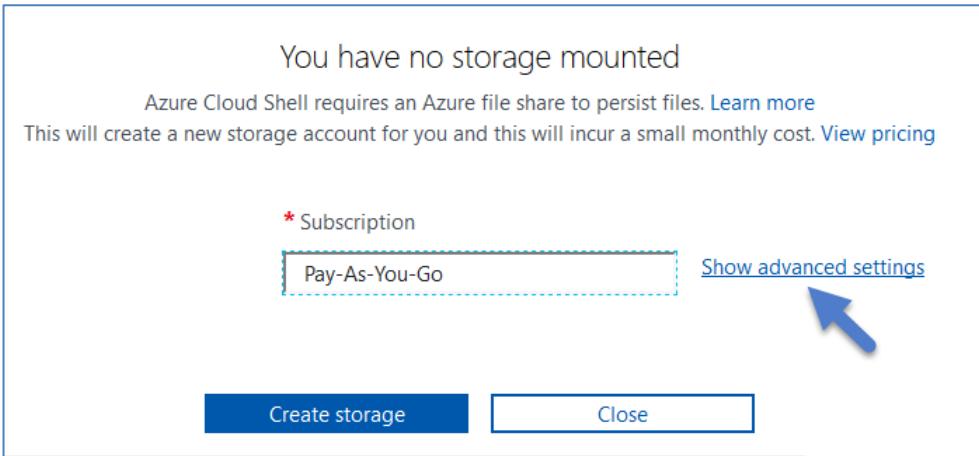
Step	Action
2-15	<p>Accept all the other default values, scroll to bottom of the page, and then click Save.</p> 
2-16	<p>Click Apply Changes.</p> 
2-17	<p>For Azure VPN Tunnel 1, click Show Phase 2 Entries (1).</p> 
2-18	<p>In the Phase2 entry, click the Edit icon.</p> 

Step	Action
2-19	<p>In the General Information section, enter the specified values in place of the defaults in the following fields:</p> <ul style="list-style-type: none"> • Local Network: 192.168.0.0/24 • Remote Network: 10.152.0.0/16 
2-20	<p>Accept all other default values, scroll to bottom of the page, and then click Save.</p> 
2-21	<p>Click Apply Changes.</p> 

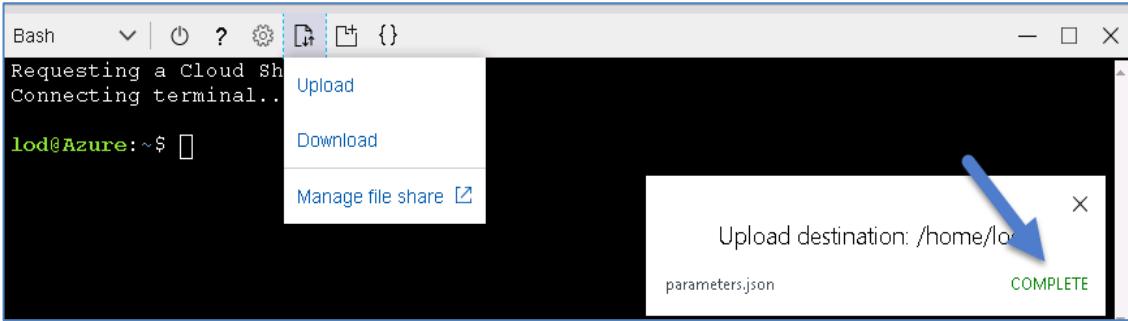
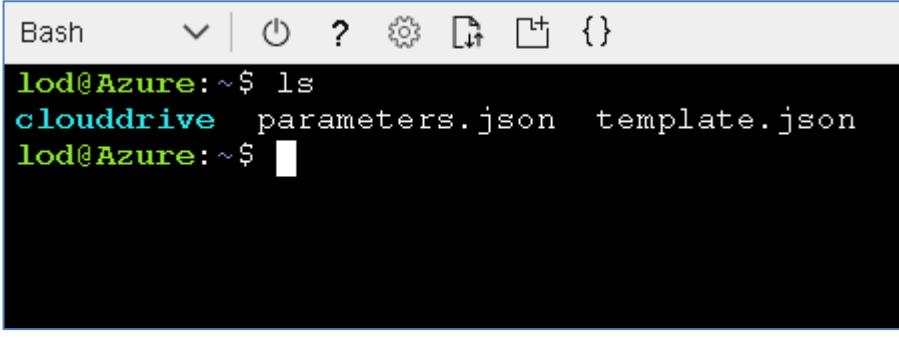
Step	Action
2-22	From the pfSense menu bar, select Status > IPsec .
	
2-23	For Azure VPN Tunnel 1, click Connect VPN .
	
2-24	Verify that the session is Established.
	

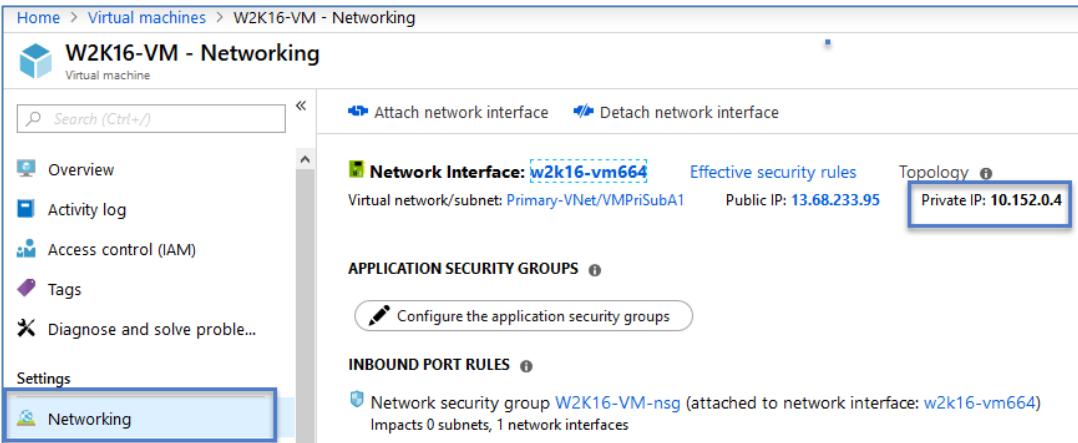
Task 3: Verify Connectivity

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

Step	Action
3-4	<p>Click Show advanced settings.</p> 
3-5	<p>In the You have no storage mounted page, do the following:</p> <ol style="list-style-type: none"> Select the Cloud Shell region East US. For the Resource group, select Use existing and then select your available resource group. For the storage account, select Create new and then enter ihcsabnu<your name>. For the file share, select Create new and then enter ihcfsribanu<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	<p>Launch a Windows Server VM by using the Azure CLI:</p> <p>(For <Your-ResourceGroup>, you can start typing RT and then press Tab to complete it.)</p> <pre>a. az group deployment create --resource-group <Your-ResourceGroup> --template-file ./template.json --parameters ./parameters.json</pre> <p>Please provide string value for 'VNetName' (? for help): RT###</p> <p>(Example concatenated output)</p> <pre>{ "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"</pre>
3-12	<p>Select Virtual Machines > W2K16-VM > Networking, and then record the Private IP Address:</p> <hr/> 

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

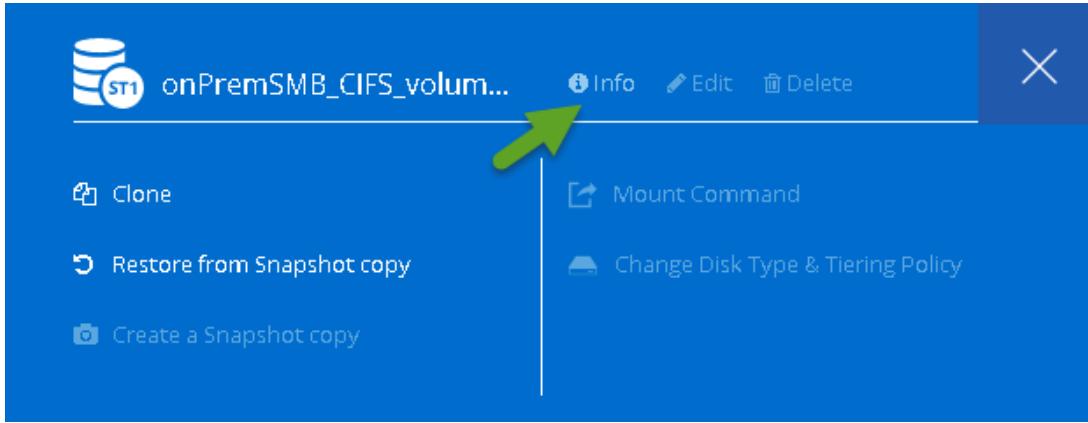
In this exercise, you tier secondary data from Cloud Volumes ONTAP to Amazon Simple Storage Service (Amazon S3).

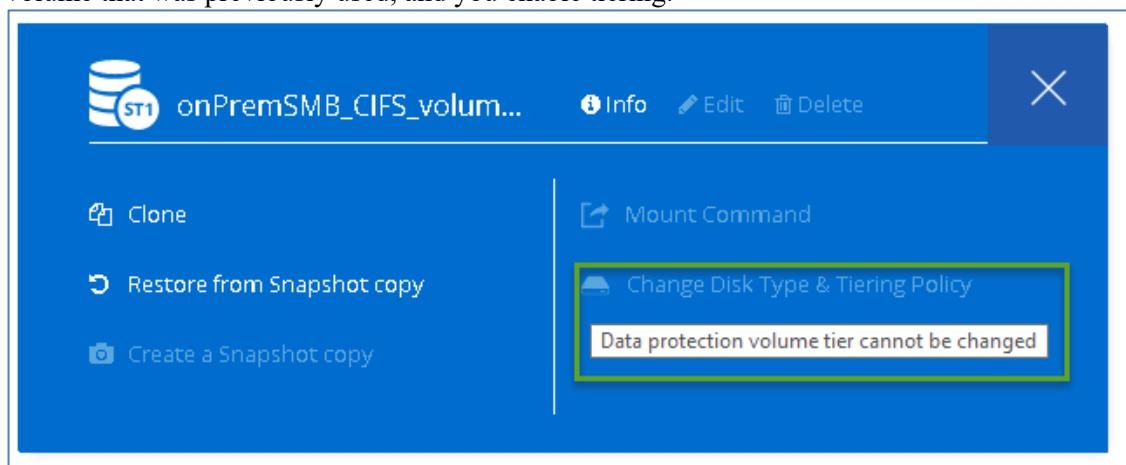
Objectives

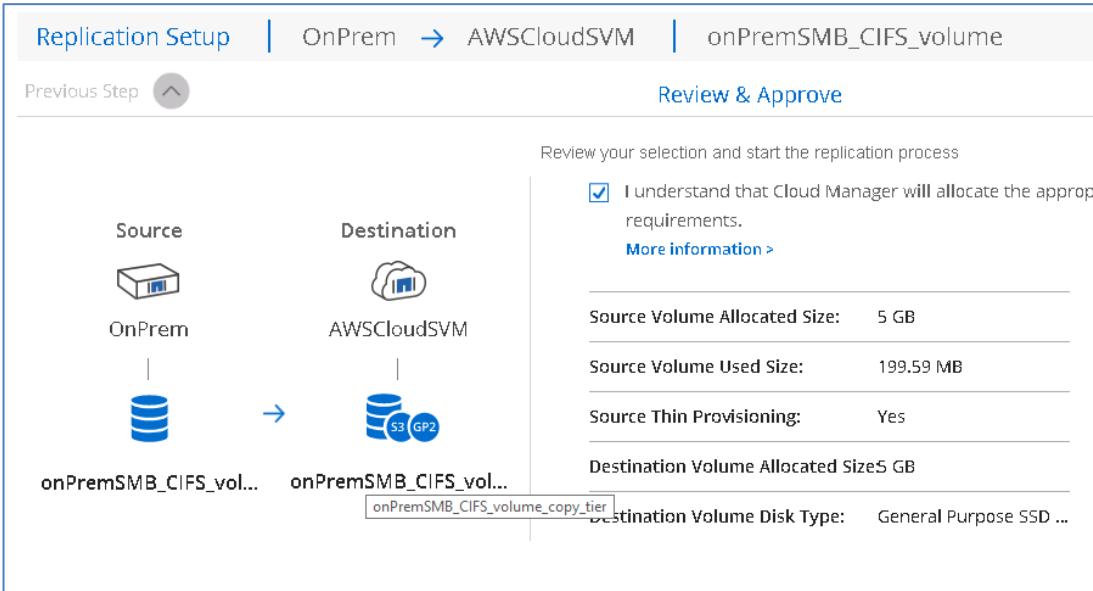
This exercise focuses on enabling you to do the following:

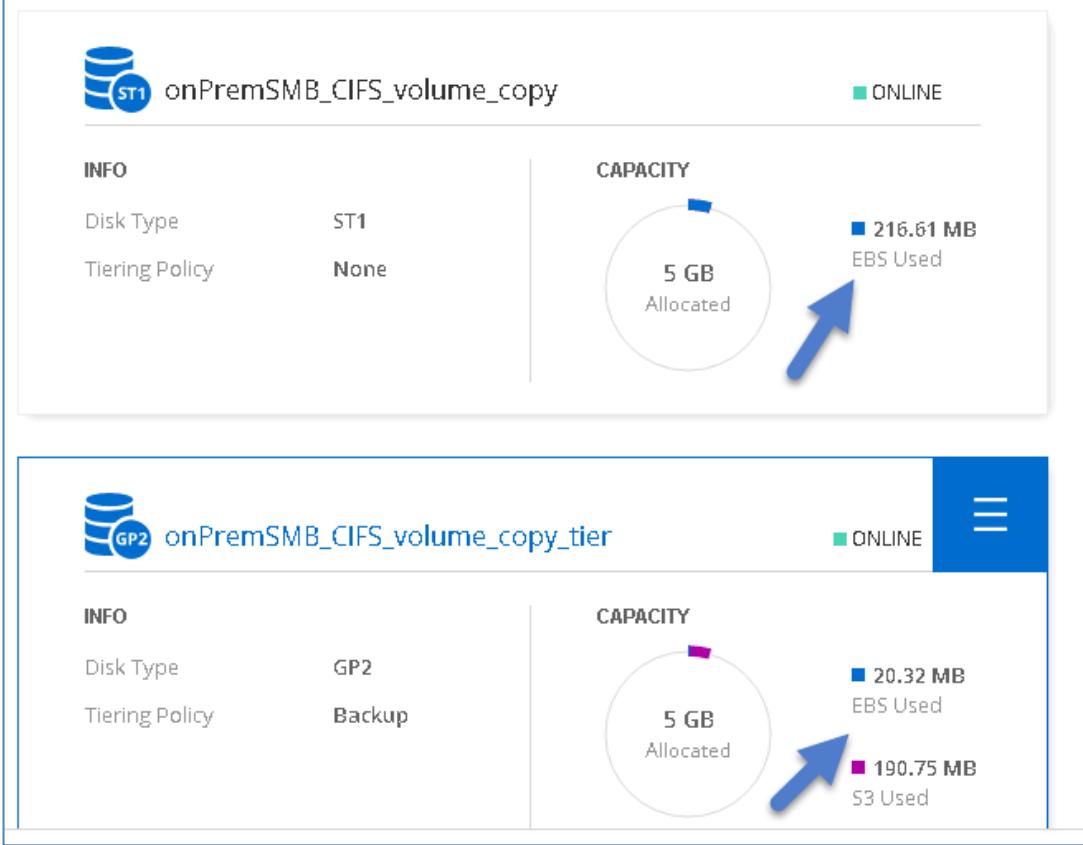
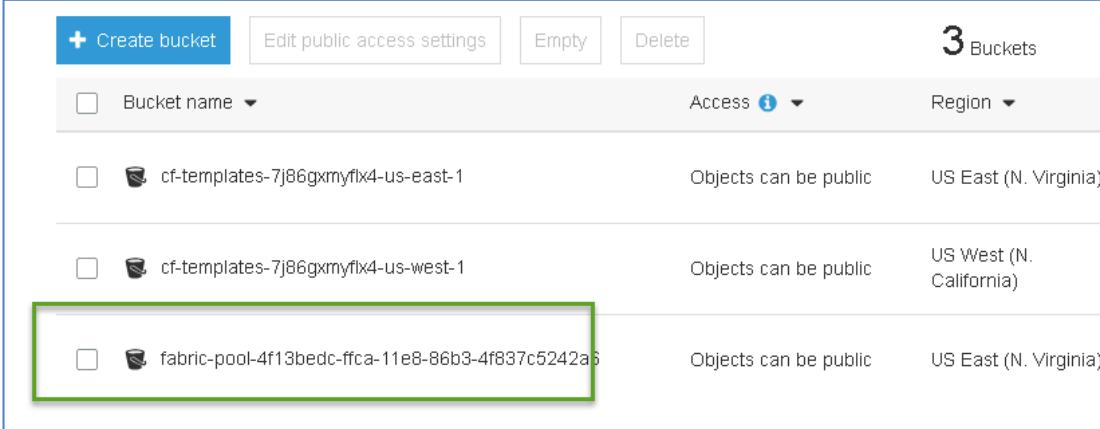
- Use OnCommand Cloud Manager to configure data tiering
- Verify that data is tiered to Amazon Simple Storage Service (Amazon S3 or S3).

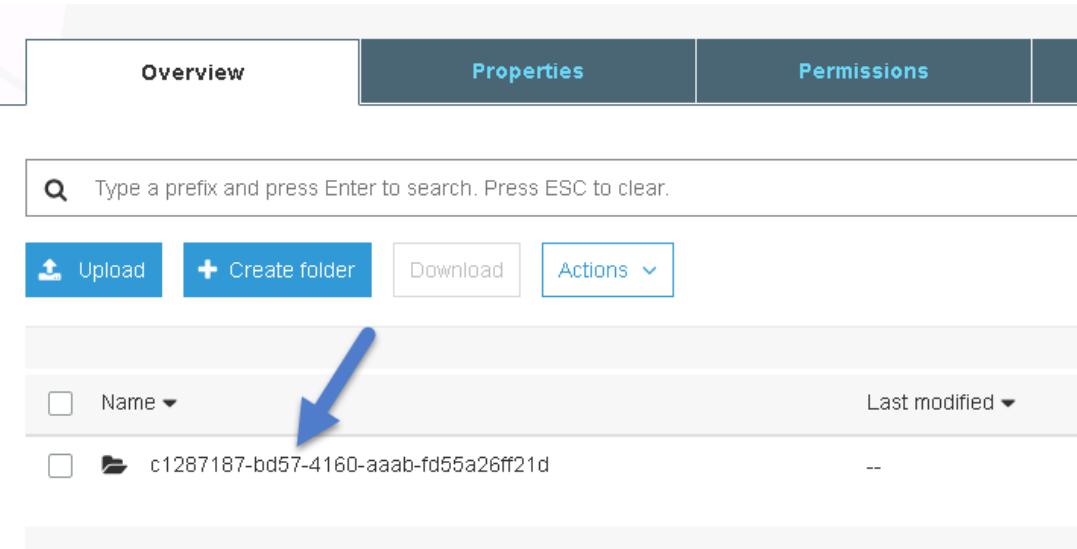
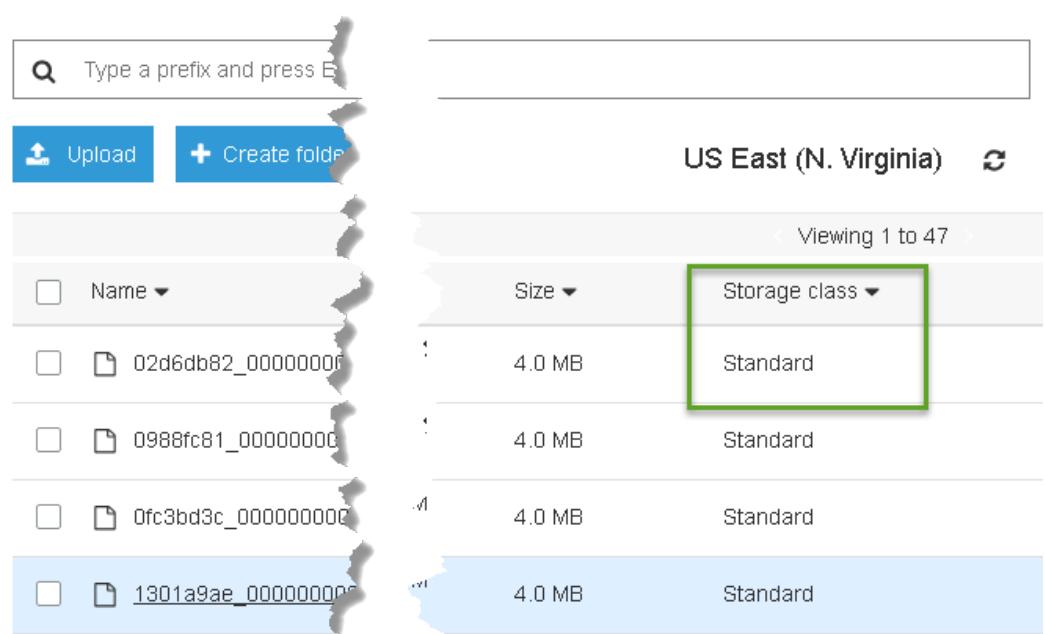
Task 1: Compare Space Allocation Between Tiering and Not Tiering

