

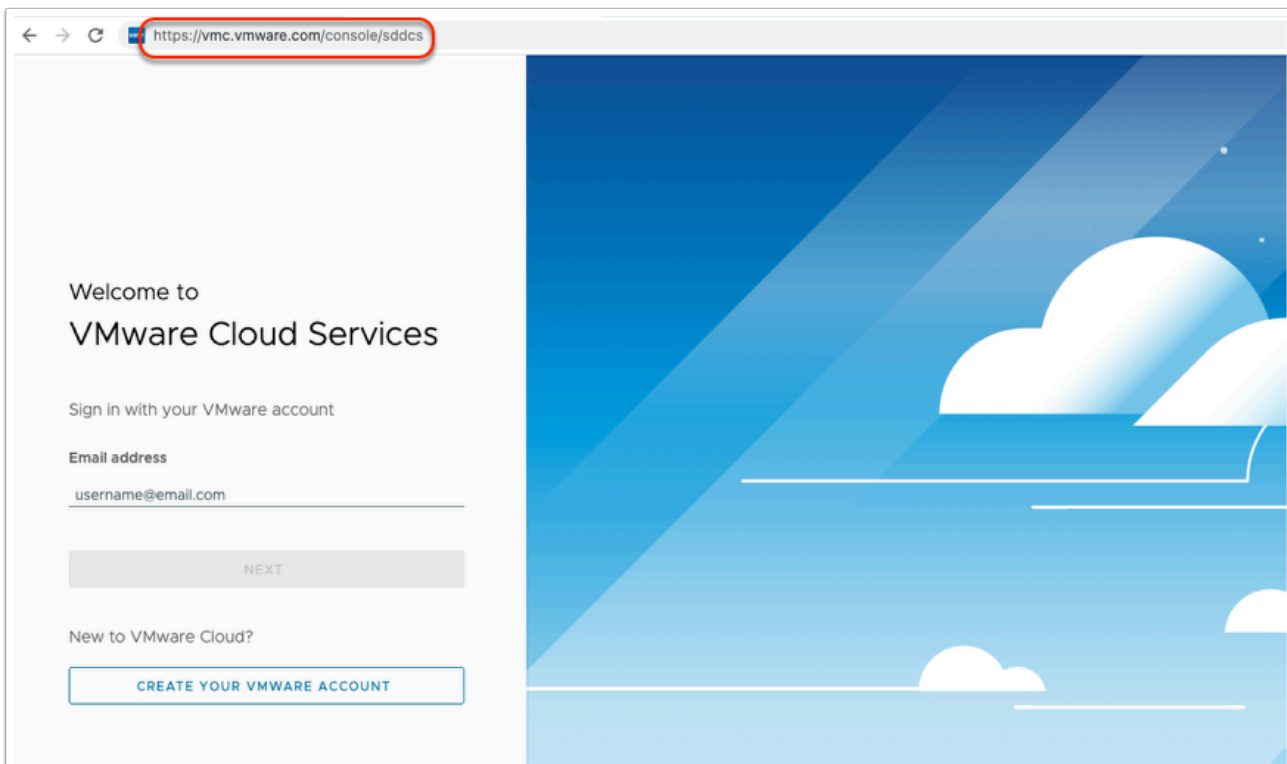
Lab 02 - Working with your SDDC

Introduction

In this lab, we will look at the basic SDDC operations you can perform to begin consumption of your cloud resources in VMC on AWS. We will perform the following:

- Create and configure network segments for our application(s)
- Configure Firewall rules to allow remote access to vCenter
- Deploy your 1st Virtual Machines in VMC on AWS


If you are still logged into your VMC on AWS Organization from the previous lab you can skip the steps outlined below and begin task one. If not, you'll first need to log into your VMC on AWS organization.

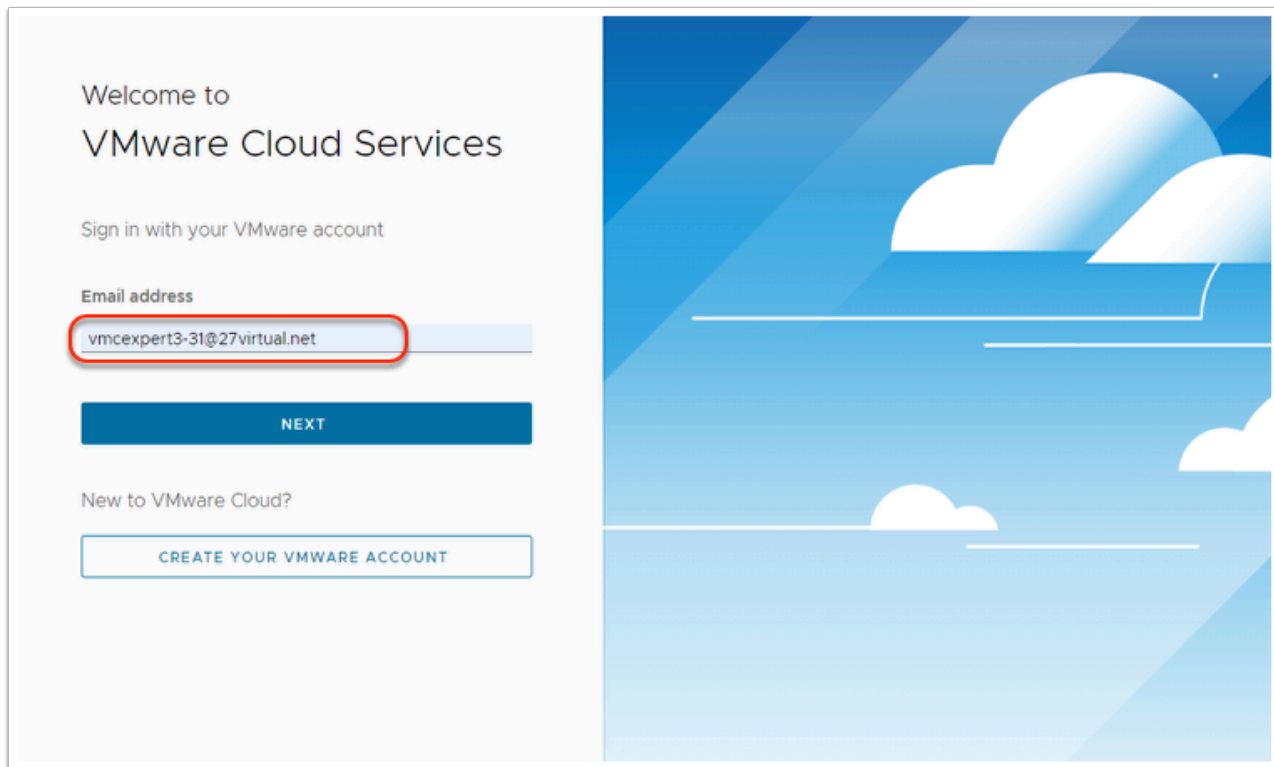


To log into your VMC on AWS Organization, follow the steps below:

1. From your Desktop/laptop launch your preferred browser
2. In the browser address bar, go to <https://vmc.vmware.com/console/sddcs> and login as

- VMware Account: **vmcexpert#-{XX}@vmware-hol.com** (Where **#** is your Environment ID, and **{XX}** is your assigned student number)
- Password: **VMware1!**

 In tests, *Google Chrome* in *Incognito mode* worked best.



TASKS

Task 1 - Create a Logical Network

You will now create and configure a network segment that will be used in Task 4 when you create your Virtual Machines in the SDDC

NOTE: VMC Network Segments are backed by VMware NSX GENEVE Overlay Segments.

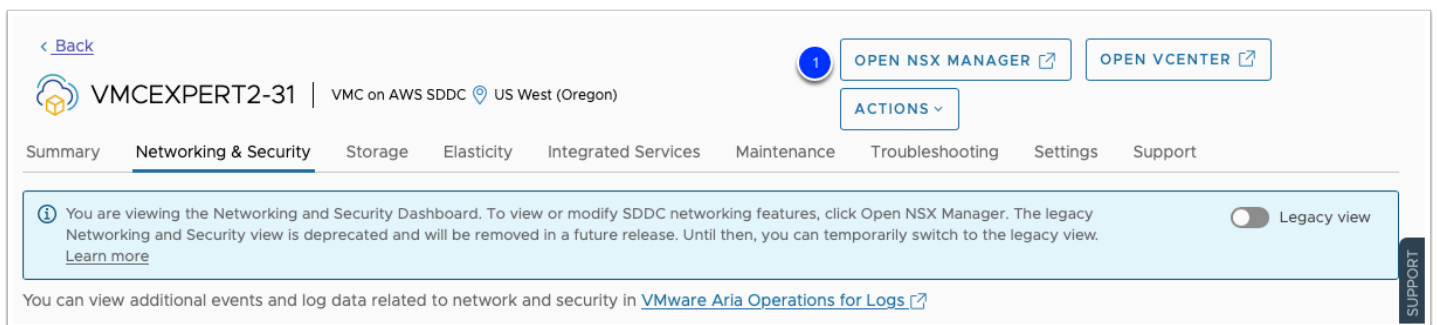
NSX Overlay-backed Segment

In an overlay-backed segment, traffic between two VMs on different hosts but attached to the same overlay segment have their layer 2 traffic carried by a tunnel between the hosts. VMware NSX instantiates and maintains this IP tunnel without the need for any

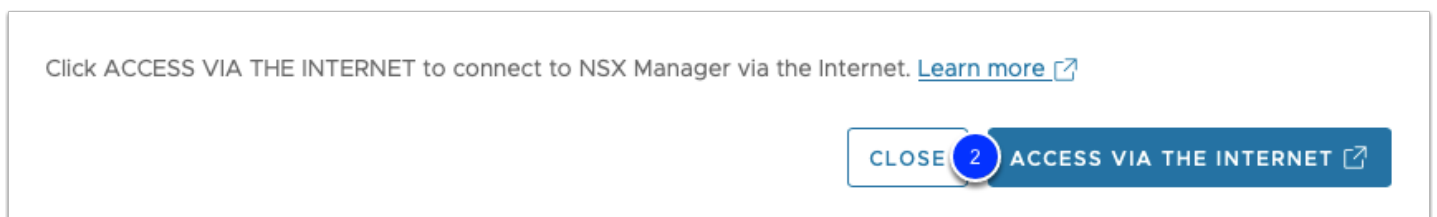
segment-specific configuration in the physical infrastructure. This means, there is no need to configure VLANs on the physical network to enforce isolation. As a result, the virtual network infrastructure is decoupled from the physical network infrastructure. That is, you can create segments dynamically without any configuration of the physical network infrastructure.