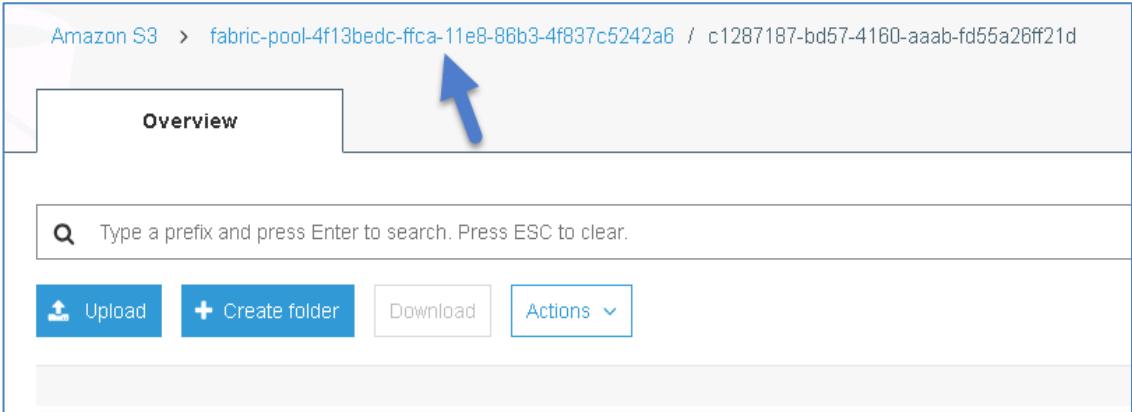
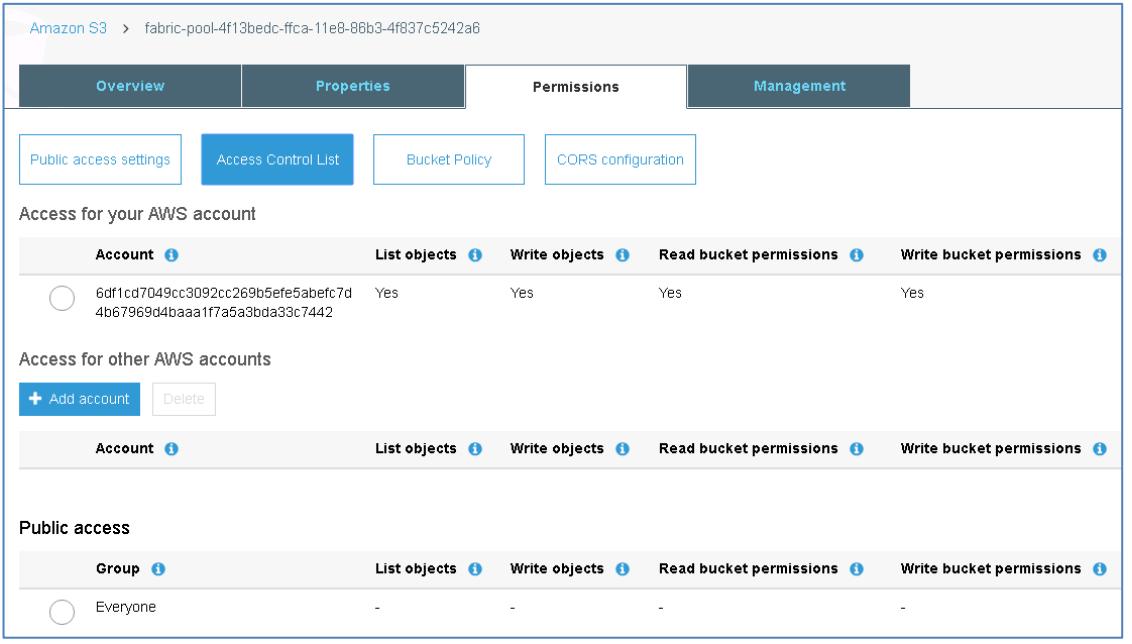
Step	Action
1-1	Return to Cloud Manager.
1-2	Enter the AWSCloudSVM working environment.
1-3	On the onPremSMB_CIFS_volume_copy, select Menu > Info . 

Step	Action														
1-4	<p>Note how much Amazon Elastic Block Store (Amazon EBS) data is used</p> <div data-bbox="295 192 1046 984"> <h3>Space Allocation</h3> <table> <tr> <td>Allocated Capacity:</td> <td>5 GB</td> </tr> <tr> <td>EBS Used Capacity:</td> <td>214.11 MB</td> </tr> <tr> <td>S3 Used Capacity:</td> <td>0 GB</td> </tr> <tr> <td>Maximum Growth Size:</td> <td>200 TB</td> </tr> </table> <h3>Storage Efficiency</h3> <table> <tr> <td>Thin Provisioning:</td> <td>Yes</td> </tr> <tr> <td>Compression Space Saved:</td> <td>2.89 MB</td> </tr> <tr> <td>Deduplication Space Saved:</td> <td>1.38 GB</td> </tr> </table> </div>	Allocated Capacity:	5 GB	EBS Used Capacity:	214.11 MB	S3 Used Capacity:	0 GB	Maximum Growth Size:	200 TB	Thin Provisioning:	Yes	Compression Space Saved:	2.89 MB	Deduplication Space Saved:	1.38 GB
Allocated Capacity:	5 GB														
EBS Used Capacity:	214.11 MB														
S3 Used Capacity:	0 GB														
Maximum Growth Size:	200 TB														
Thin Provisioning:	Yes														
Compression Space Saved:	2.89 MB														
Deduplication Space Saved:	1.38 GB														
1-5	<p>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.</p> <div data-bbox="295 1216 1421 1681">  <p>The screenshot shows a software interface for managing volumes. At the top, there's a volume icon and the name "onPremSMB_CIFS_volum...". Below it are several actions: "Clone", "Restore from Snapshot copy", "Create a Snapshot copy", "Info", "Edit", "Delete", "Mount Command", and "Change Disk Type & Tiering Policy". A tooltip for the "Change Disk Type & Tiering Policy" option displays the message "Data protection volume tier cannot be changed".</p> </div>														

Step	Action														
1-6	<p>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.</p> <p>Note: Follow the same data replication procedure as before, but remember to enable S3 tiering for this new relationship.</p> 														
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	<p>View the EBS Used Capacity and the S3 Used Capacity.</p> <p>Space Allocation</p> <table> <tbody> <tr> <td>Allocated Capacity:</td> <td>5 GB</td> </tr> <tr> <td>EBS Used Capacity:</td> <td>20.32 MB</td> </tr> <tr> <td>S3 Used Capacity:</td> <td>190.75 MB</td> </tr> <tr> <td>Maximum Growth Size:</td> <td>200 TB</td> </tr> </tbody> </table> <p>Storage Efficiency</p> <table> <tbody> <tr> <td>Thin Provisioning:</td> <td>Yes</td> </tr> <tr> <td>Compression Space Saved:</td> <td>2.94 MB</td> </tr> <tr> <td>Deduplication Space Saved:</td> <td>1.38 GB</td> </tr> </tbody> </table>	Allocated Capacity:	5 GB	EBS Used Capacity:	20.32 MB	S3 Used Capacity:	190.75 MB	Maximum Growth Size:	200 TB	Thin Provisioning:	Yes	Compression Space Saved:	2.94 MB	Deduplication Space Saved:	1.38 GB
Allocated Capacity:	5 GB														
EBS Used Capacity:	20.32 MB														
S3 Used Capacity:	190.75 MB														
Maximum Growth Size:	200 TB														
Thin Provisioning:	Yes														
Compression Space Saved:	2.94 MB														
Deduplication Space Saved:	1.38 GB														

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.

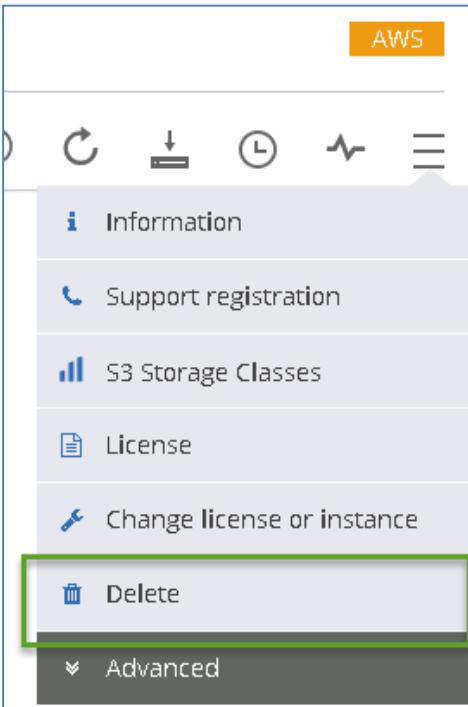
Step	Action															
1-16	<p>Click the folder.</p> 															
1-17	<p>Verify that all the objects are currently in the Standard storage class.</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>02d6db82_0000000f</td> <td>4.0 MB</td> <td>Standard</td> </tr> <tr> <td>0988fc81_00000000</td> <td>4.0 MB</td> <td>Standard</td> </tr> <tr> <td>0fc3bd3c_00000000</td> <td>4.0 MB</td> <td>Standard</td> </tr> <tr> <td>1301a9ae_00000000</td> <td>4.0 MB</td> <td>Standard</td> </tr> </tbody> </table>	Name	Size	Storage class	02d6db82_0000000f	4.0 MB	Standard	0988fc81_00000000	4.0 MB	Standard	0fc3bd3c_00000000	4.0 MB	Standard	1301a9ae_00000000	4.0 MB	Standard
Name	Size	Storage class														
02d6db82_0000000f	4.0 MB	Standard														
0988fc81_00000000	4.0 MB	Standard														
0fc3bd3c_00000000	4.0 MB	Standard														
1301a9ae_00000000	4.0 MB	Standard														

Step	Action																														
1-18	<p>At the top of the page, click the fabric-pool name in the path.</p> 																														
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.  <table border="1"> <caption>Access for your AWS account</caption> <thead> <tr> <th>Account</th> <th>List objects</th> <th>Write objects</th> <th>Read bucket permissions</th> <th>Write bucket permissions</th> </tr> </thead> <tbody> <tr> <td>6df1cd7049cc3092cc269b5efe5abefc7d 4b67969d4baaa1f7a5a3bda33c7442</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> </tbody> </table> <table border="1"> <caption>Access for other AWS accounts</caption> <thead> <tr> <th>Account</th> <th>List objects</th> <th>Write objects</th> <th>Read bucket permissions</th> <th>Write bucket permissions</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <caption>Public access</caption> <thead> <tr> <th>Group</th> <th>List objects</th> <th>Write objects</th> <th>Read bucket permissions</th> <th>Write bucket permissions</th> </tr> </thead> <tbody> <tr> <td>Everyone</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table>	Account	List objects	Write objects	Read bucket permissions	Write bucket permissions	6df1cd7049cc3092cc269b5efe5abefc7d 4b67969d4baaa1f7a5a3bda33c7442	Yes	Yes	Yes	Yes	Account	List objects	Write objects	Read bucket permissions	Write bucket permissions						Group	List objects	Write objects	Read bucket permissions	Write bucket permissions	Everyone	-	-	-	-
Account	List objects	Write objects	Read bucket permissions	Write bucket permissions																											
6df1cd7049cc3092cc269b5efe5abefc7d 4b67969d4baaa1f7a5a3bda33c7442	Yes	Yes	Yes	Yes																											
Account	List objects	Write objects	Read bucket permissions	Write bucket permissions																											
Group	List objects	Write objects	Read bucket permissions	Write bucket permissions																											
Everyone	-	-	-	-																											

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 .



The screenshot shows a portion of the AWS Cloud Manager interface. At the top, there's a toolbar with icons for refresh, download, support, clock, and more. Below the toolbar is a vertical menu. The menu items are: Information, Support registration, S3 Storage Classes, License, Change license or instance, Delete, and Advanced. The 'Delete' option is highlighted with a green rectangular box around its icon and text.

Step	Action
2-4	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Delete 'AWSCloudSVM' Working Environment</p> <p>Disks & Snapshots All disks and Snapshots associated with this working environment will be permanently deleted.</p> <p>Active Replication All active data replication relationships for this working environment will be deleted.</p> <hr/> <p>Type the name of the working environment in order to delete it.</p> <p>Working Environment Name</p> <input type="text" value="AWSCloudSVM"/> <p><input checked="" type="checkbox"/> Delete this working environment even though it has an active data replication relationship.</p> <div style="text-align: right; margin-top: 10px;"> Delete Cancel </div> </div>
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.

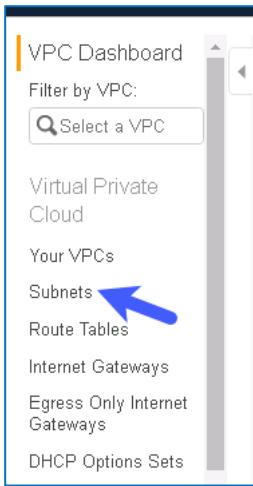
Objectives

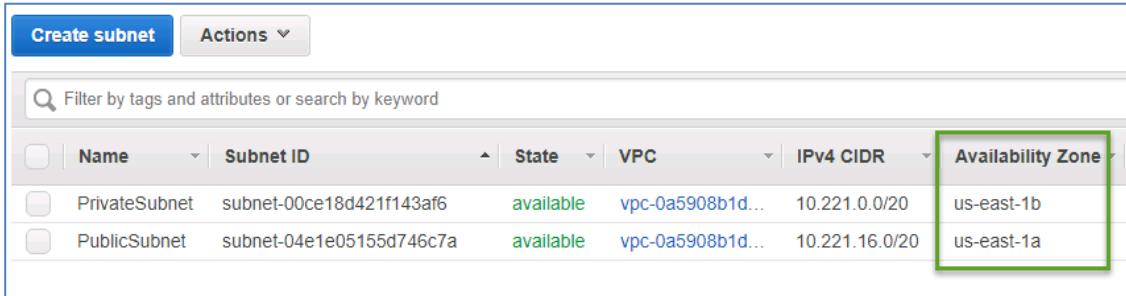
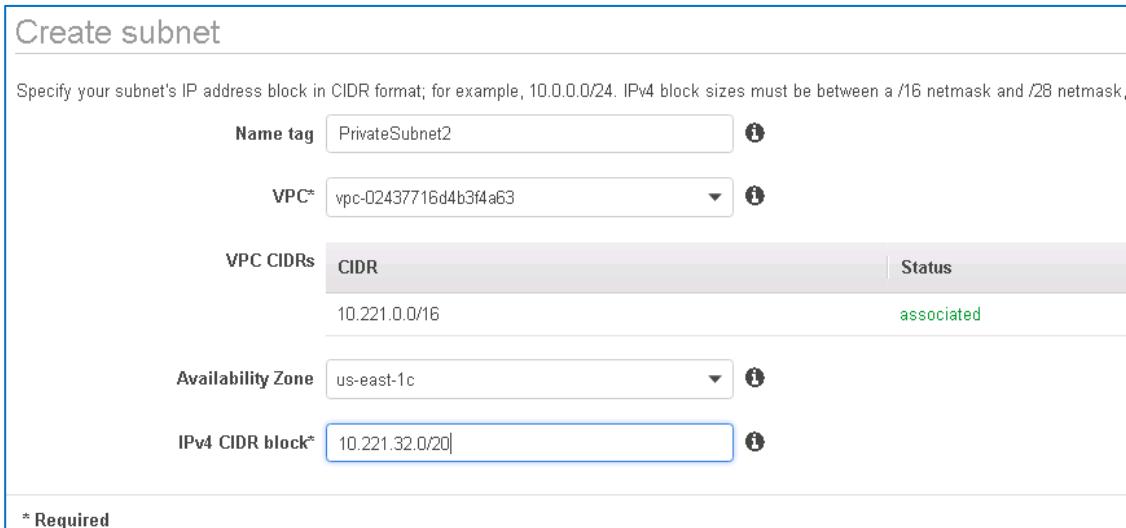
This exercise focuses on enabling you to do the following:

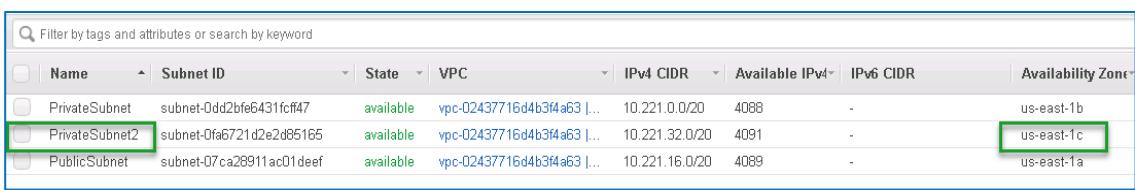
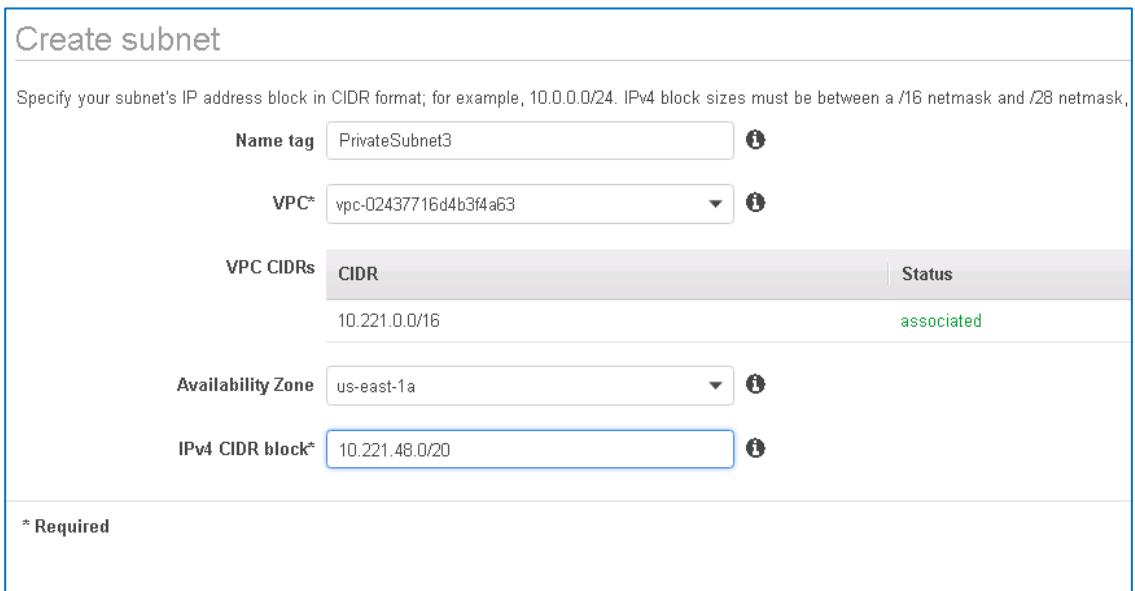
- Deploy Cloud Volumes ONTAP in HA mode by using Cloud Manager
- Use floating IPs and deploy the Cloud Volumes ONTAP high availability in multiple Availability Zones (AZs)
- Perform a failover and fallback and verify that client access to data continues with the same data LIF

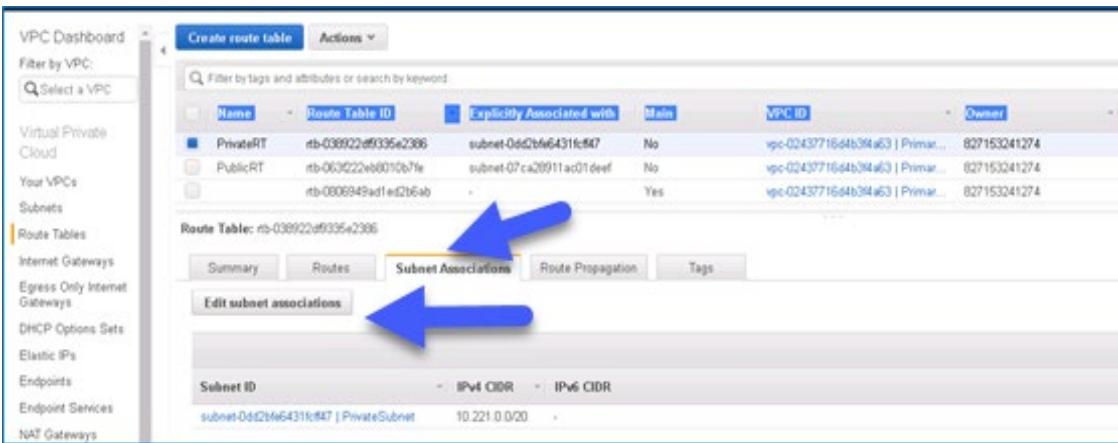
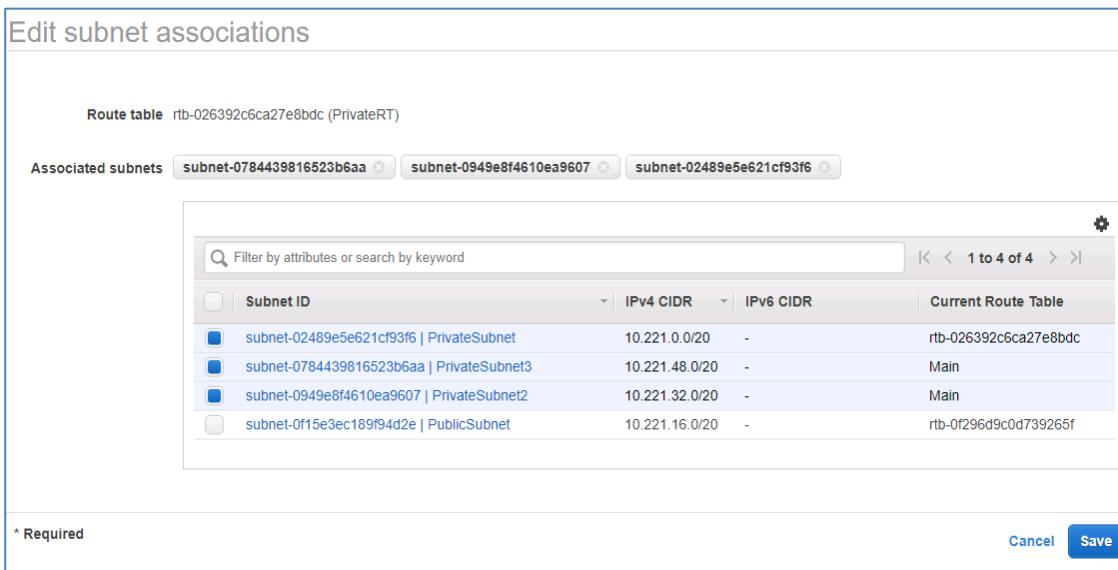
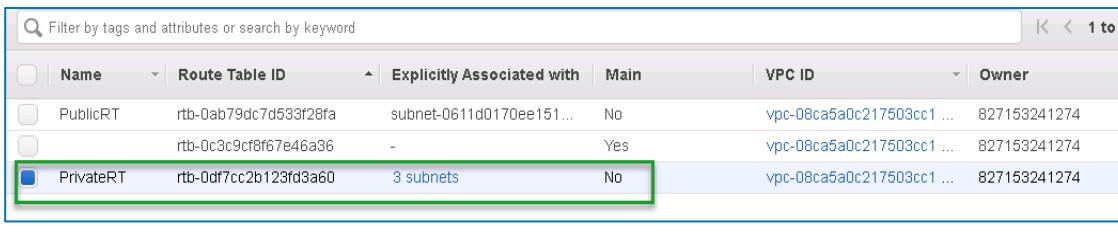
Task 1: Create Additional Subnets to Deploy HA Nodes of Cloud Volumes ONTAP

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 . 