Select your SDDC, if you aren't currently within it, then click **View Details**

1. Click the **OPEN NSX MANAGER** button

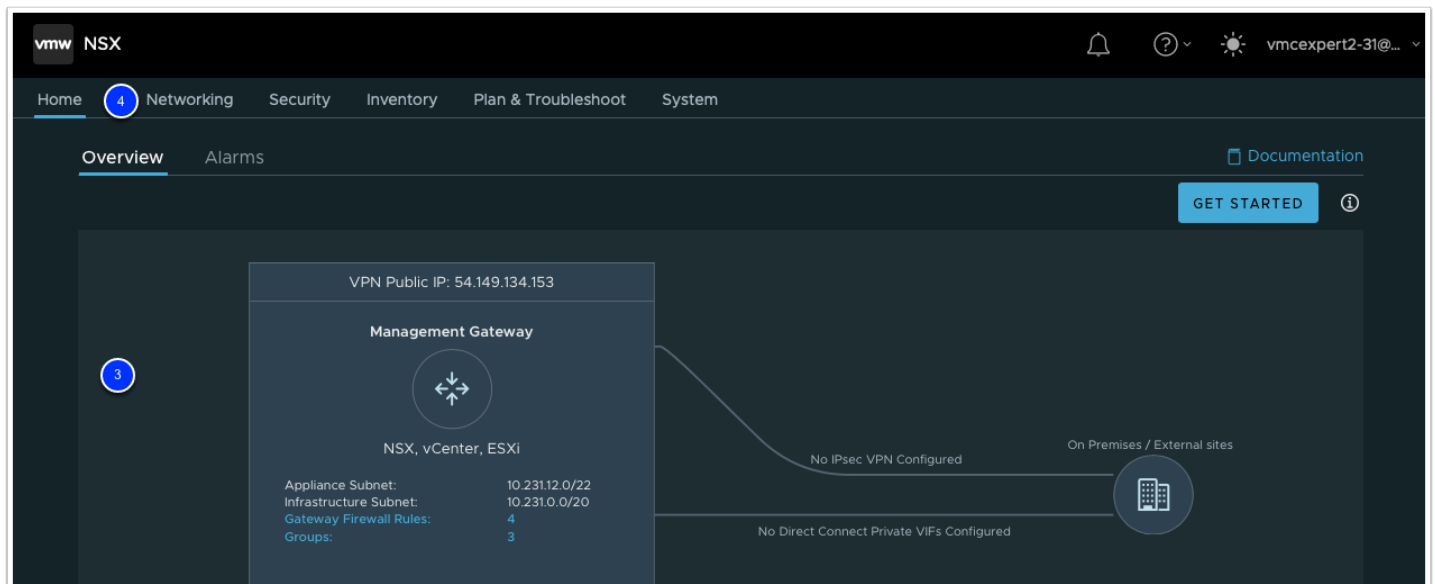


2. Click **ACCESS VIA THE INTERNET** to connect to NSX Manager UI

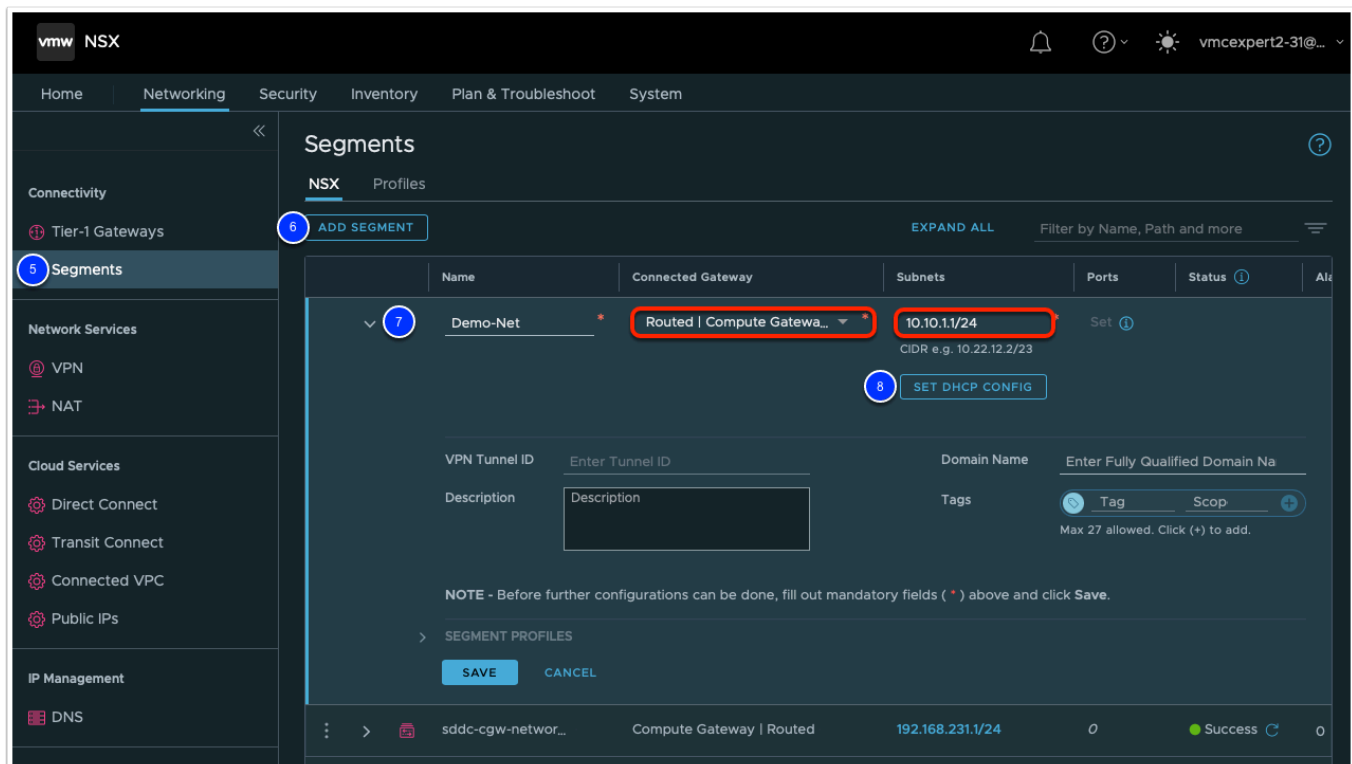


3. Wait till page with NSX Manager will be loaded and you will see Overview dashboard.

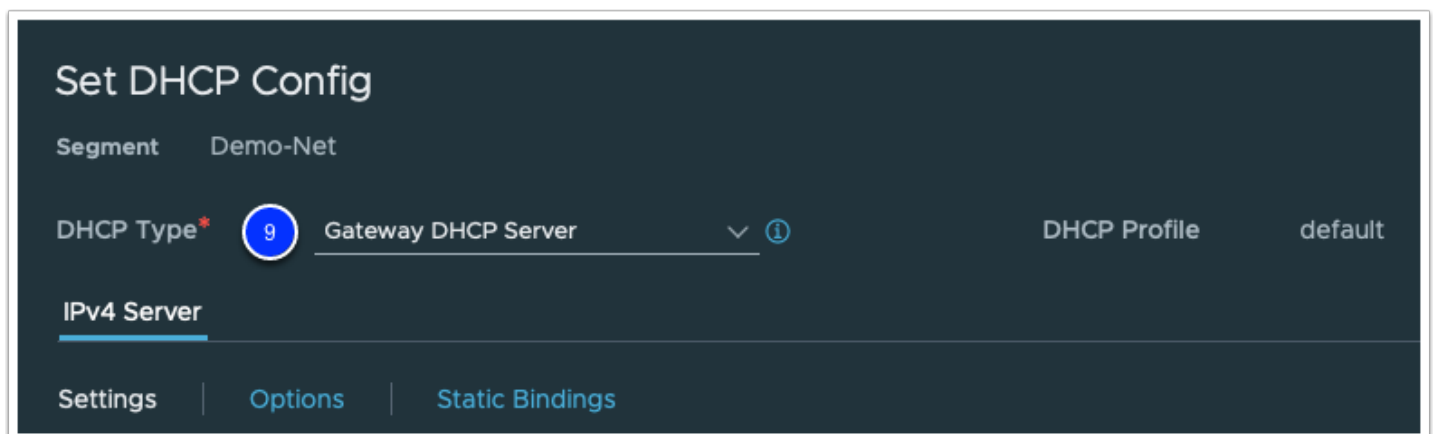
4. Click on **Networking** tab



5. Click **Segments** to display the existing network segments.
6. Click on **ADD SEGMENT** to create a new network segment.
7. Enter the following values:
 - Name: **Demo-Net**
 - Connected Gateway: **Routed**
 - Subnets: **10.10.xx.1/24** (where **xx** is your student number, for students(1-9) do not include a leading 0), i.e. **10.10.1.1/24**
 - This represents the default gateway and the prefix length of the network
 - VPN Tunnel ID: *Leave Blank*
 - Domain Name: *Leave Blank*
 - Description: *Leave Blank*
 - Tags: *Leave Blank*
8. Click the **SET DHCP CONFIG** button to enable and configure DHCP in the pop-up



9. On the drop down Choose **Gateway DHCP Server** from the DHCP Type Field



10. Enter **10.10.XX.11-10.10.XX.200** for the **DHCP IP Range**. (Where **XX** is your student number)
 - a. This is the range of IP addresses the DHCP server will grant to workloads attached to the network.
 - b. NOTE: Ensure the DHCP range turns blue, matches the range, and puts a bubble around the range. If it is red, please redo the steps.
 - c. If you have a student number in the single digits, you must omit the leading zero. (ie 10.10.8.11)
11. Leave the other fields as their default values. As before ensure the bubble turns blue and not red.
 - Lease Time: **Leave Blank**
 - DNS Servers: **Leave Blank**

Set DHCP Config

Segment: Demo-Net

DHCP Type: Gateway DHCP Server | DHCP Profile: default

IPv4 Server

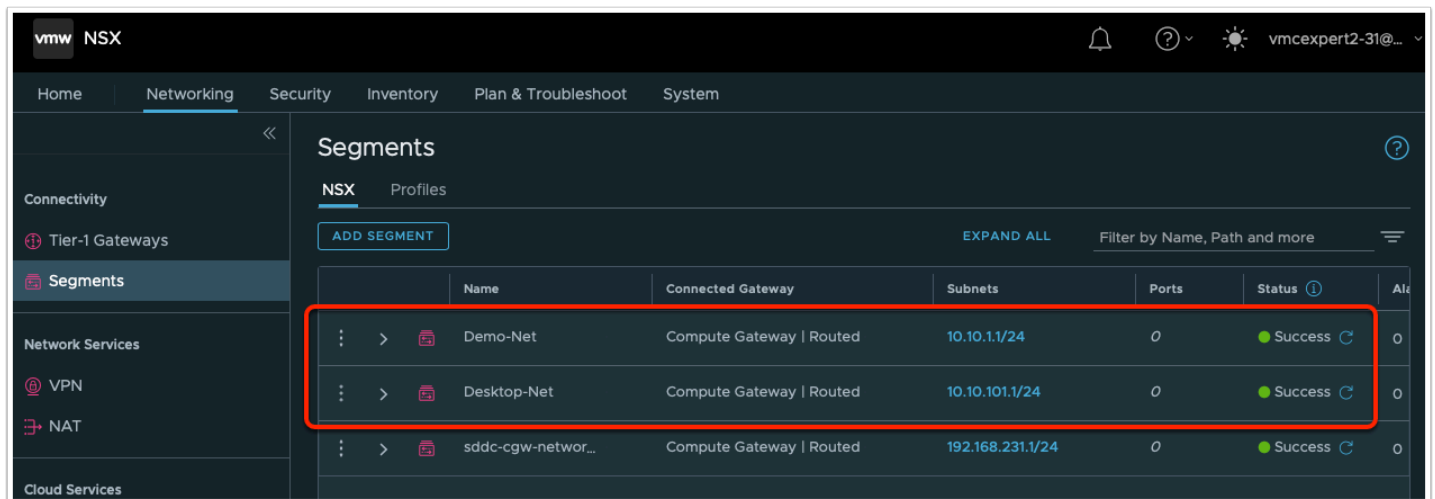
Settings | Options | Static Bindings

DHCP Server Address: 10.231.13.253/30

DHCP Ranges: 10 (10.10.1.11-10.10.1.200) | IPv4 Gateway: 10.10.1.1/24

Lease Time (seconds): 86400 | DNS Servers: Enter IP Addresses (e.g. 10.10.10.10)