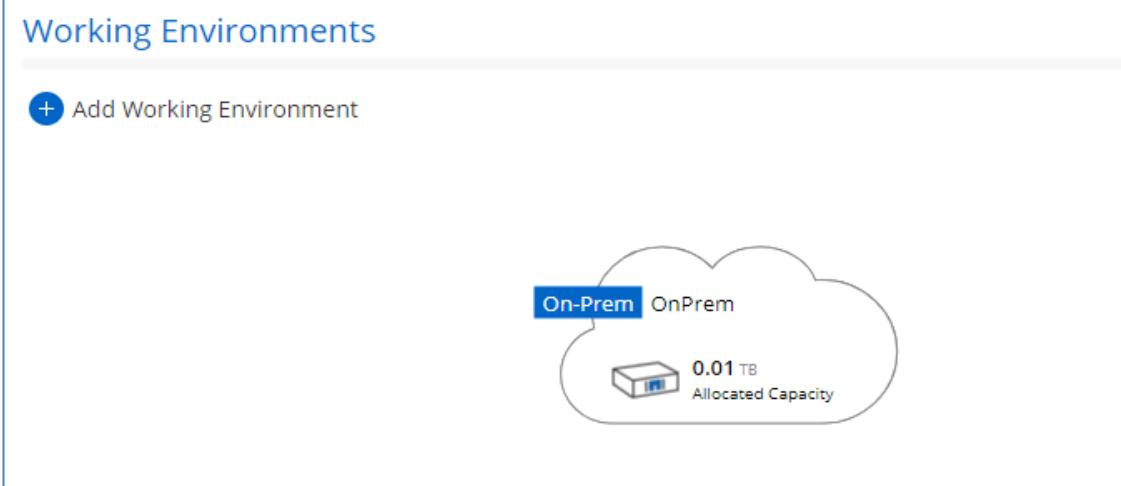
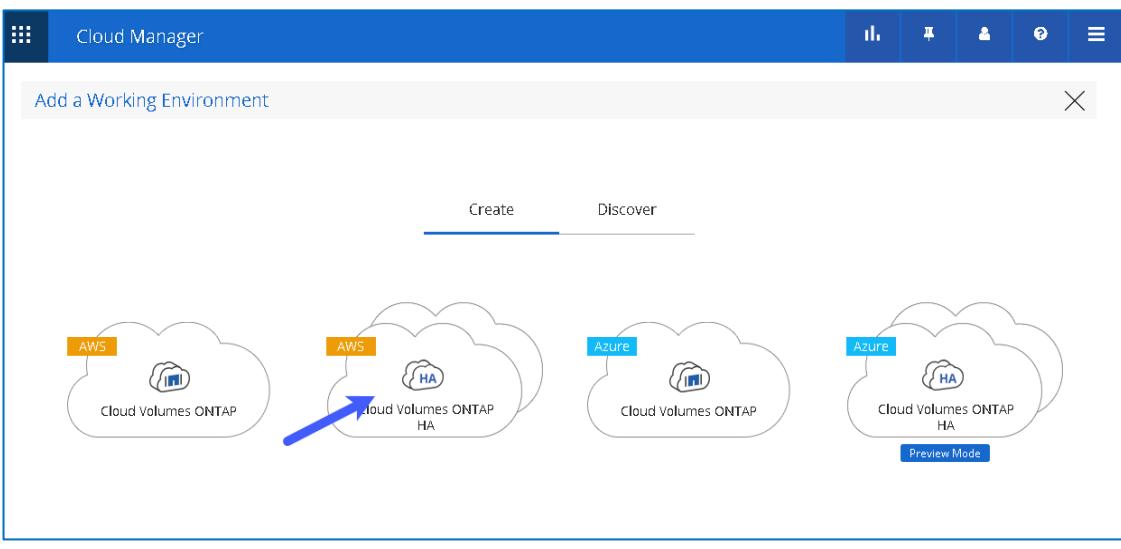
Step	Action
1-3	<p>Record the Availability Zones being used by your subnets, PrivateSubnet and PublicSubnet.</p> <p>PrivateSubnet: _____</p> <p>PublicSubnet: _____</p> 
1-4	<p>Click Create Subnet and configure the following information:</p> <ul style="list-style-type: none"> ▪ Name tag: PrivateSubnet2 ▪ 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 .

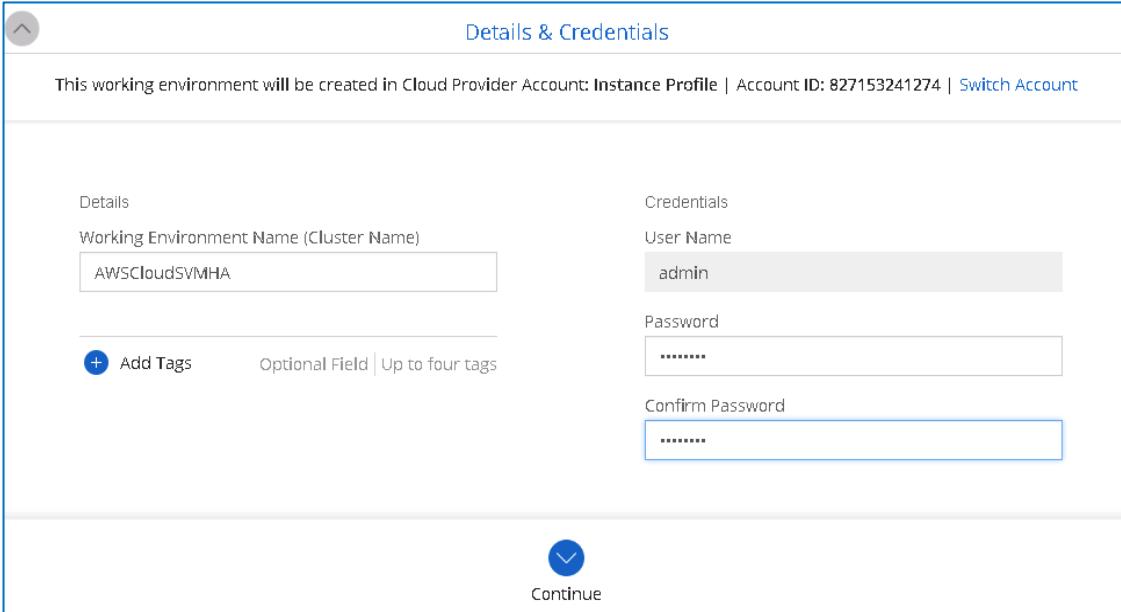
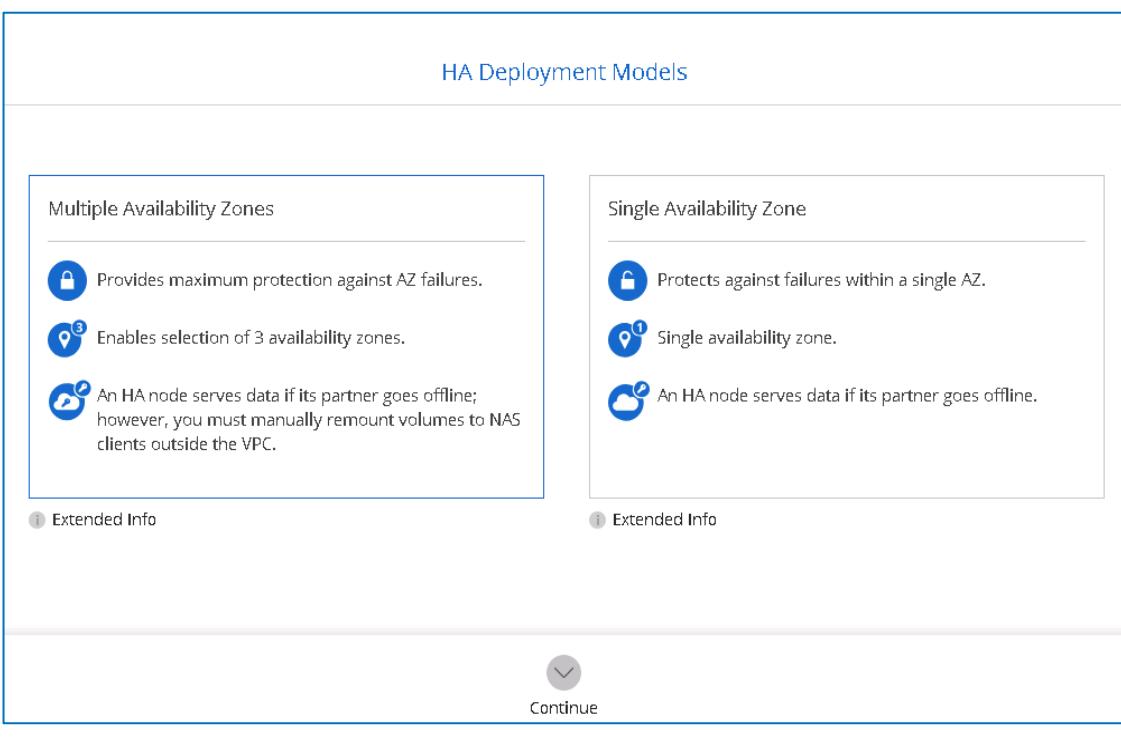
Step	Action
1-7	<p>Verify that the private subnet was created in an AZ that is unique from the AZs of the other subnets in your Primary VPC.</p> 
1-8	<p>Create another subnet, and configure the following information:</p> <ul style="list-style-type: none"> ▪ Name tag: PrivateSubnet3 ▪ VPC: PrimaryVPC ▪ Availability Zone: Choose the same AZ as your PublicSubnet. ▪ IPv4 CIDR block: 10.221.48.0/20 
1-9	<p>Verify that you have three private subnets in three different AZs.</p> 
1-10	<p>In the VPC Dashboard, click Route Tables, and then select the PrivateRT.</p>

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.
	

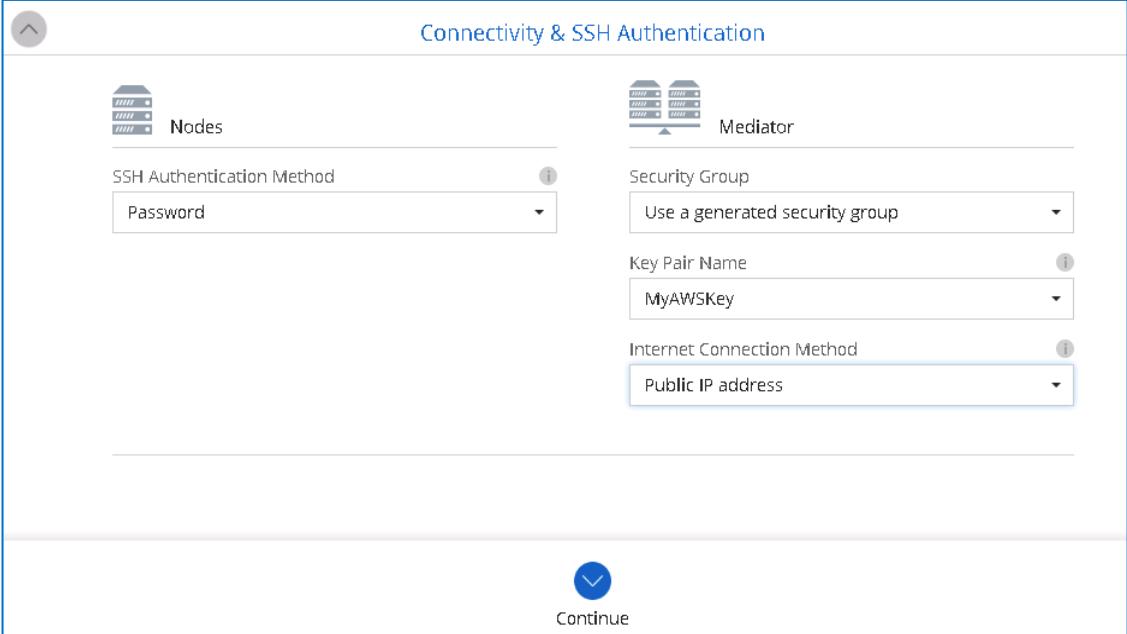
Task 2: Deploy Cloud Volumes ONTAP High Availability

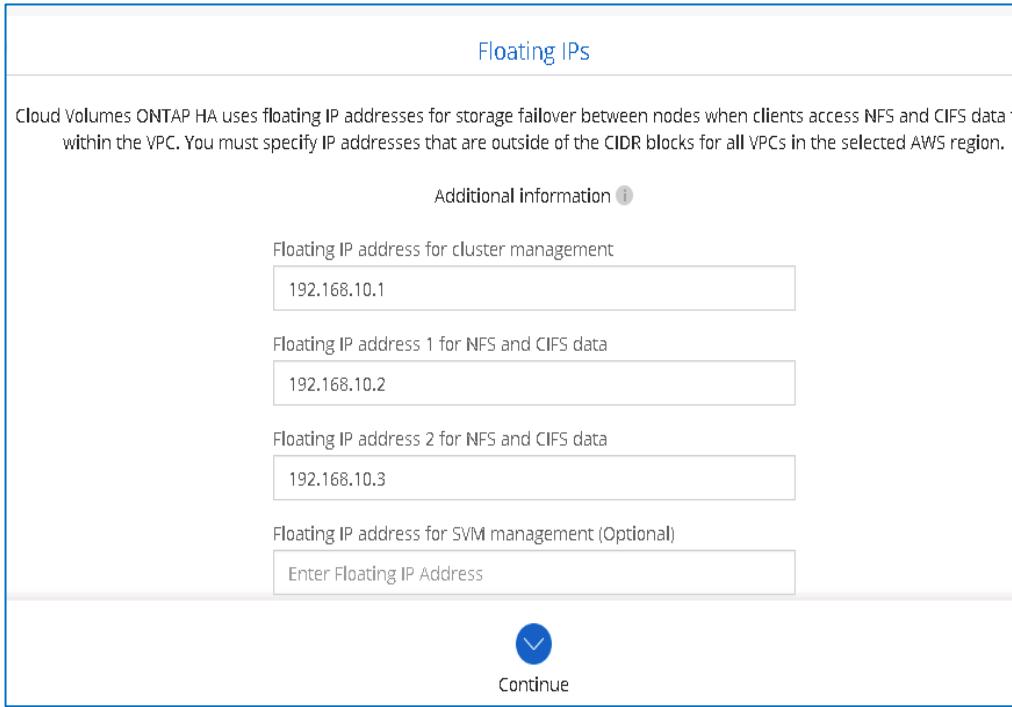
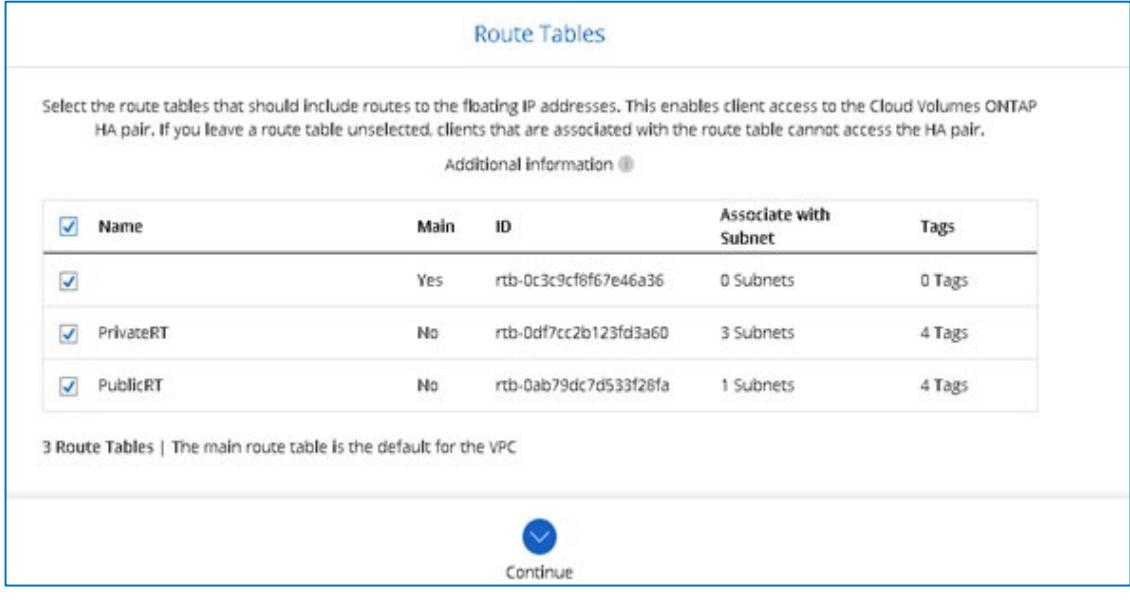
In this task, you use Cloud Manager to deploy Cloud Volumes ONTAP high availability in multiple AZs.

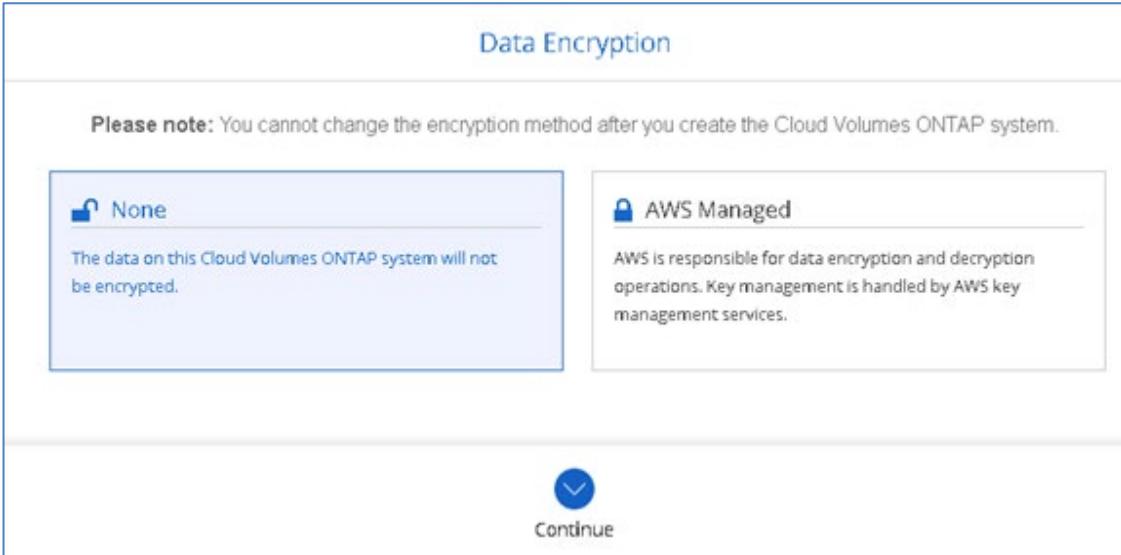
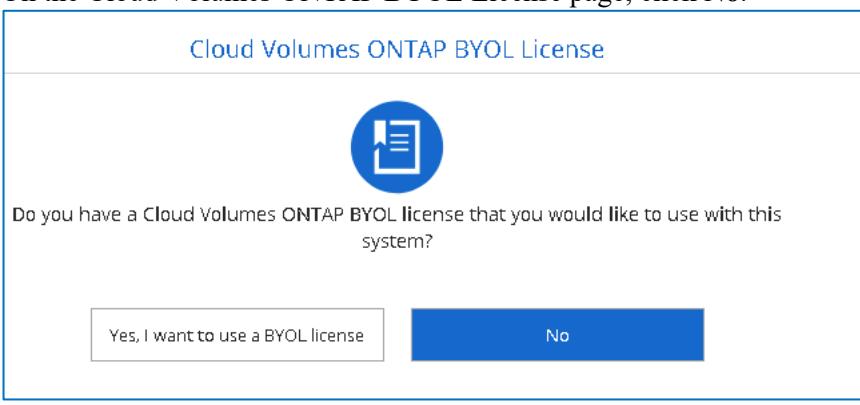
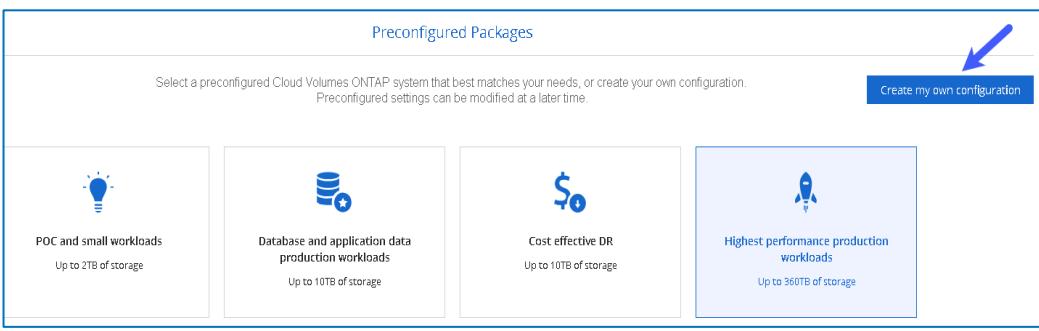
Step	Action
2-1	Return to the Cloud Manager interface on your browser.
2-2	Click Add Working Environment .
	
2-3	In the Add a Working Environment page, click Create , and select Cloud Volumes ONTAP HA .
	

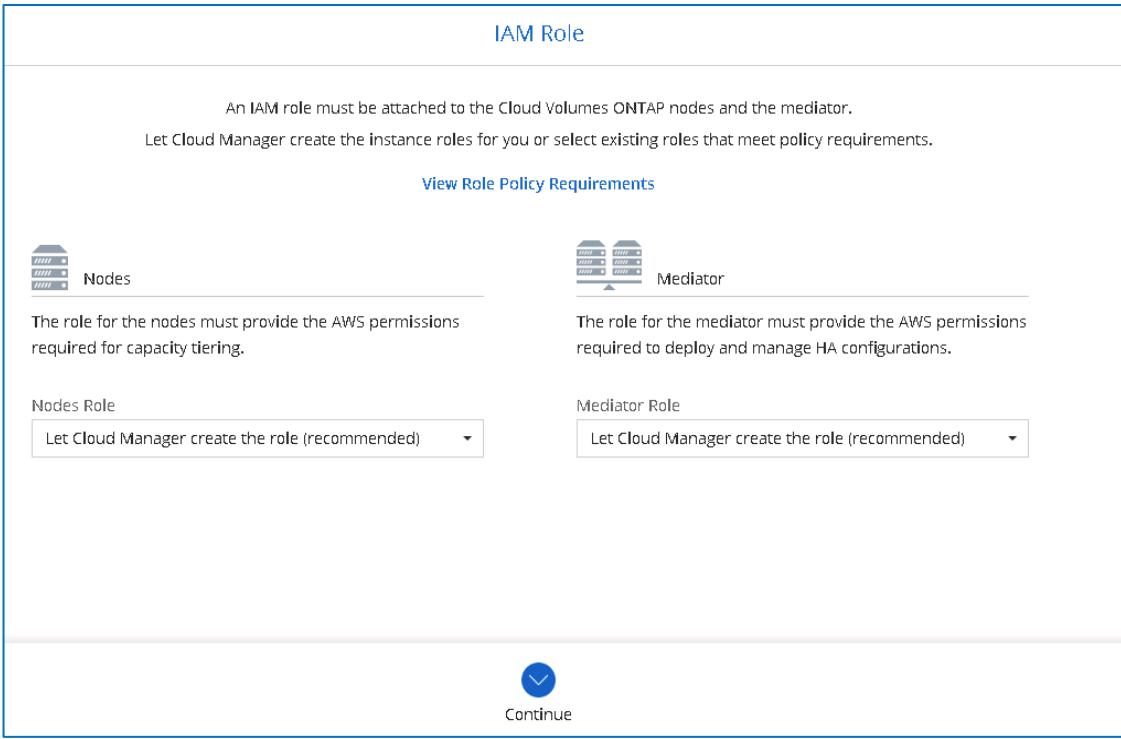
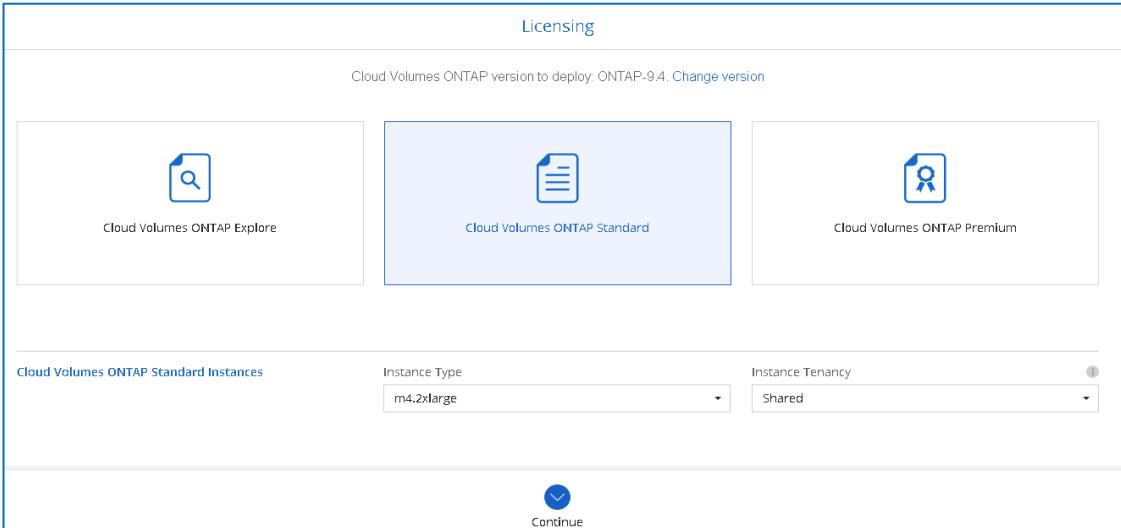
Step	Action
2-4	<p>On the Details & Credentials page, enter the following, and then click Continue.</p> <ul style="list-style-type: none"> ▪ Working Environment Name: AWSCloudSVMHA ▪ Password: Netapp1! ▪ Confirm Password: Netapp1! 
2-5	<p>In the HA Deployment Models Page, click Multiple Availability Zones, and then click Continue.</p> 

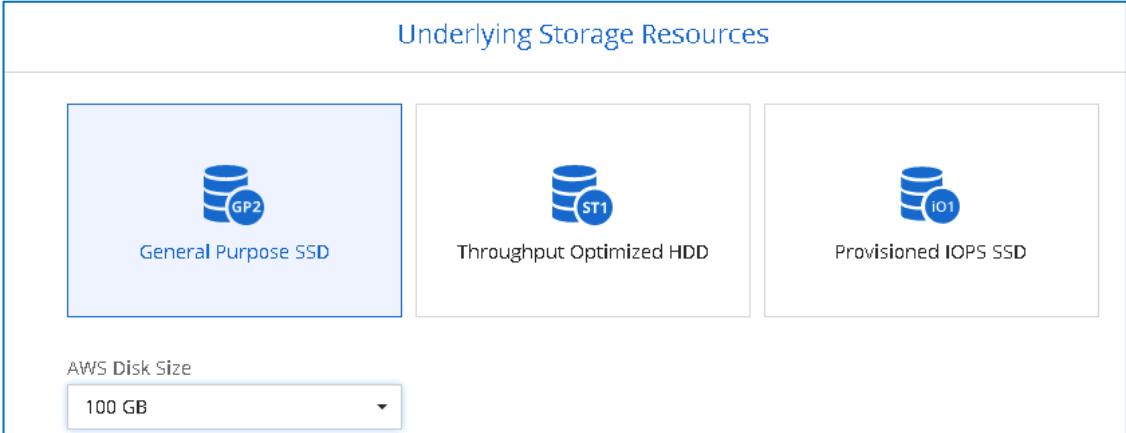
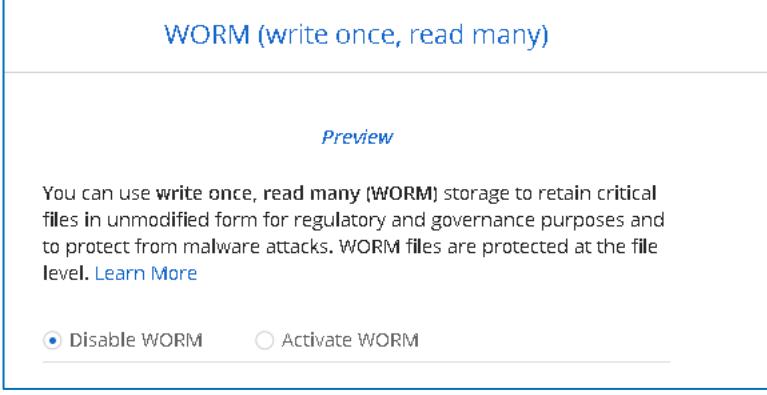
Step	Action
2-6	<p>On the Region and VPC page, enter the following values and then click Continue.</p> <ul style="list-style-type: none"> AWS Region: US East N.Virginia VPC: PrimaryVPC Security group: Use a generated security group Place Node 1, Node 2, and Mediator in the subnets below. Your exact AZs may be different from those AZs in this example, but they should all be unique. <ul style="list-style-type: none"> Node 1: <ul style="list-style-type: none"> Availability zone: us-east-1b Subnet: PrivateSubnet Node 2: <ul style="list-style-type: none"> Availability zone: us-east-1c Subnet: PrivateSubnet2 Mediator: <ul style="list-style-type: none"> Availability zone: us-east-1a Subnet: PrivateSubnet3

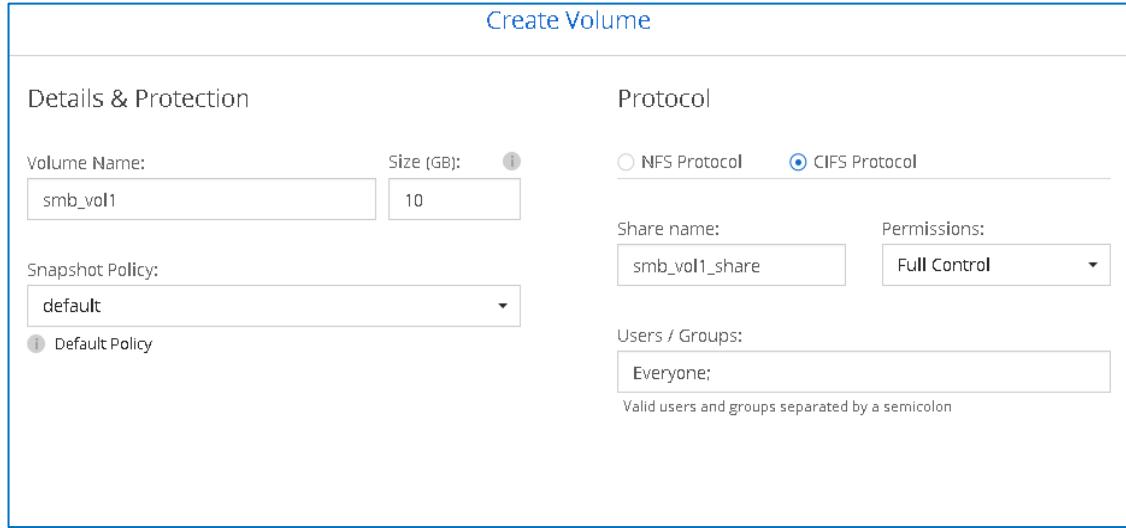
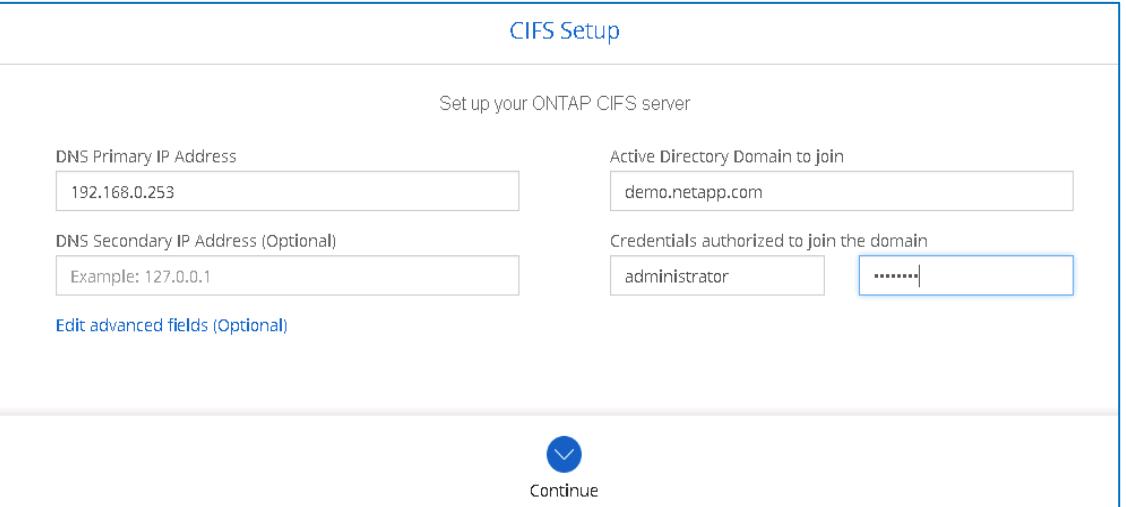
Step	Action
2-7	<p>On the Connectivity & SSH Authentication page, use the following values, and then click Continue:</p> <ul style="list-style-type: none"> ▪ SSH Authentication Method: Password ▪ Security Group: Use a generated security group ▪ Key Pair Name: MyAWSKey ▪ Internet Connection Method: Public IP address 

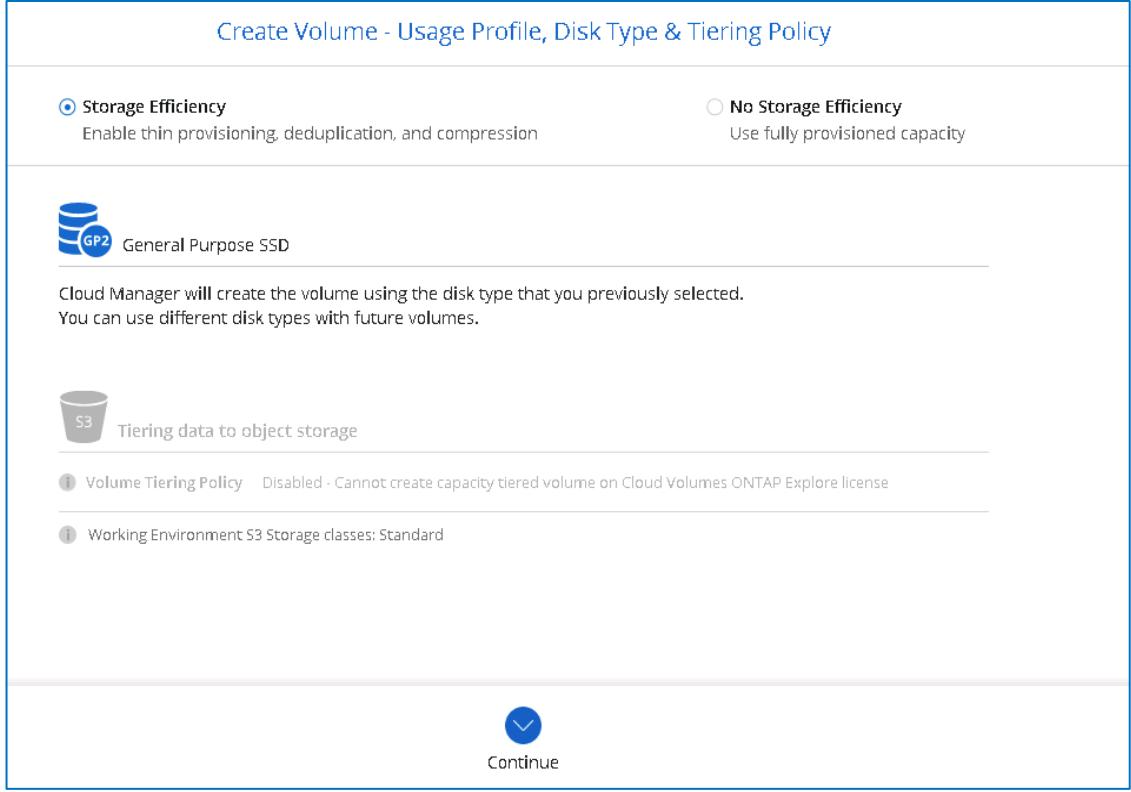
Step	Action																								
2-8	<p>On the Floating IPs page, provide the following floating IPs, and then click Continue:</p> <ul style="list-style-type: none"> Floating IP for cluster management: 192.168.10.1 Floating IP address 1 for NFS and CIFS data: 192.168.10.2 Floating IP address 2 for NFS and CIFS data: 192.168.10.3 																								
2-9	<p>On the Route Tables page, select the checkboxes for all three route tables, and then click Continue.</p>  <table border="1"> <thead> <tr> <th><input checked="" type="checkbox"/></th> <th>Name</th> <th>Main</th> <th>ID</th> <th>Associate with Subnet</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>Yes</td> <td>rtb-0c3c9cf8f67e46a36</td> <td>0 Subnets</td> <td>0 Tags</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>PrivateRT</td> <td>No</td> <td>rtb-0df7cc2b123fd3a60</td> <td>3 Subnets</td> <td>4 Tags</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>PublicRT</td> <td>No</td> <td>rtb-0ab79dc7d533f28fa</td> <td>1 Subnets</td> <td>4 Tags</td> </tr> </tbody> </table> <p>3 Route Tables The main route table is the default for the VPC</p>	<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags	<input checked="" type="checkbox"/>		Yes	rtb-0c3c9cf8f67e46a36	0 Subnets	0 Tags	<input checked="" type="checkbox"/>	PrivateRT	No	rtb-0df7cc2b123fd3a60	3 Subnets	4 Tags	<input checked="" type="checkbox"/>	PublicRT	No	rtb-0ab79dc7d533f28fa	1 Subnets	4 Tags
<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags																				
<input checked="" type="checkbox"/>		Yes	rtb-0c3c9cf8f67e46a36	0 Subnets	0 Tags																				
<input checked="" type="checkbox"/>	PrivateRT	No	rtb-0df7cc2b123fd3a60	3 Subnets	4 Tags																				
<input checked="" type="checkbox"/>	PublicRT	No	rtb-0ab79dc7d533f28fa	1 Subnets	4 Tags																				

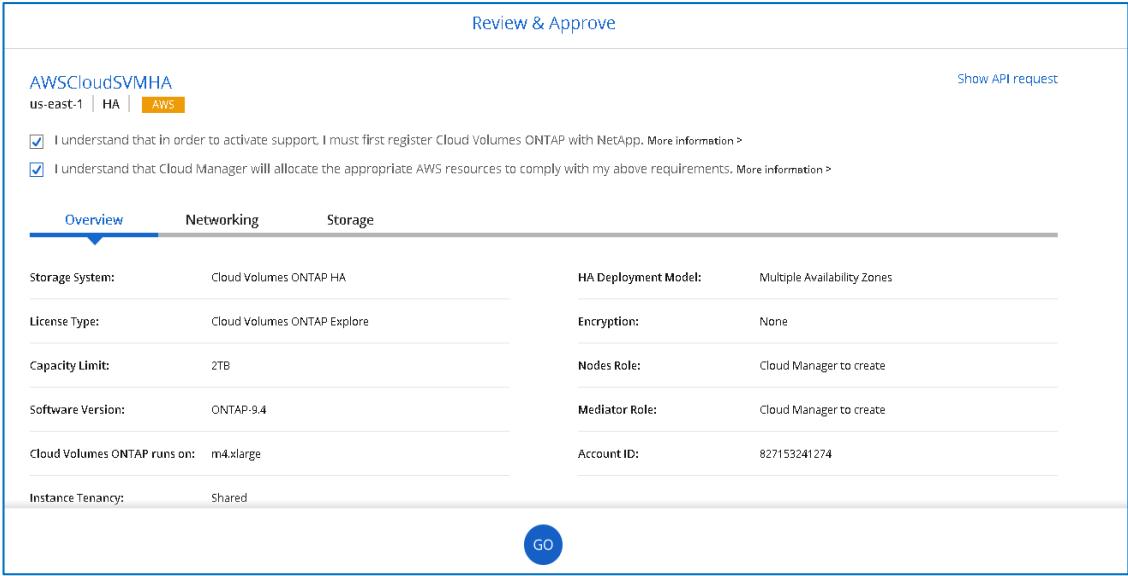
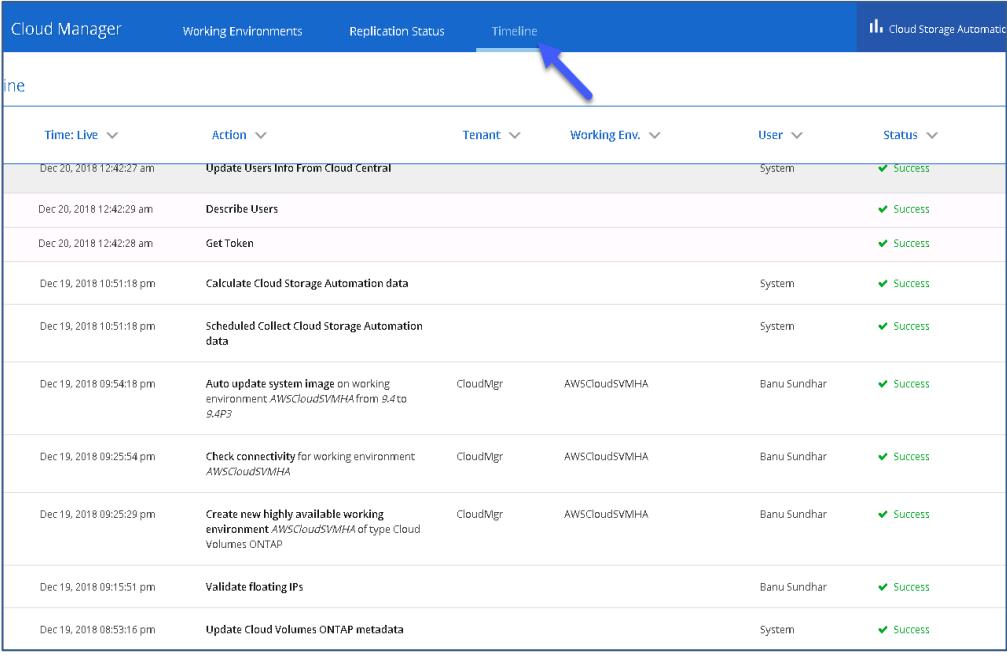
Step	Action
2-10	<p>In the Data Encryption Page, select None, and then click Continue.</p>  <p>The screenshot shows the 'Data Encryption' page. It contains two options: 'None' and 'AWS Managed'. The 'None' option is selected, indicated by a blue outline around its icon and text. A note below says: 'The data on this Cloud Volumes ONTAP system will not be encrypted.' The 'AWS Managed' option is also shown with its own description: 'AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.' At the bottom is a 'Continue' button with a downward arrow icon.</p>
2-11	<p>On the Cloud Volumes ONTAP BYOL License page, click No.</p>  <p>The screenshot shows the 'Cloud Volumes ONTAP BYOL License' page. It features a question icon and the text: 'Do you have a Cloud Volumes ONTAP BYOL license that you would like to use with this system?'. Below the question are two buttons: 'Yes, I want to use a BYOL license' and a larger blue 'No' button. The 'No' button is highlighted with a blue arrow pointing to it.</p>
2-12	<p>On the Preconfigured Packages page, click Create my own configuration.</p>  <p>The screenshot shows the 'Preconfigured Packages' page. It displays four package options: 'POC and small workloads' (Up to 2TB of storage), 'Database and application data production workloads' (Up to 10TB of storage), 'Cost effective DR' (Up to 10TB of storage), and 'Highest performance production workloads' (Up to 360TB of storage). To the right of the packages is a blue button labeled 'Create my own configuration', which is highlighted with a blue arrow pointing to it.</p>