11. Scroll down, Click **Apply**
12. Click **Save** to save the logical network.
Note: You might need to scroll down to the bottom of the add segment box for the Save button to appear
13. When prompted to continue configuring the segment, Click **NO**
14. Repeat Steps 1 - 11 using the information below to create a 2nd virtual network segment in the SDDC
 - Segment Name: **Desktop-Net**
 - Connected Gateway: **Routed**
 - Subnet: **10.10.1(xx).1/24** - where **xx** is your student number.
 For students(1-9) include the a leading 0), **i.e. 10.10.109.1/24**
 - DHCP Config
 - DHCP Type: **Gateway DHCP Server**
 - DHCP Range: **10.10.1(xx).11-10.10.1(xx).50** - where **xx** (1 - 30) is your student number
 - DNS Servers (click add item each IP):
 1. **8.8.8.8**
 2. **192.168.110.10**
15. Verify the network segments were added correctly. Your Segments List should be displaying both the Demo and Desktop segments as shown in the screenshot below.



Task 2 - Configure Firewall rule and log in to vCenter Server

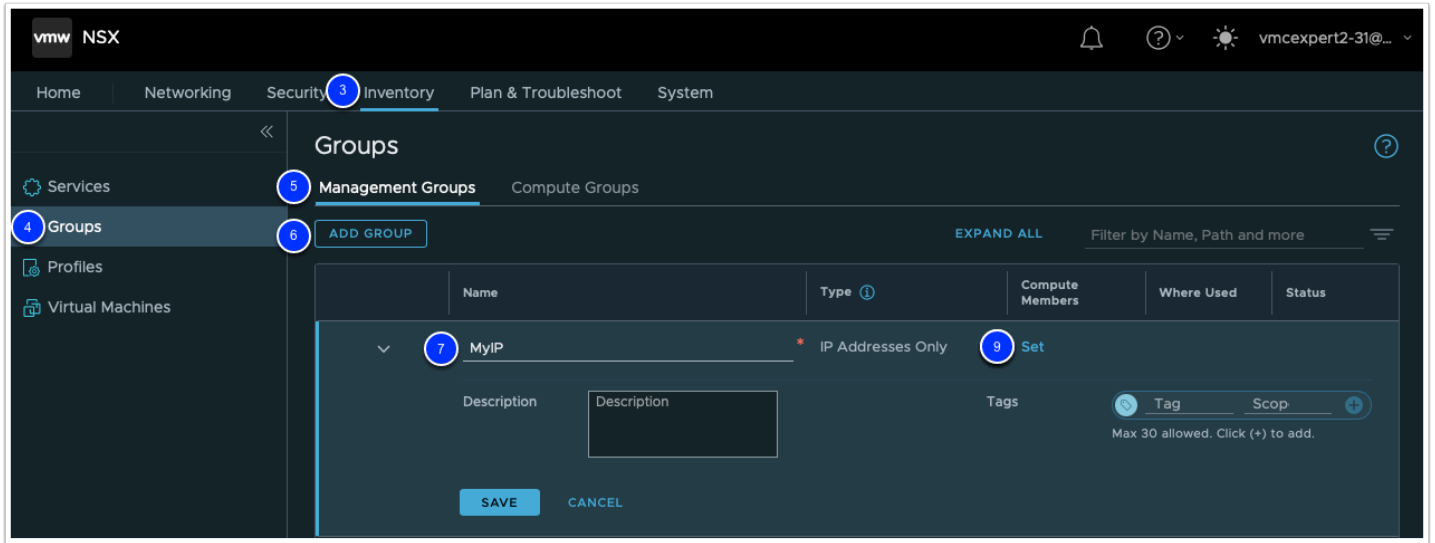
By default, all inbound firewall traffic into the SDDC is denied in VMware Cloud on AWS. To access vCenter from your Desktop/Laptop or any other external device, you will need to configure a firewall rule allowing inbound access. The Management Gateway (MGW) controls access to vCenter, the ESXi hosts, and all other management components.

Note: In most enterprise environments, you would configure a VPN or Direct Connect VIF to allow limited access firewall rules to vCenter. In this lab, we will use your home/work PCs public IP address to create a firewall rule to access the vCenter server. In a later lab we will switch to a VPN.

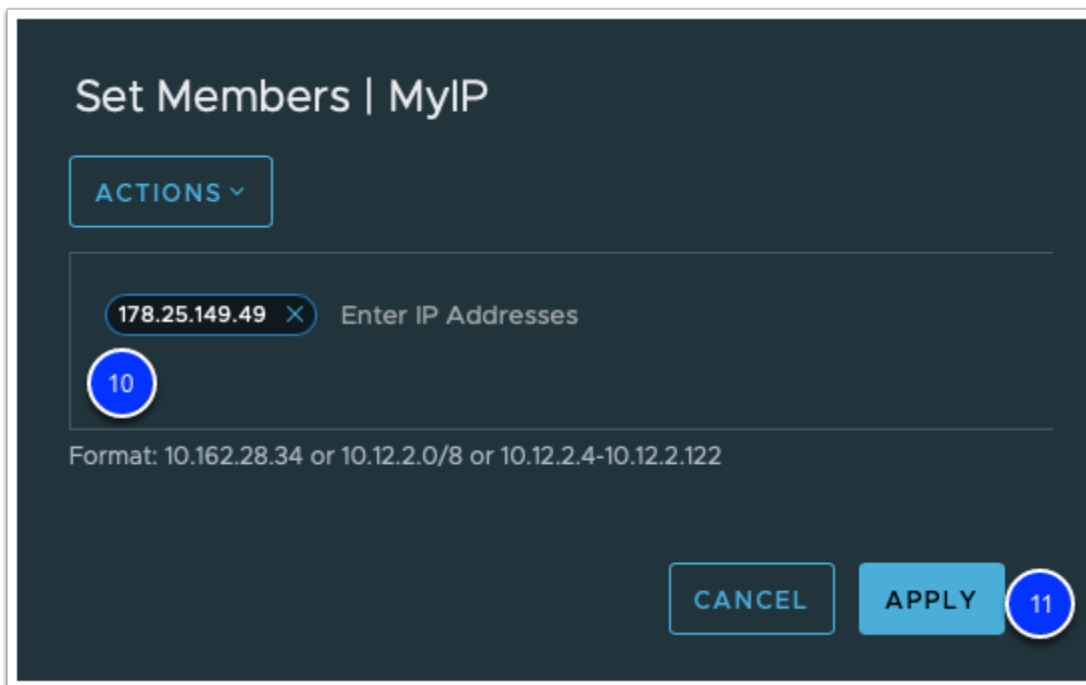
As of the June 2021 release of VMC on AWS, a High Severity notification is triggered when the SDDC vCenter is exposed to the world using an ANY to vCenter Firewall rule and it will be disabled automatically after a brief while.