Step	Action
2-13	<p>On the IAM Role page, leave the default recommendation, Let Cloud Manager create the role, and then click Continue.</p> 
2-14	<p>On the Licensing page, configure the following information and then click Continue.</p> <ol style="list-style-type: none"> Click Change Version and select ONTAP-9.5 from the list. Click Cloud Volumes ONTAP Standard. Select instance type m4.2xlarge. 
2-15	<p>On the NetApp Support site credentials page, leave all the fields blank, and then click Continue.</p>

Step	Action
2-16	<p>On the Underlying Storage Resources page, select the following, and then click Continue.</p> <ul style="list-style-type: none"> ▪ Select General Purpose SSD. ▪ AWS Disk Size: Select 100 GB from the list. 
2-17	<p>On the WORM page, select Disable WORM, and then click Continue.</p> 

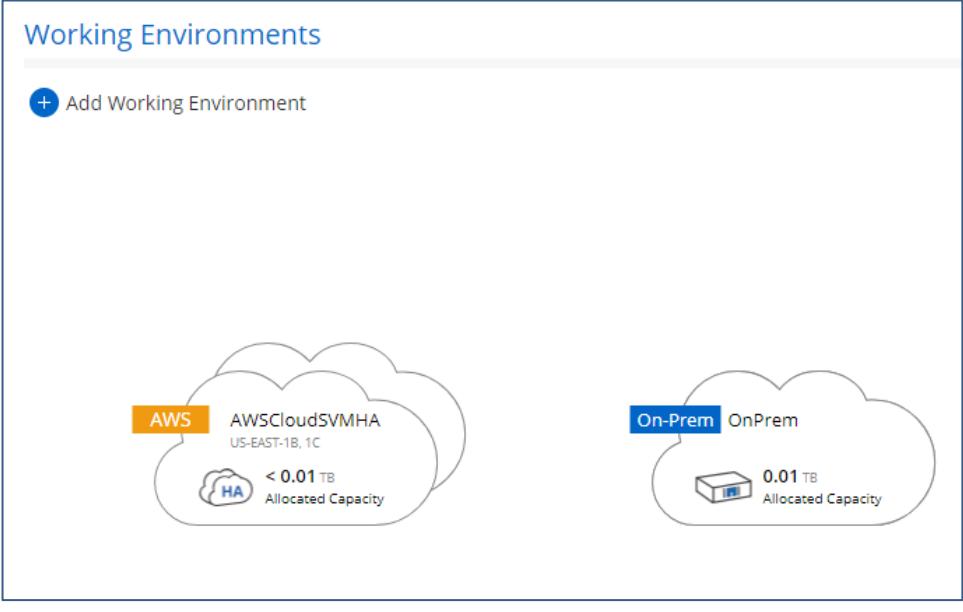
Step	Action
2-18	<p>On the Create Volume page, configure the following, and then click Continue.</p> <ul style="list-style-type: none"> Volume Name: smb_vol1 Size: 10 Protocol: CIFS Protocol Leave all other values as the defaults. 
2-19	<p>On the CIFS Setup page, enter the following values, and then click Continue.</p> <ul style="list-style-type: none"> 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! 

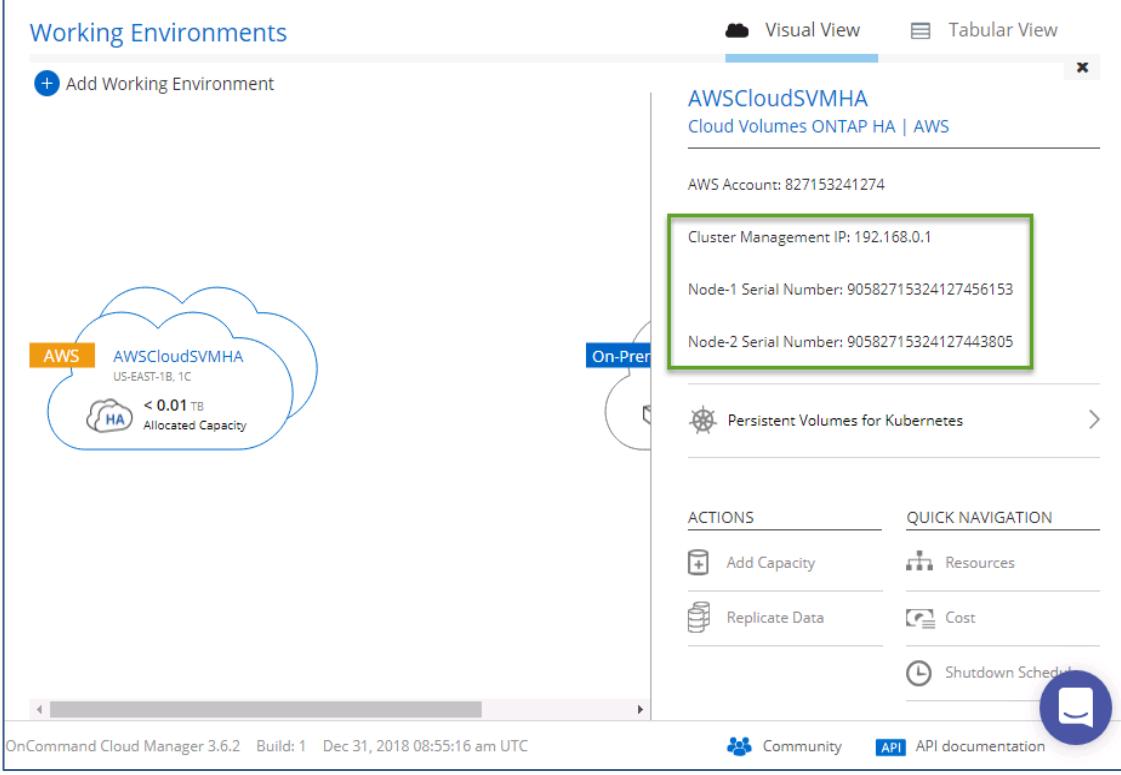
Step	Action
2-20	<p>On the Create Volume – Usage Profile, Disk Type & Tiering Policy page, select Storage Efficiency, and then click Continue.</p> 

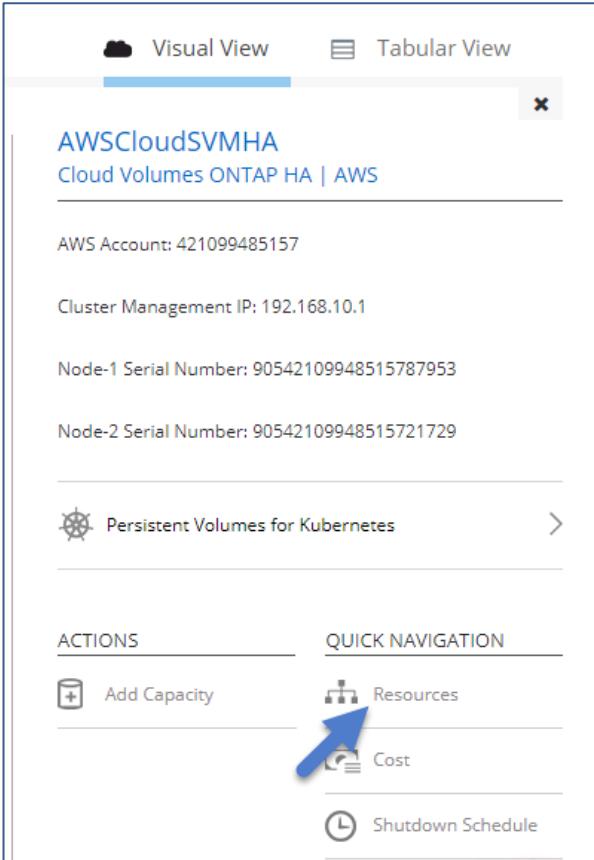
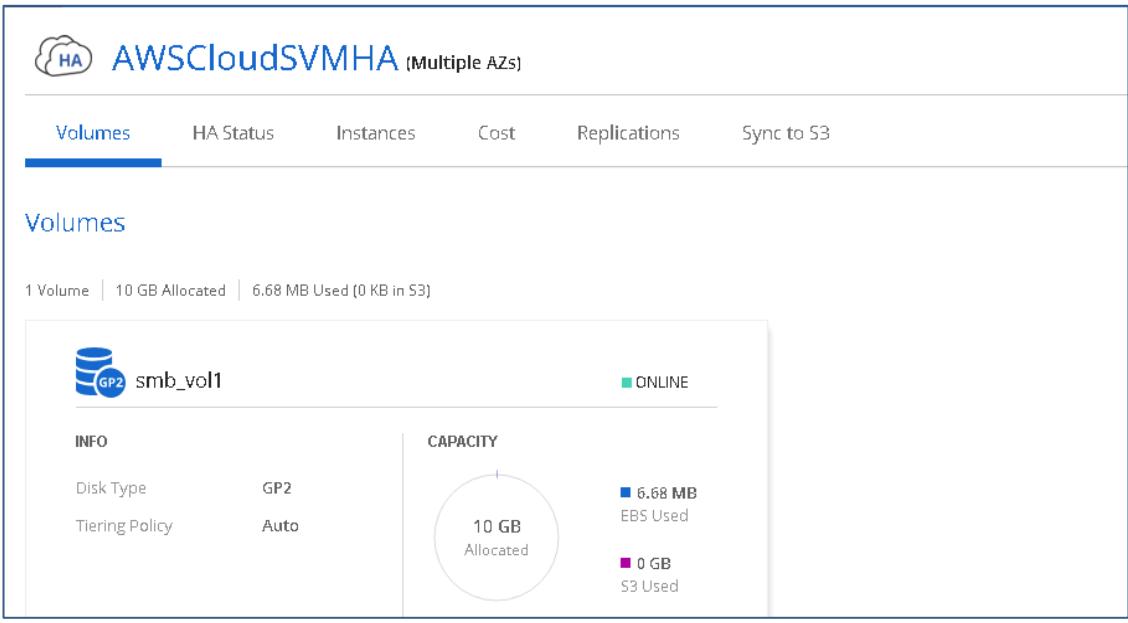
Step	Action
2-21	<p>On the Review & Approve page, review the information, and then complete the following actions:</p> <ol style="list-style-type: none"> Select the two checkboxes <ul style="list-style-type: none"> I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. 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. 

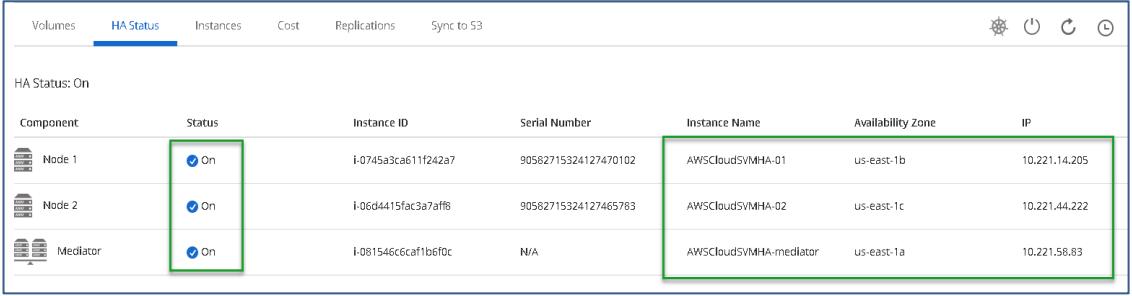
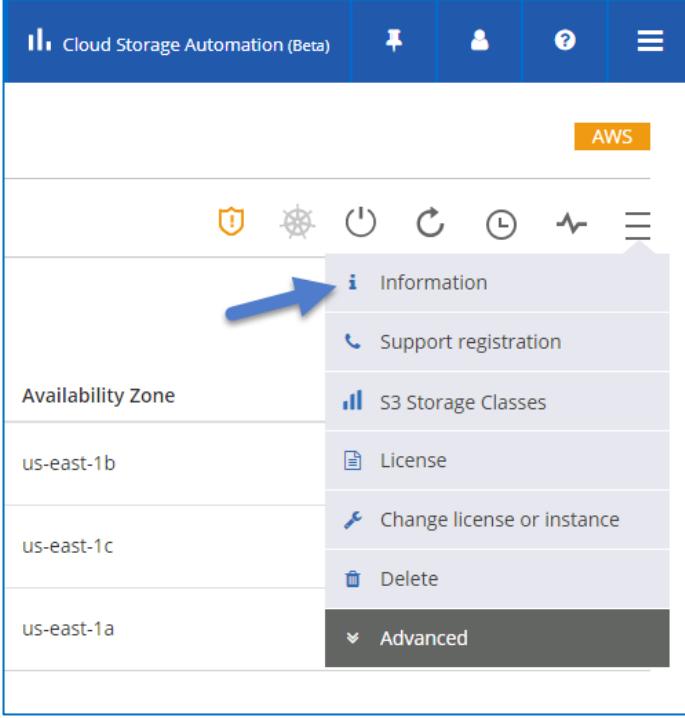
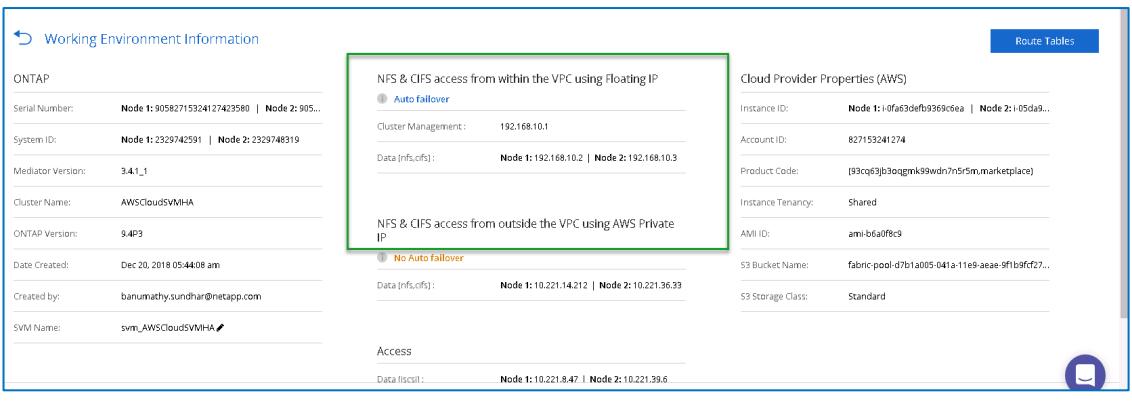
Task 3: Review the Cloud Volumes ONTAP High Availability by Using Cloud Manager

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.  <p>The screenshot shows the 'Working Environments' section of the Cloud Manager interface. It displays two environment entries:</p> <ul style="list-style-type: none">AWSCloudSVMHA (AWS): Located in US-EAST-1B, 1C. It has an HA icon and shows an allocated capacity of < 0.01 TB.OnPrem: Shows an allocated capacity of 0.01 TB.

Step	Action
3-3	<p>Click the AWSCloud image in the browser to see the cluster management IP and the node serial numbers on the right.</p>  <p>The screenshot shows the 'Working Environments' section of the OnCommand Cloud Manager. On the left, there's a cloud icon labeled 'AWSCloudSVMHA US-EAST-1B, 1C' with 'HA' and 'Allocated Capacity < 0.01 TB'. On the right, a detailed view for 'AWSCloudSVMHA' is shown under 'Cloud Volumes ONTAP HA AWS'. It displays the 'AWS Account: 827153241274' and three main sections: 'Cluster Management IP: 192.168.0.1', 'Node-1 Serial Number: 90582715324127456153', and 'Node-2 Serial Number: 90582715324127443805'. A green box highlights the cluster management IP and both node serial numbers. Below this, there are sections for 'Persistent Volumes for Kubernetes' and 'Actions' like 'Add Capacity' and 'Replicate Data'. At the bottom, it shows the build information 'OnCommand Cloud Manager 3.6.2 Build: 1 Dec 31, 2018 08:55:16 am UTC' and links for 'Community' and 'API documentation'.</p>

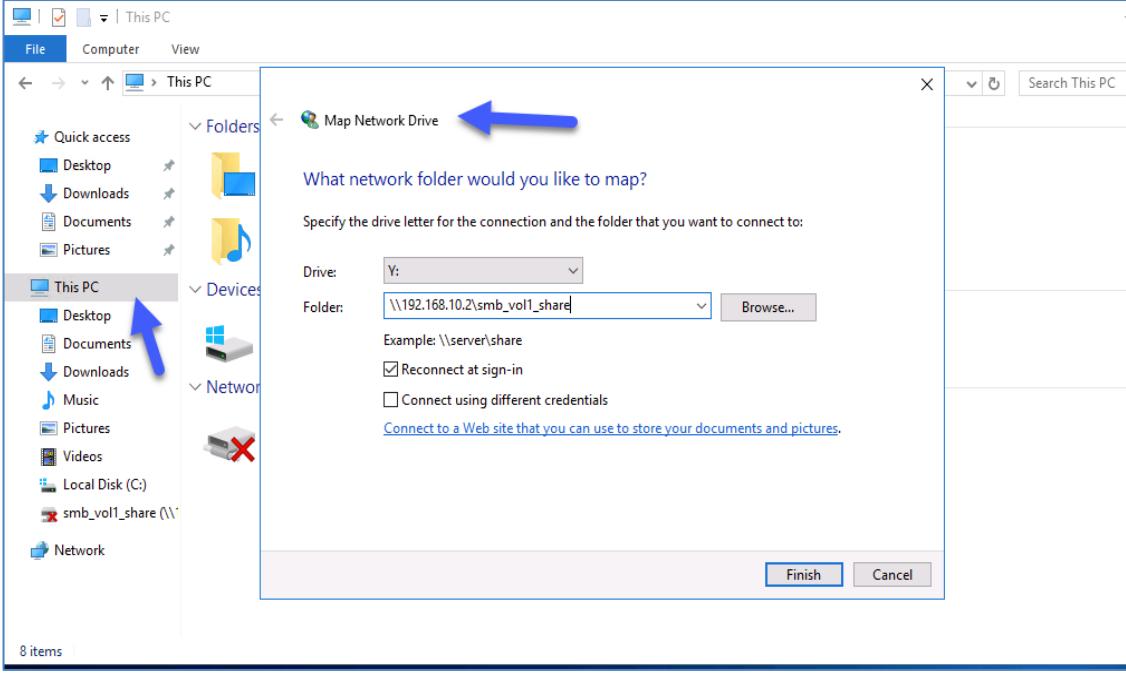
Step	Action
3-4	<p>Under QUICK NAVIGATION, click Resources.</p> 
3-5	<p>Verify that you see the Volumes information.</p> 

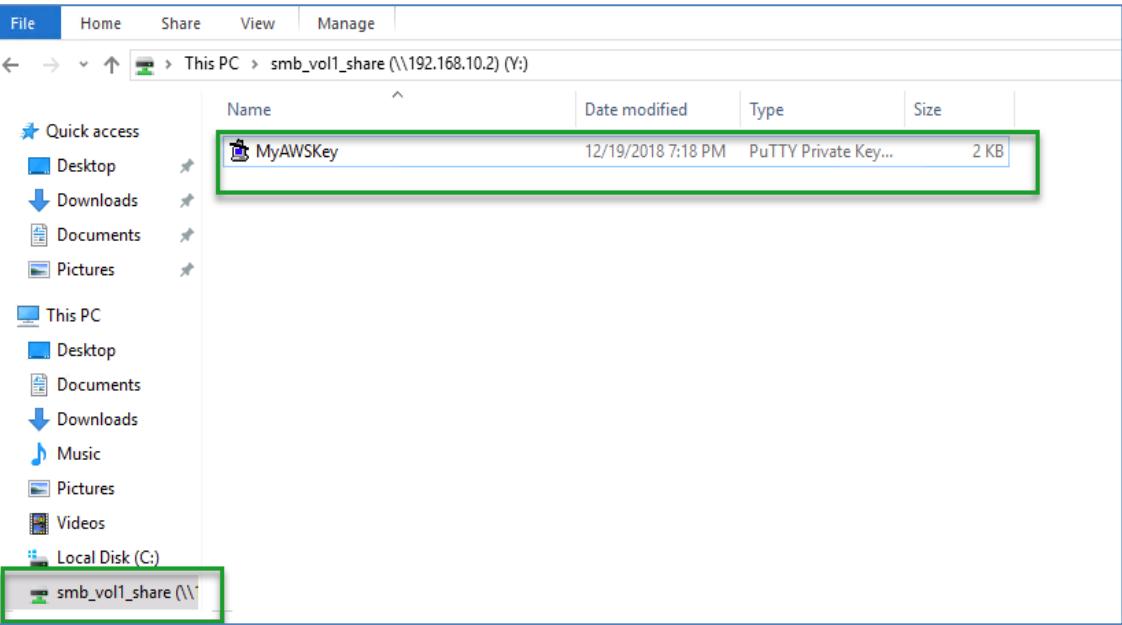
Step	Action
3-6	Click HA Status and review the information about the HA nodes and the mediator node.
	
3-7	Click the menu icon with 3 bars on the far right, and then click Information.
	
3-8	Review all information in the Working Environment Information page and pay attention to the NFS & CIFS access 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

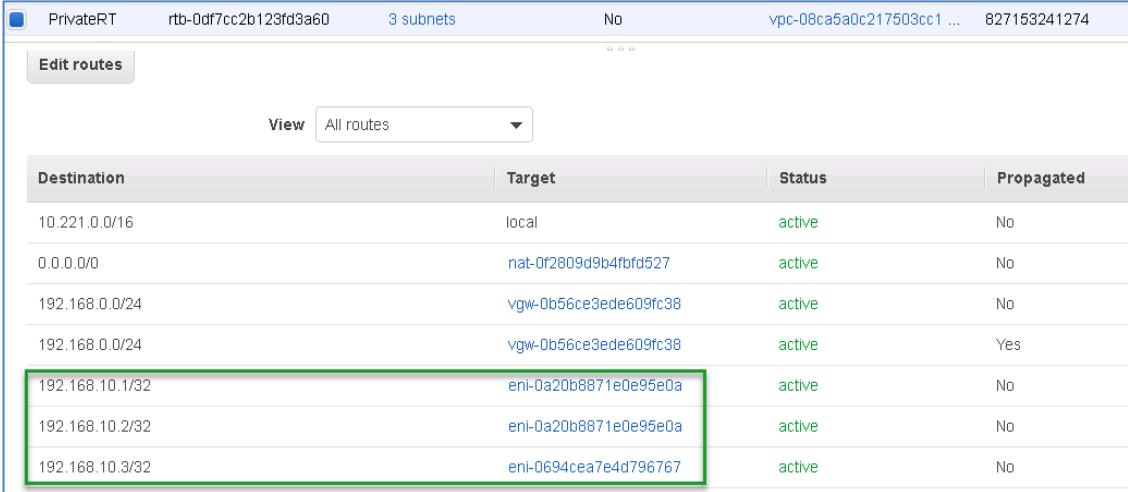
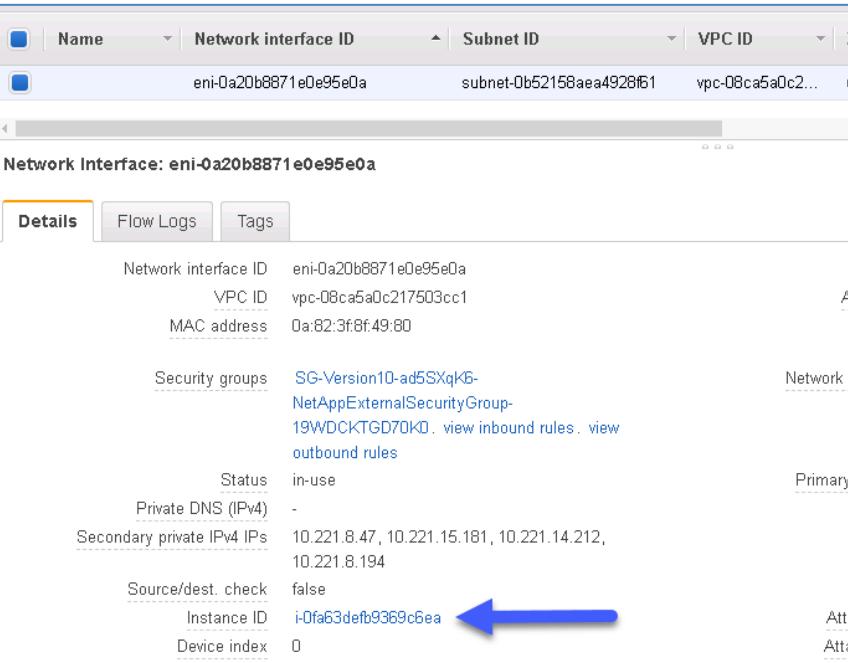
In this task, you connect an SMB client to the SMB volume in your Cloud Volumes ONTAP high availability and write data into it.

Step	Action
4-1	<p> 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.</p>
4-2	<p>If you have disconnected from your Win2k16_Public, reconnect to it by using Remote Desktop Protocol (RDP) from your jump host.</p> <p>Note: The public IP, user name, and password are in the Win2k16_Public_Login.txt file in the CourseFiles folder.</p>
4-3	<p>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:</p> <ul style="list-style-type: none">▪ Folder: \\\192.168.10.2\smb_vol1_share▪ User name: Demo\Administrator▪ Password: Netapp1! 

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

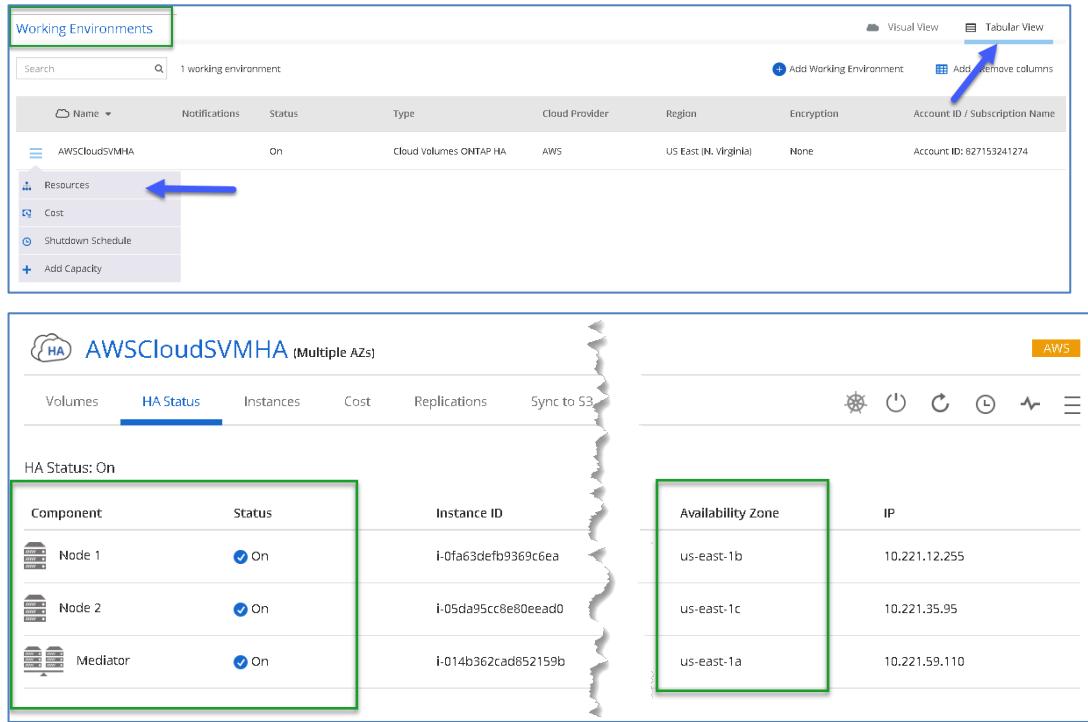
Task 5: Review the Routes in AWS

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.

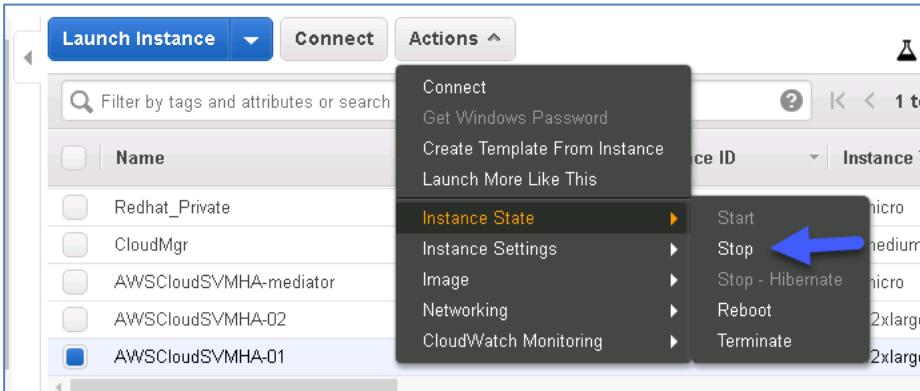
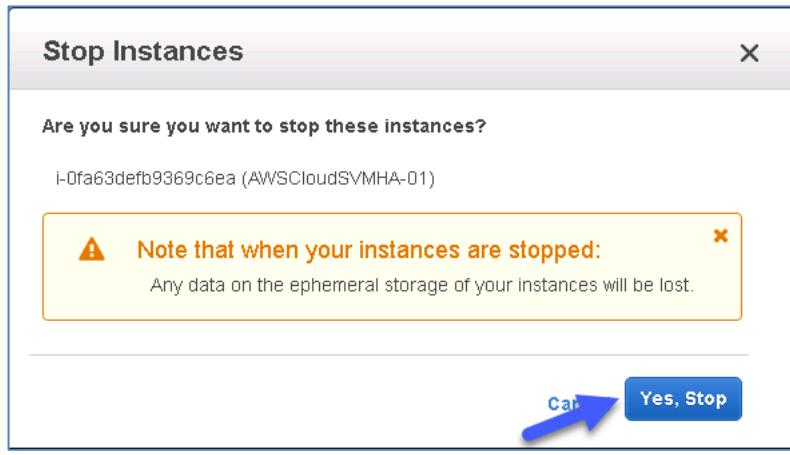
Step	Action
5-1	Return to your browser tab with AWS Console.
5-2	Select VPC > Route Tables .
5-3	Select the Routes tab, and review the routes for the floating IPs. 
5-4	Click the target eni for the route destination 192.168.10.2/32.
5-5	In the Networking Interfaces page that appears click the Instance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

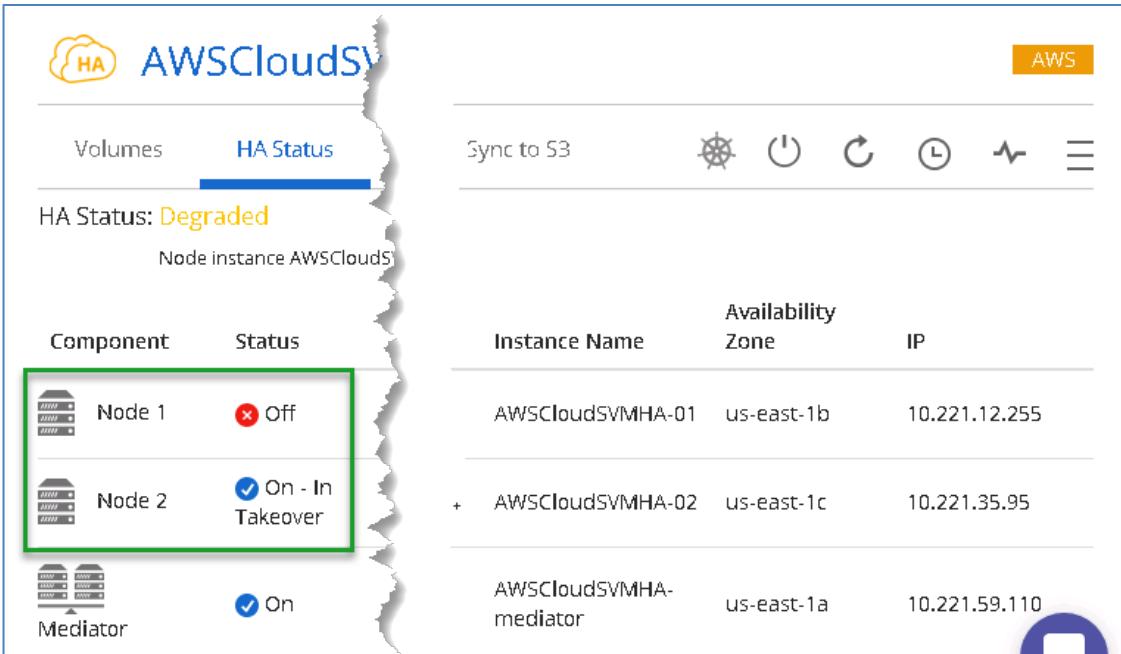
Task 6: Perform a Failover

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	<p> You can click Working Environments > Tabular View > Resources > HA Status to review the HA Status.</p> 
6-3	Go back to the Amazon EC2 dashboard, and select AWSCloudSVMHA-01 .
6-4	<p> 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.</p>

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

Step	Action								
6-7	<p>Go back to your Cloud Manager UI and review the HA status again. Node 1 is Off after a few minutes.</p>  <table border="1"> <thead> <tr> <th>Component</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Node 1</td> <td>Off</td> </tr> <tr> <td>Node 2</td> <td>On - In Takeover</td> </tr> <tr> <td>Mediator</td> <td>On</td> </tr> </tbody> </table>	Component	Status	Node 1	Off	Node 2	On - In Takeover	Mediator	On
Component	Status								
Node 1	Off								
Node 2	On - In Takeover								
Mediator	On								
6-8	<p> 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.</p>								
6-9	<p>Verify that you are still connected to your SMB share on your client.</p>								
6-10	<p> 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.</p>								

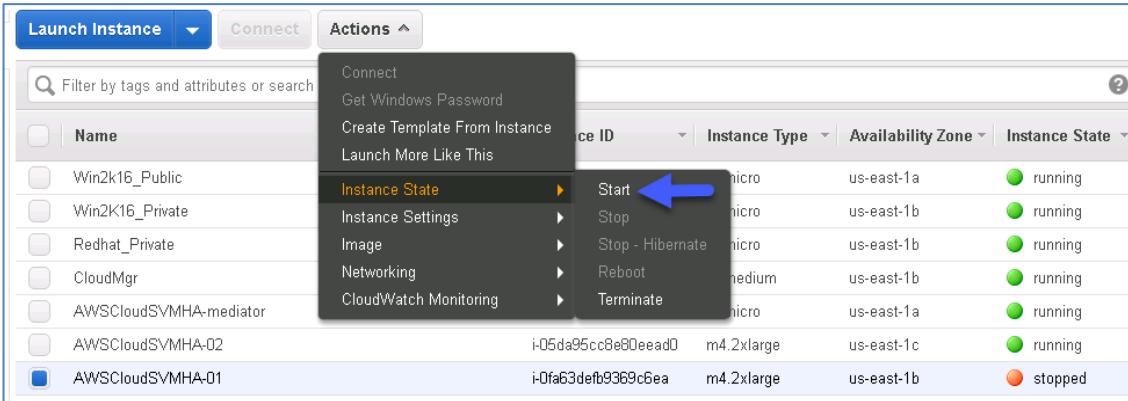
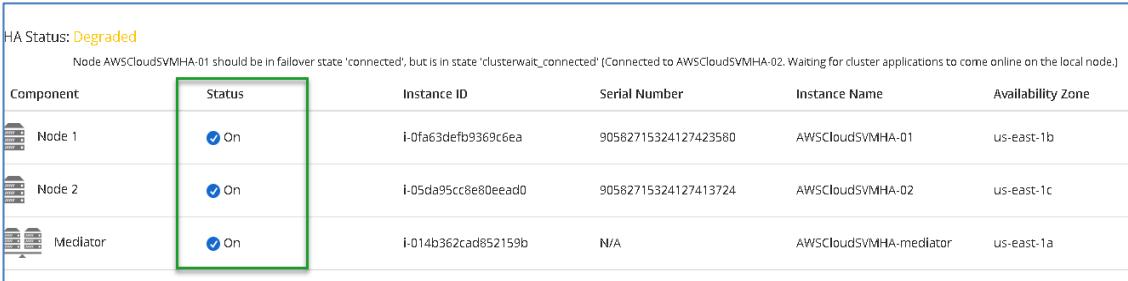
Task 7: Verify That Routes Are Updated After Failover

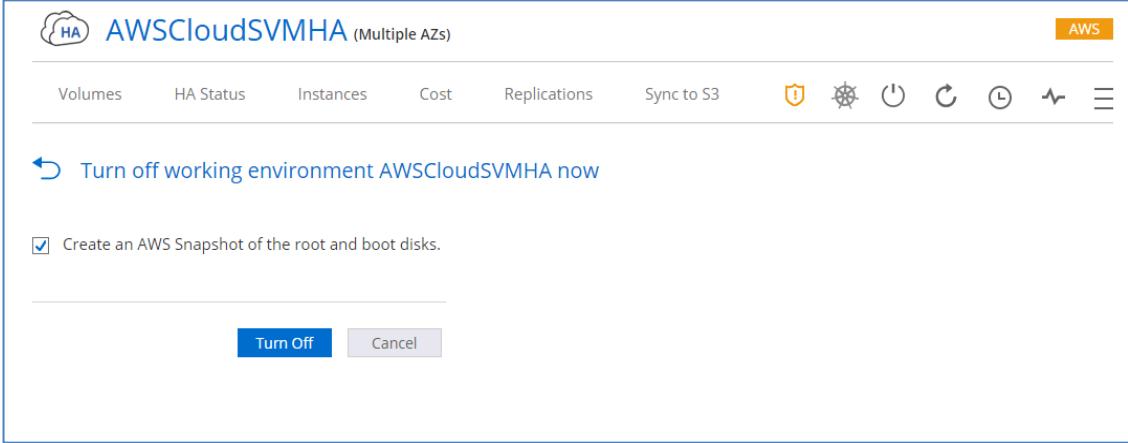
In this task, you confirm the route destination for the data LIF 192.168.10.2 that was used to connect from the client after the failover.

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	<p>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)</p> <ol style="list-style-type: none"> Return to the Cloud Manager UI Go back to Working Environments. Double-click AWSCloudSVMHA. Click the power button on the top right. Click Turn Off. 
8-7	 <p>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.</p>

End of Exercise

Module 8: Cloud Sync Service

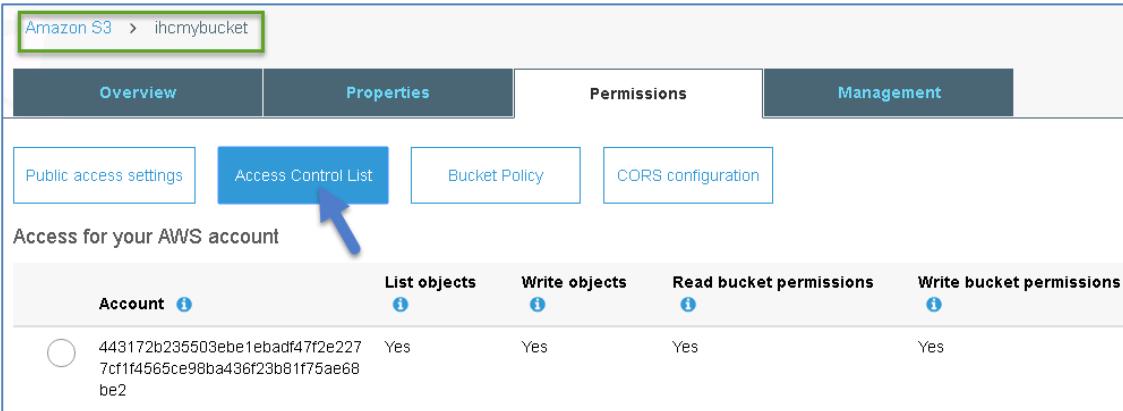
Exercise 1: Synchronize Data From On-Premises to Amazon Simple Storage Service

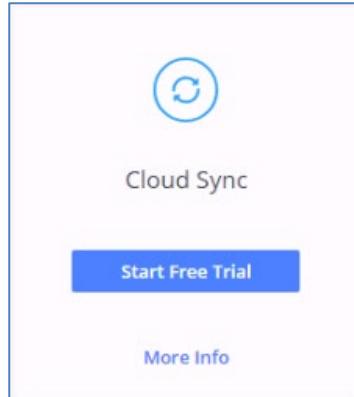
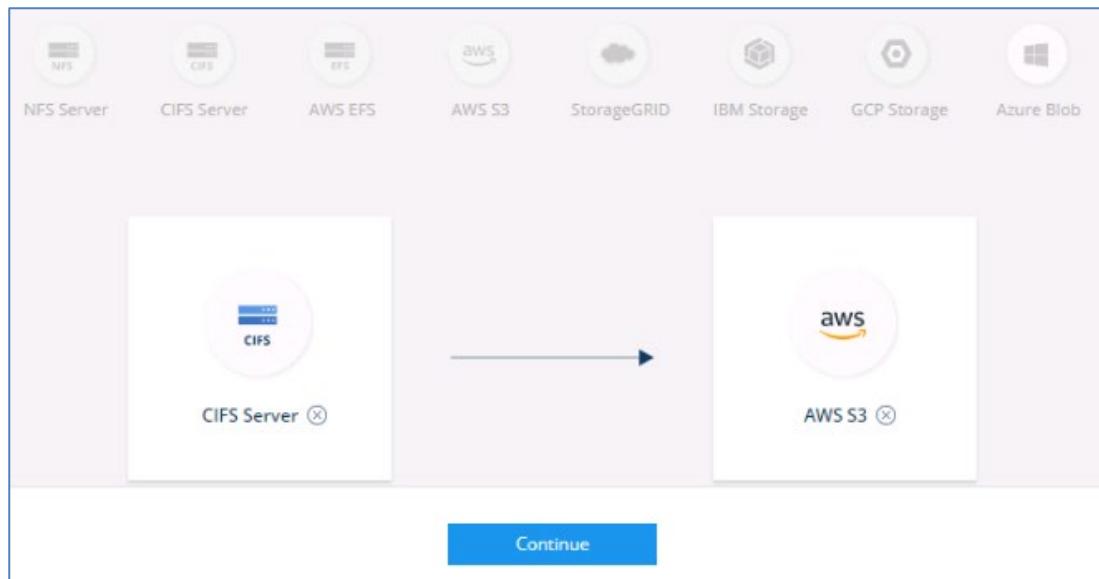
In this exercise, you implement the Cloud Sync service within the Data Fabric to synchronize data between the on-premises cluster and Amazon Simple Storage Service (Amazon S3 or S3).