1. If your NSX Manager UI tab is active then go to step #3. If you already closed NSX Manager tab then Select your SDDC, if you aren't currently within it, then click **View Details**
2. Click the **OPEN NSX MANAGER** button and click **ACCESS VIA THE INTERNET** to connect to NSX Manager UI. Wait till page with NSX Manager will be loaded and you will see **Home - Overview** dashboard.
3. Choose **Inventory** tab
4. Click on **Groups** on the left hand side of the screen.
5. Click on **Management Groups**
6. Click on **Add Group**
7. Name: **MyIP**

8. In a separate browser tab, go to <http://whatismyip.com> to confirm the public IPv4 address that your local PC is currently using. Copy that IP address to your clipboard and close the browser tab.
9. Back on the NSX Manager UI tab, click **Set** to add your Public IP address to the MyIP group

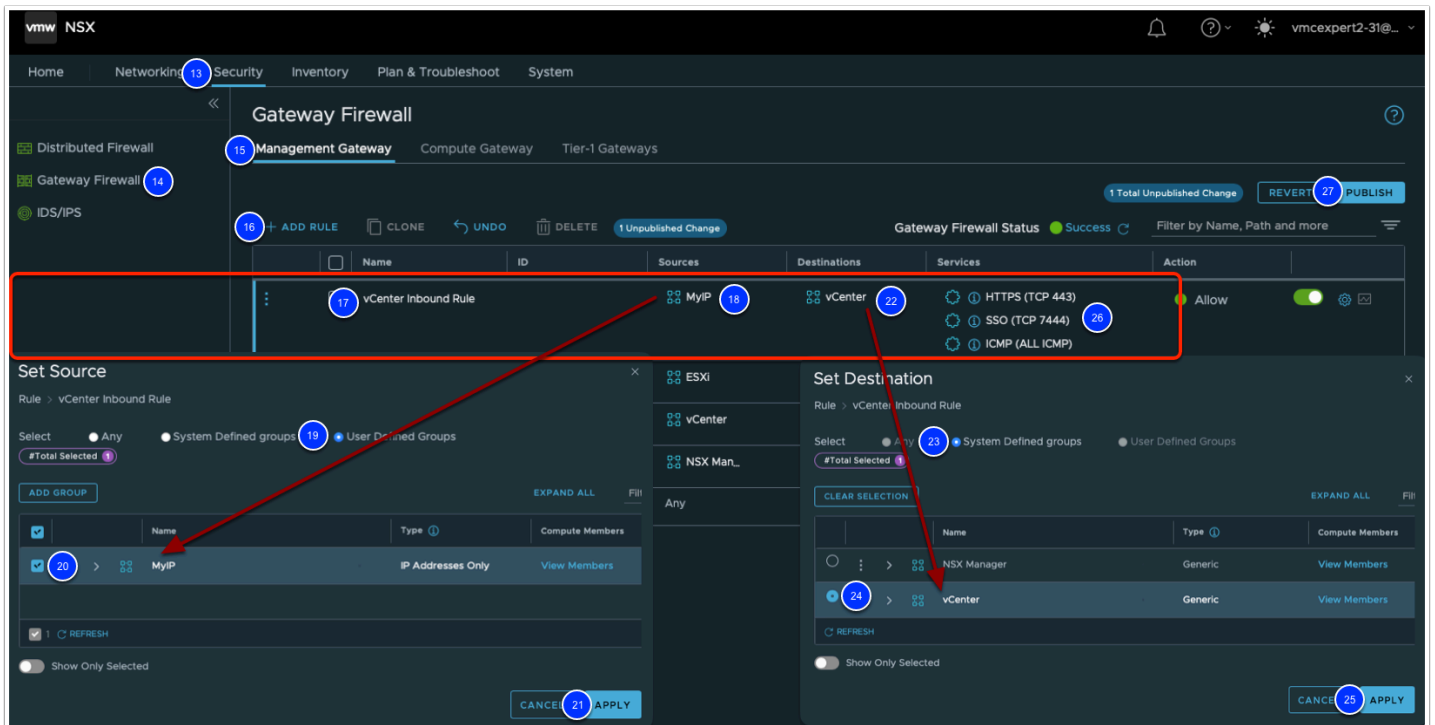


10. Right click over the words **Enter IP Addresses** field and paste your public IP address from the clipboard
11. Click **APPLY**
12. Click **SAVE**



13. Select **Security** tab
14. Click on **Gateway Firewall** on the left-hand side of the screen.
15. If it is not already selected, click on **Management Gateway** to create firewall rules that allow access to management components in the SDDC.