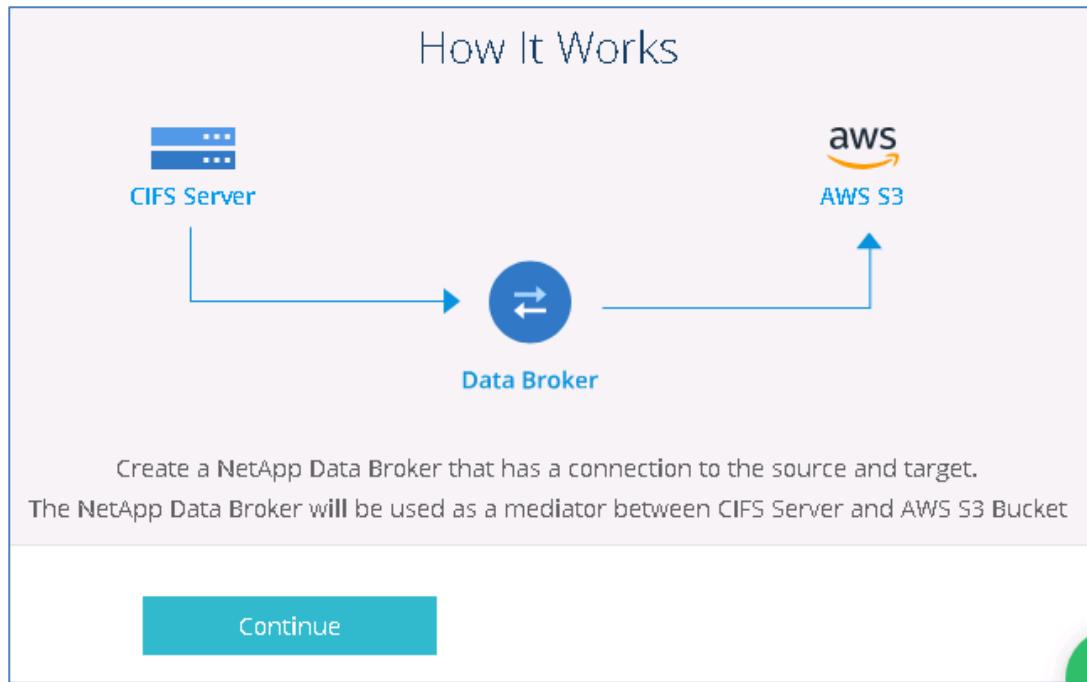
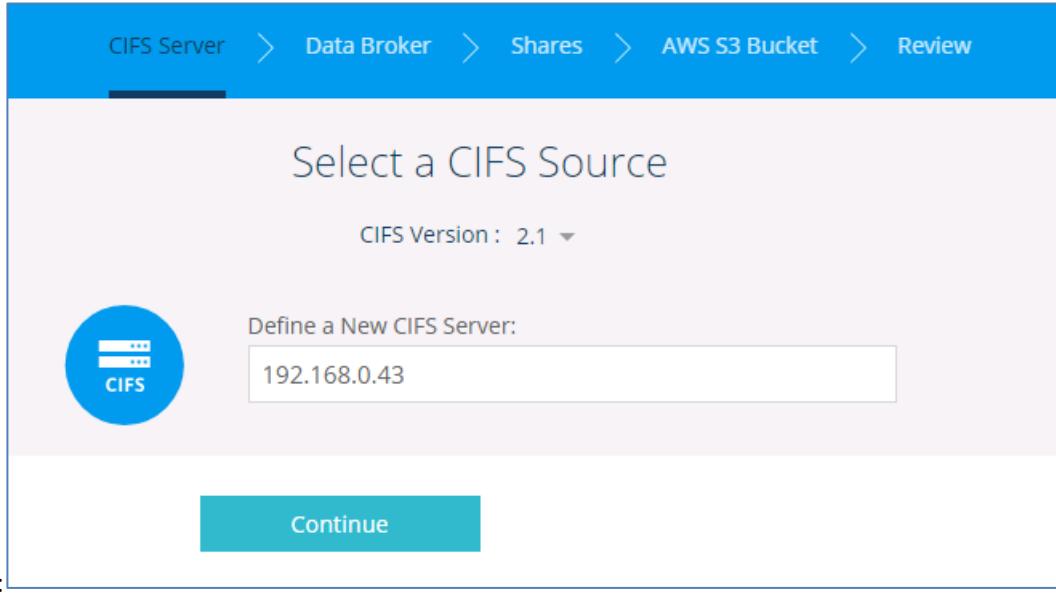
Objectives

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.

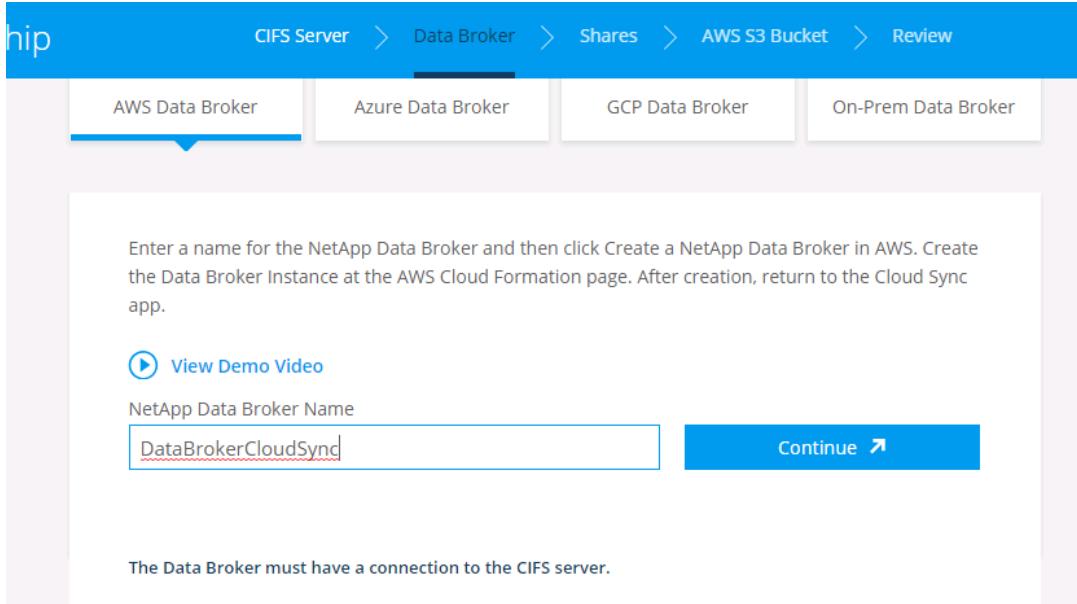
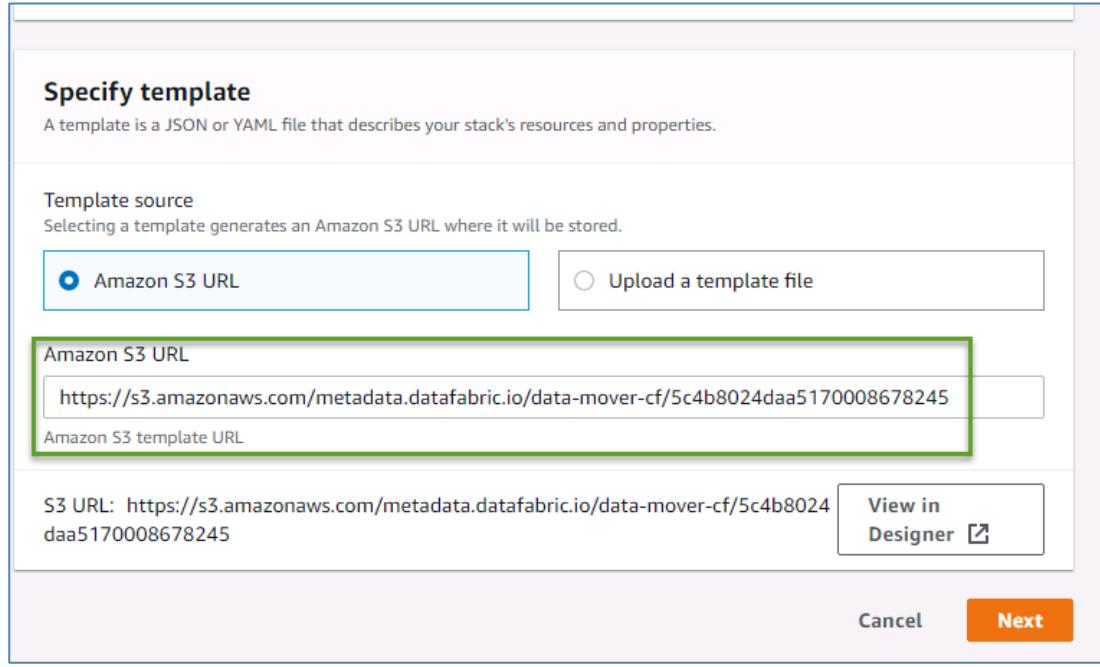
Task 1: Deploy the Cloud Sync Service

Step	Action										
1-1	<p>Create an empty S3 bucket for the Cloud Sync service to use by going to the AWS console and doing the following:</p> <ol style="list-style-type: none">Select Services > S3.Click Create bucket.For bucket name, enter anything unique.Click Create. <p>NOTE: The bucket permissions must enable your AWS account's user ID, which is configured in the access control list by default.</p>  <p>The screenshot shows the AWS S3 console interface for a bucket named 'ihcmybucket'. The 'Permissions' tab is selected. Below it, the 'Access Control List' tab is highlighted with a blue arrow pointing to it. The table below lists permissions for the account '443172b235503eb...be2'. All permissions (List objects, Write objects, Read bucket permissions, Write bucket permissions) are set to 'Yes'.</p> <table border="1"><thead><tr><th>Account</th><th>List objects</th><th>Write objects</th><th>Read bucket permissions</th><th>Write bucket permissions</th></tr></thead><tbody><tr><td>443172b235503eb...be2</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td></tr></tbody></table>	Account	List objects	Write objects	Read bucket permissions	Write bucket permissions	443172b235503eb...be2	Yes	Yes	Yes	Yes
Account	List objects	Write objects	Read bucket permissions	Write bucket permissions							
443172b235503eb...be2	Yes	Yes	Yes	Yes							

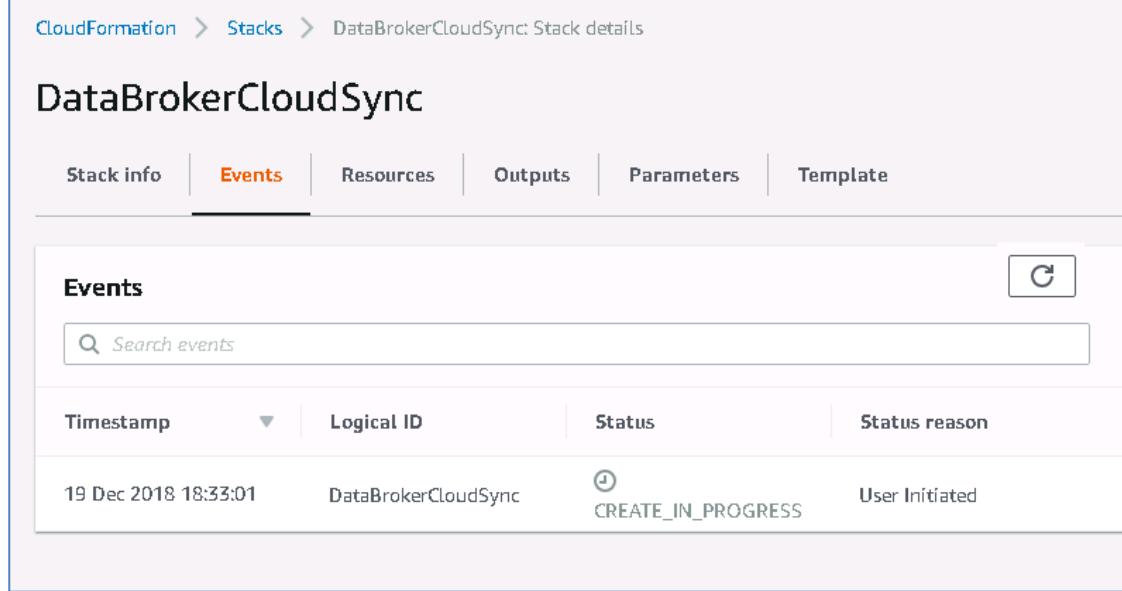
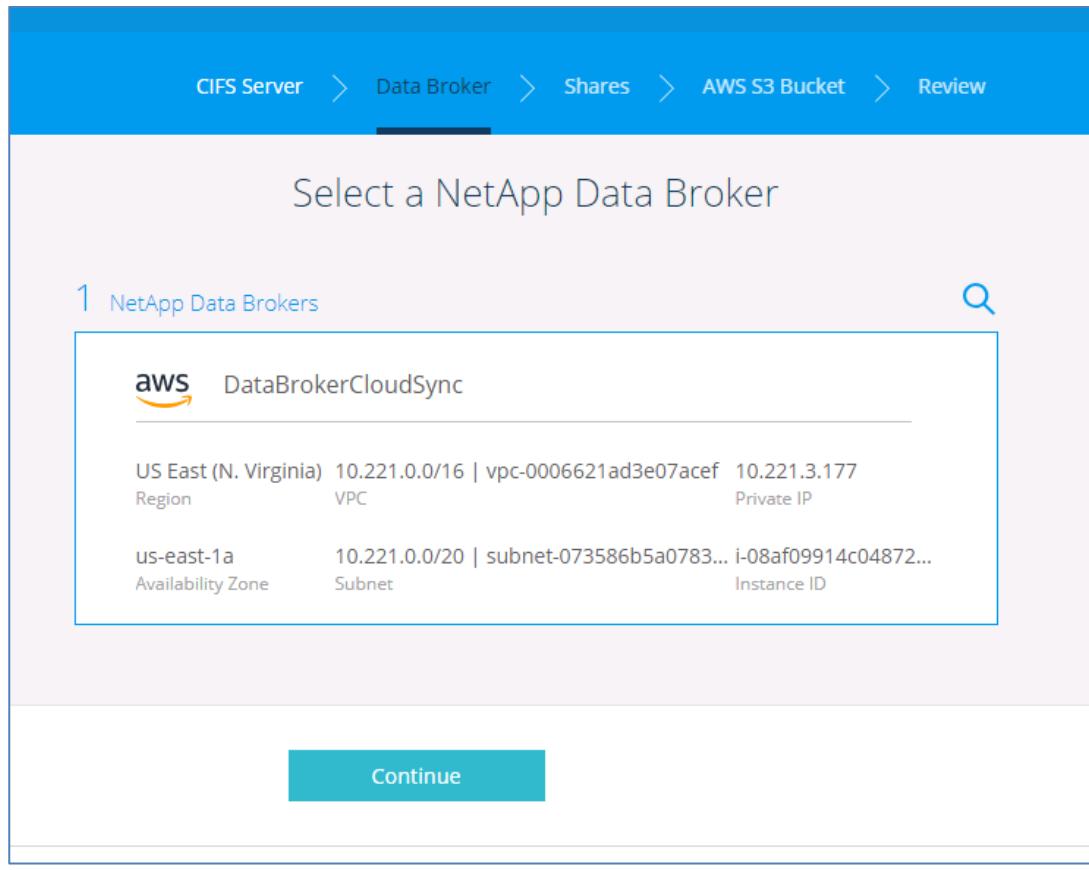
Step	Action
1-2	<p>Go to cloud.netapp.com and click Start Free Trial.</p> 
1-3	<p>Drag the CIFS Server icon to the source bubble and drag the AWS S3 icon to the destination bubble. Note: You may have to reduce the font size of your web browser for example use <CTRL --> to see the source and destination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

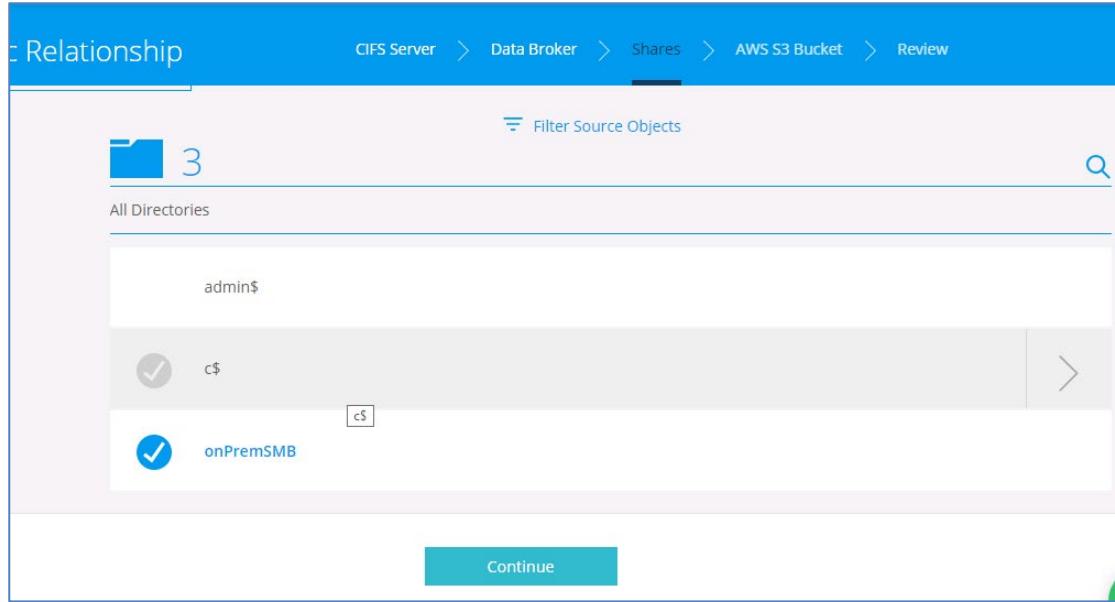
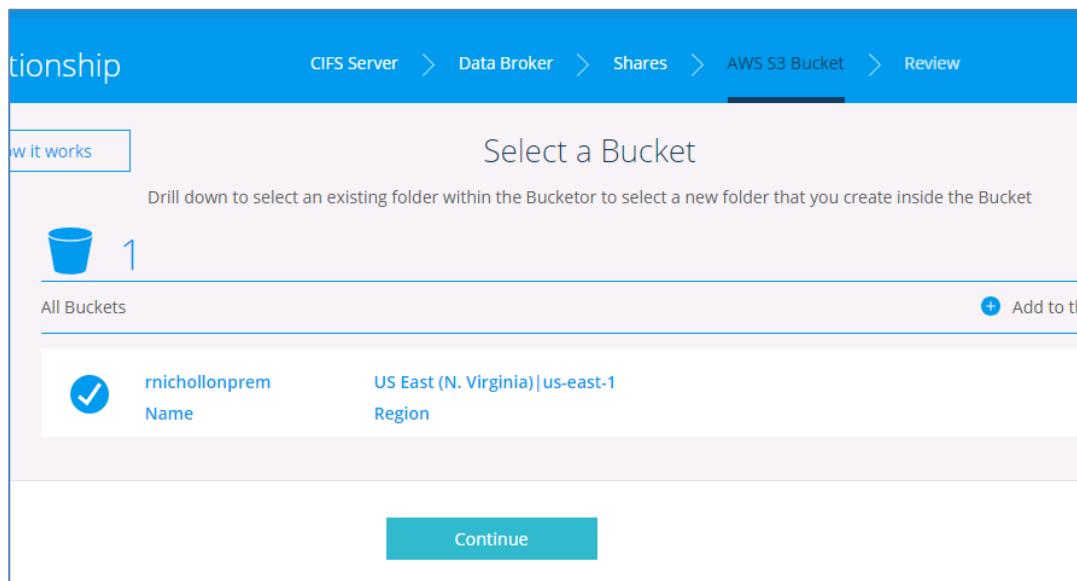
Step	Action
1-5	<p>Click Continue.</p>  <p>Create a NetApp Data Broker that has a connection to the source and target. The NetApp Data Broker will be used as a mediator between CIFS Server and AWS S3 Bucket</p> <p>Continue</p>
1-6	<p>Enter the Data LIF of the on-premises storage virtual machine (SVM) 192.168.0.43, and then click Continue.</p> 

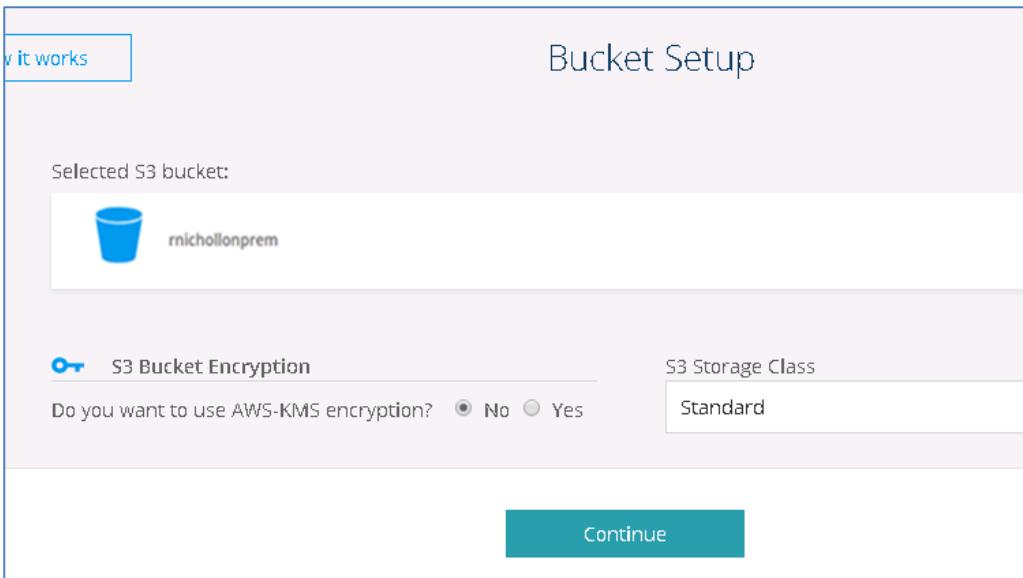
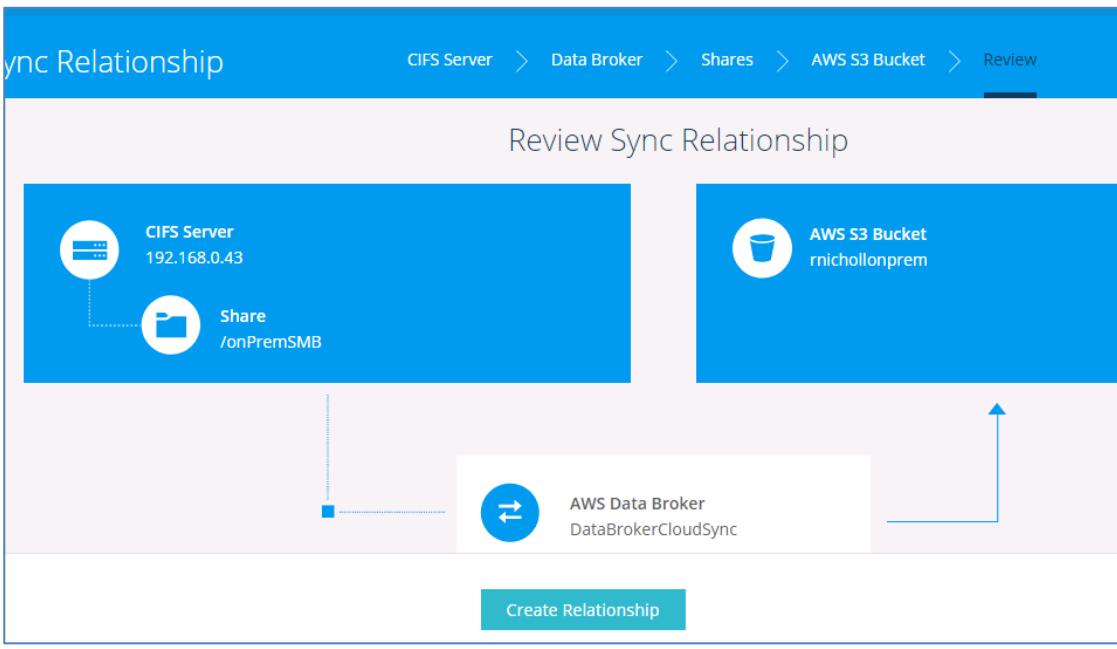
Step	Action
1-7	<p>Enter the following CIFS credentials:</p> <ul style="list-style-type: none"> • User Name: Administrator • Password: Netapp1! • Domain: Demo 
1-8	Click Continue .
1-9	Click AWS Data Broker .
1-10	 You can click View Demo Video link to watch the procedure for launching a Data Broker in AWS. You can also follow the instructions shown below.

Step	Action
1-11	<p>Enter the NetApp Data Broker Name DataBrokerCloudSync, and then click Continue.</p>  <p>The screenshot shows the AWS Cloud Sync interface with the path: CIFS Server > Data Broker > Shares > AWS S3 Bucket > Review. A sub-menu for 'AWS Data Broker' is open, showing four options: AWS Data Broker (selected), Azure Data Broker, GCP Data Broker, and On-Prem Data Broker. Below the menu, there is a note: "Enter a name for the NetApp Data Broker and then click Create a NetApp Data Broker in AWS. Create the Data Broker instance at the AWS Cloud Formation page. After creation, return to the Cloud Sync app." A 'View Demo Video' button is present. A text input field contains 'DataBrokerCloudSync'. A blue 'Continue' button is to the right.</p>
1-12	<p>In the Cloud Formation Create Stack page, verify that an S3 URL is prepopulated and click Next.</p>  <p>The screenshot shows the 'Specify template' page of the AWS CloudFormation 'Create Stack' wizard. It has two tabs: 'Amazon S3 URL' (selected) and 'Upload a template file'. The 'Amazon S3 URL' field contains the URL: https://s3.amazonaws.com/metadata.datafabric.io/data-mover-cf/5c4b8024daa5170008678245. Below the URL, there is a note: 'S3 URL: https://s3.amazonaws.com/metadata.datafabric.io/data-mover-cf/5c4b8024daa5170008678245' and a 'View in Designer' button. At the bottom are 'Cancel' and 'Next' buttons, with 'Next' being highlighted.</p>

Step	Action
1-13	<p>In the Specify stack details, do the following:</p> <ul style="list-style-type: none"> 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. <div style="border: 1px solid #ccc; padding: 10px;"> <p>NetApp Data Broker Placement</p> <p>Which VPC should this be deployed to? The list of your Virtual Private Cloud (VPC)</p> <input style="width: 100%;" type="text" value="vpc-00b406fbe6d7a65e6 (10.221.0.0/16) (PrimaryVPC)"/> <p>Which subnet should this be deployed to? The list of subnet IDs in your Virtual Private Cloud (VPC)</p> <input style="width: 100%;" type="text" value="subnet-02489e5e621cf93f6 (10.221.0.0/20) (PrivateSubnet)"/> <p>NetApp Data Broker Security</p> <p>EC2 KeyPair Name of an existing EC2 KeyPair to enable SSH access to the NetApp Data Broker</p> <input style="width: 100%;" type="text" value="MyAWSKey"/> <p>Assign a public IP address? Indicates whether the NetApp Data Broker instance should receive a public IP address</p> <input style="width: 100%;" type="text" value="False"/> </div>
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	 <p>To watch CloudFormation stack, might need to press refresh to see DataBrokerCloudSync stack appear.</p> 
1-17	<p>When CloudFormation reaches the Status CREATE_COMPLETE, return to the Cloud Sync tab, and click Continue.</p> 

Step	Action
1-18	<p>Select onPremSMB, and click Continue.</p> 
1-19	<p>Select your bucket, and click Continue.</p> 

Step	Action
1-20	<p>In the Bucket Setup page, click Continue.</p> 
1-21	<p>Click Create Relationship.</p> 

Step	Action												
1-22	<p>Click View in Dashboard.</p>												
1-23	<p>Return to the AWS Console, and verify that contents exist in your S3 bucket.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Last modified</th> <th>Size</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>File_500M</td> <td>Dec 19, 2018 6:52:39 PM GMT+0000</td> <td>500.7 MB</td> <td>Standard</td> </tr> <tr> <td>File_750M</td> <td>Dec 19, 2018 6:52:39 PM GMT+0000</td> <td>752.0 MB</td> <td>Standard</td> </tr> </tbody> </table>	Name	Last modified	Size	Storage class	File_500M	Dec 19, 2018 6:52:39 PM GMT+0000	500.7 MB	Standard	File_750M	Dec 19, 2018 6:52:39 PM GMT+0000	752.0 MB	Standard
Name	Last modified	Size	Storage class										
File_500M	Dec 19, 2018 6:52:39 PM GMT+0000	500.7 MB	Standard										
File_750M	Dec 19, 2018 6:52:39 PM GMT+0000	752.0 MB	Standard										

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).

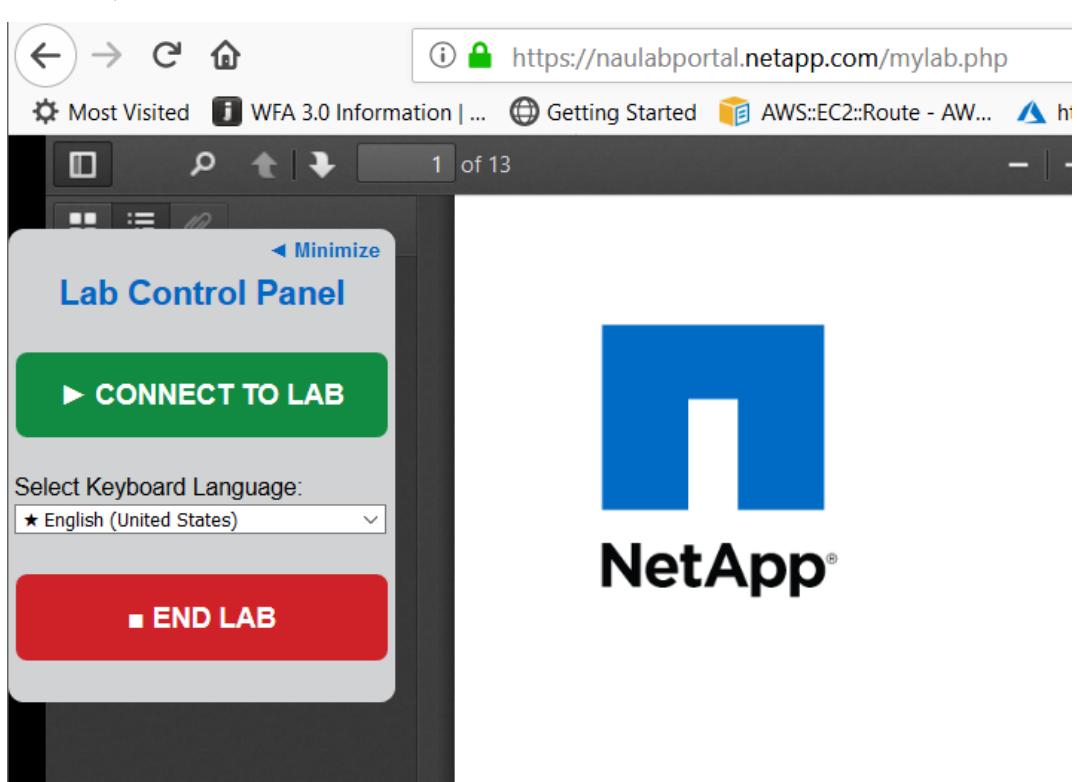
Objectives

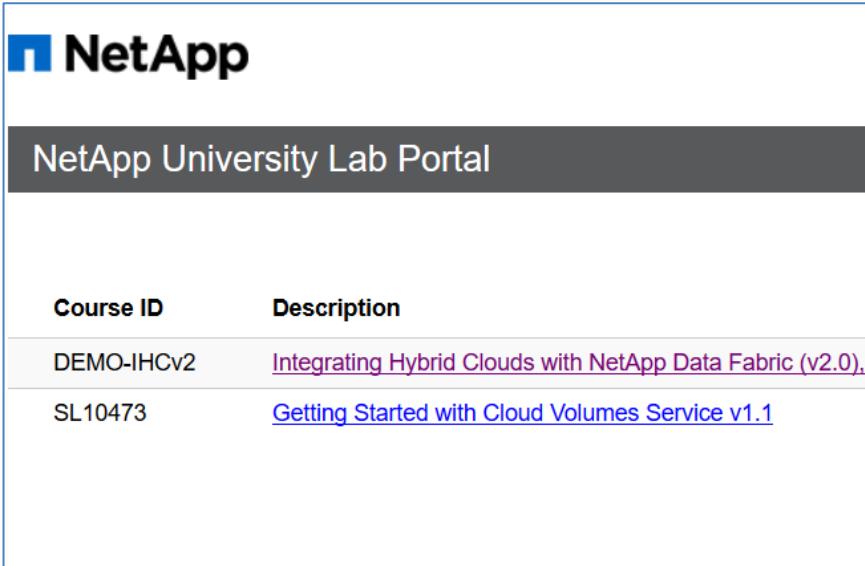
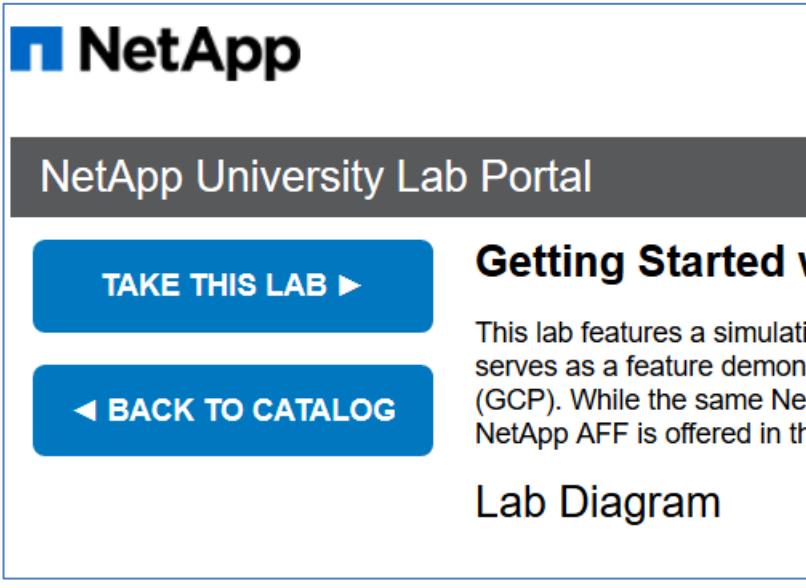
This exercise focuses on enabling you to do the following:

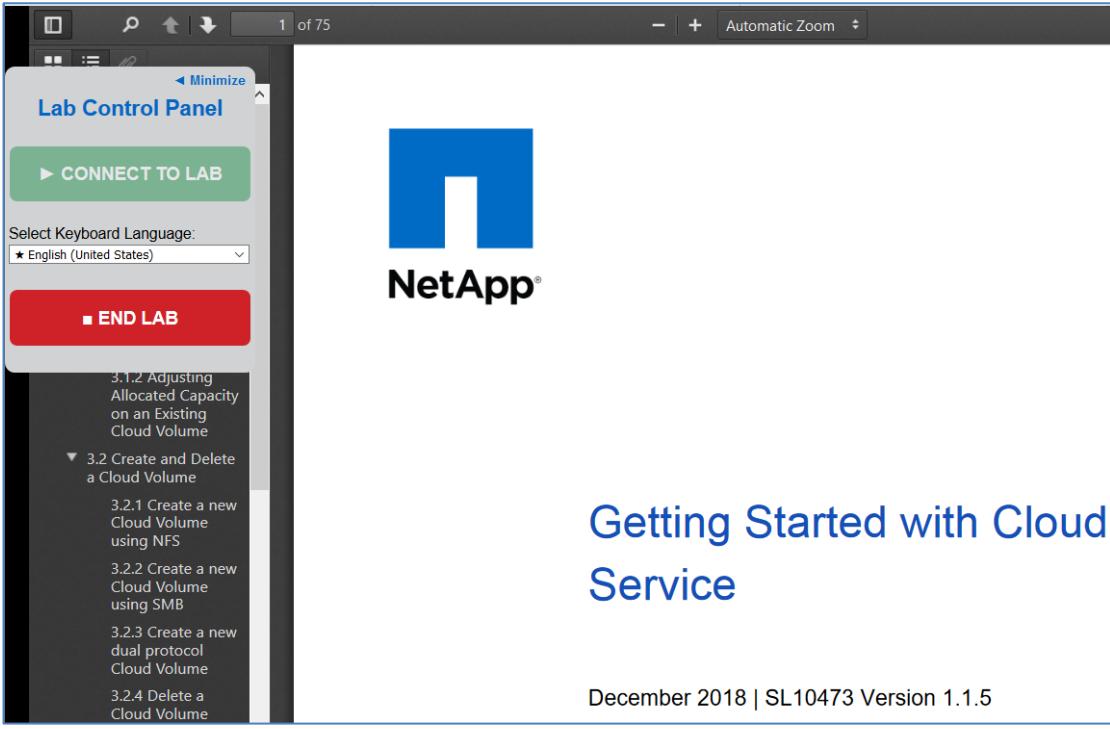
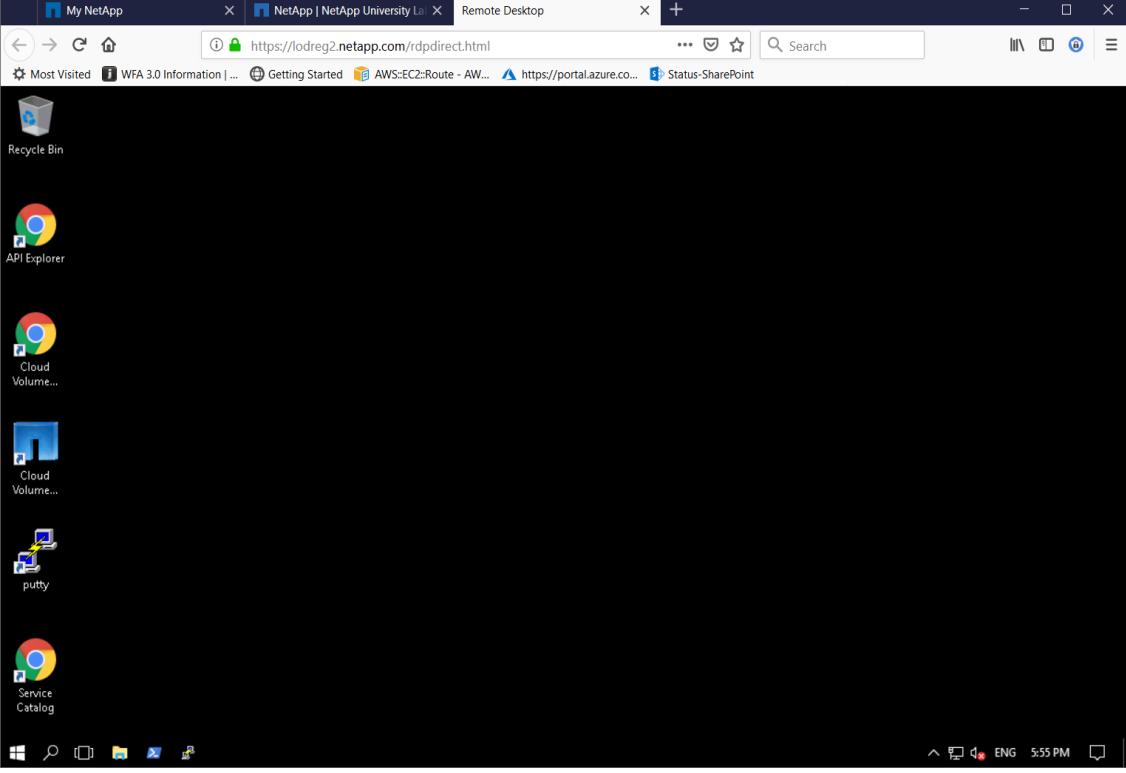
- Create NFS and CIFS volumes using Cloud Volumes Service
- Use clients to mount and access Cloud Volumes.

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	<p>Click Getting Started with Cloud Volumes Service 1.1.</p>  <p>The screenshot shows the NetApp University Lab Portal interface. At the top is the NetApp logo and the portal title. Below is a table listing courses:</p> <table border="1"> <thead> <tr> <th>Course ID</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>DEMO-IHCv2</td> <td>Integrating Hybrid Clouds with NetApp Data Fabric (v2.0)</td> </tr> <tr> <td>SL10473</td> <td>Getting Started with Cloud Volumes Service v1.1</td> </tr> </tbody> </table>	Course ID	Description	DEMO-IHCv2	Integrating Hybrid Clouds with NetApp Data Fabric (v2.0)	SL10473	Getting Started with Cloud Volumes Service v1.1
Course ID	Description						
DEMO-IHCv2	Integrating Hybrid Clouds with NetApp Data Fabric (v2.0)						
SL10473	Getting Started with Cloud Volumes Service v1.1						
1-5	<p>Click TAKE THIS LAB.</p>  <p>The screenshot shows the NetApp University Lab Portal interface. It displays a lab titled "Getting Started with Cloud Volumes Service v1.1". A blue button labeled "TAKE THIS LAB ▶" is visible. Below it is another blue button labeled "◀ BACK TO CATALOG". To the right, there is descriptive text about the lab's purpose and availability across different clouds.</p>						
1-6	Click OK.						

Step	Action
1-7	<p>Verify that the lab guide appears in your browser tab.</p>  <p>The screenshot shows a browser window with a "Lab Control Panel" overlay. The overlay includes a "CONNECT TO LAB" button, a dropdown for "Select Keyboard Language" set to "English (United States)", and a red "END LAB" button. Below these are several sections of content, including "3.1.2 Adjusting Allocated Capacity on an Existing Cloud Volume" and "3.2 Create and Delete a Cloud Volume" with sub-points like "3.2.1 Create a new Cloud Volume using NFS". To the right of the overlay, the main content of the page is visible, featuring the NetApp logo and the title "Getting Started with Cloud Service" with the date "December 2018 SL10473 Version 1.1.5".</p>
1-8	Click CONNECT TO LAB .
1-9	Verify a new tab is opened with the jump host desktop.
	 <p>The screenshot shows a Windows desktop with a dark theme. Several icons are pinned to the taskbar, including "Recycle Bin", "API Explorer", "Cloud Volume...", "Cloud Volume...", "putty", and "Service Catalog". The system tray at the bottom right shows the date and time as "5:55 PM".</p>
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