16. Click **+ ADD RULE** to add a new rule to the edge gateway. A row titled new rule should appear.
17. Click the "New Rule" text from the "Name" column and change it to **vCenter Inbound Rule**.
18. Under Sources, hover your mouse over the word **ANY** and click the pencil icon
19. Click the radio button labels **User Defined Groups**
20. Click the check box to select the **MyIP** group
21. Click **Apply**
22. Hover over the new rule's "**Destinations**" column, then click the **blue Edit button** to edit the destination field.
23. On the Pop Up, click the radio button next to **System Defined Groups**.
24. Select the Radio-button next to **vCenter**.
25. Click **Apply**
26. Hover over the new rule's "**Services**" column, then click the **blue Edit button**, select **HTTPS (TCP 443), SSO (TCP 7444) and ICMP (ALL ICMP)** to allow access to the vCenter server.
27. Click **PUBLISH**



Task 3 - Log in to vCenter Server

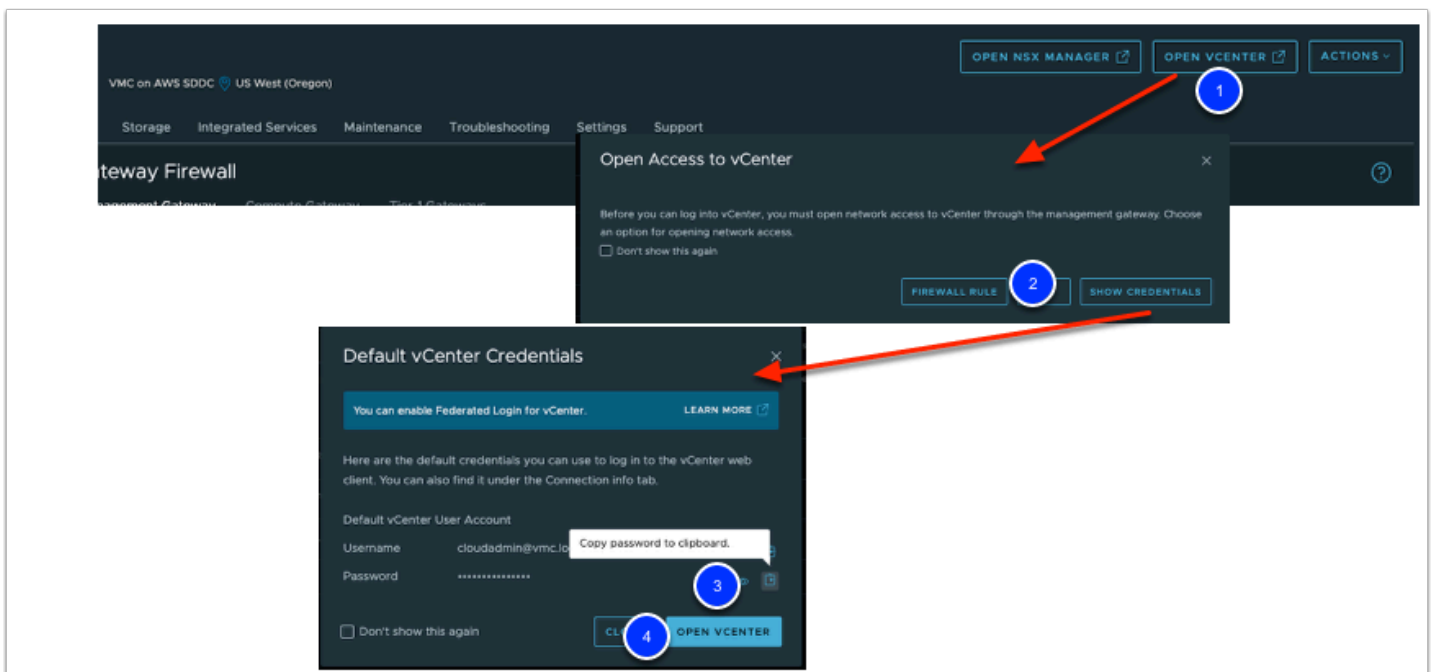
Now that the firewall rule has been modified to allow external access to vCenter, we would be able to log in, but before doing so, we need to first gather the following pieces of information from our VMC Console:

- vCenter (FQDN and/or IP)
- Default Cloud Admin Account

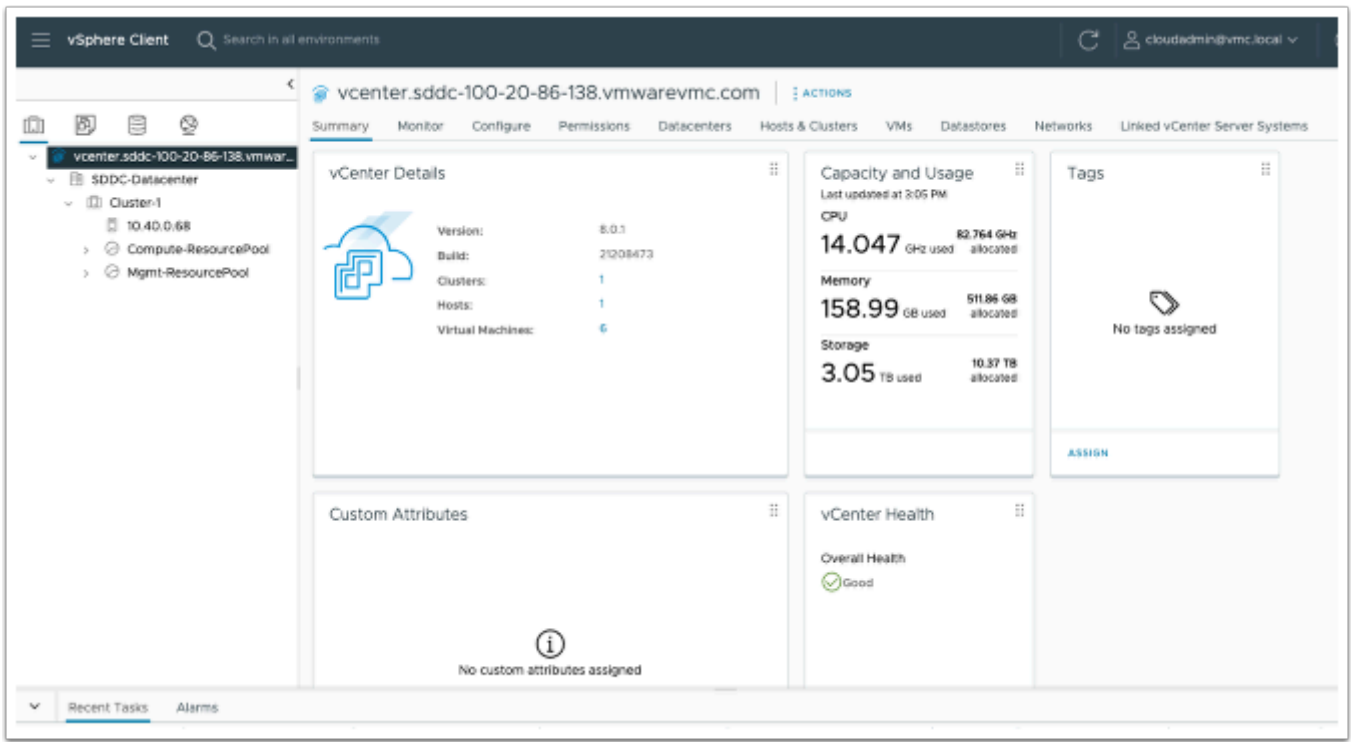
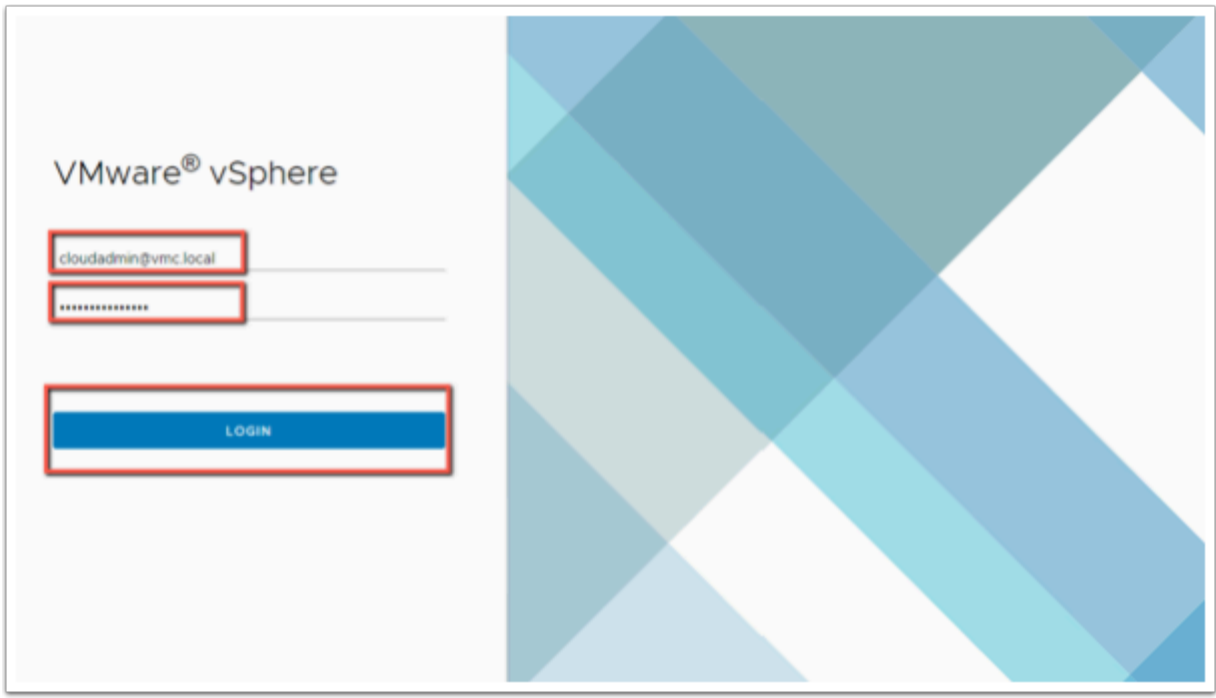
- Default Cloud Admin Password

We can gather this information by going to the **Settings** tab, however while logged in to the VMC Console, the fastest way to get the information is clicking on **OPEN VCENTER** in the upper right.

1. Go back to your VMC on AWS browser tab. At the top right of the page, click **OPEN VCENTER**
2. On the Pop Up, click on the **SHOW CREDENTIALS Button**
3. Click the Clipboard **icon** next to Password to copy the administrative user password to your clipboard.
4. Click the **OPEN VCENTER** button to open a connection to the vCenter HTML5 client.



5. In the example@domain.local field enter **cloudadmin@vmc.local**
6. Right-click in the **Password** field and paste the password copied in the previous step.
7. Click **LOGIN**.
8. On the Summary page Click **Reset to green** for any visible warnings and/or errors



Task 4 - Create Content Library

Content Libraries

Content libraries are container objects for VM templates, vApp templates, and other types of files like ISO images.

You can create a content library in the vSphere Client (HTML5), and populate it with templates, which you can use to deploy virtual machines or vApps in your VMware Cloud on AWS environment. If you already have a Content Library in your on-premises data center, you can use the Content Library to import content into your SDDC.

You can create two types of libraries: local or subscribed libraries.

Local Libraries

You use a local library to store items in a single vCenter Server instance. You can publish the local library so that users from other vCenter Server systems can subscribe to it. When you publish a content library externally, you can configure a password for authentication.

VM templates and vApps templates are stored as OVF file formats in the content library. You can also upload other file types, such as ISO images, text files, and so on, in a content library.

Subscribed Libraries

You subscribe to a published library by creating a subscribed library. You can create the subscribed library in the same vCenter Server instance where the published library is, or in a different vCenter Server system. In the Create Library wizard, you have the option to download all the contents of the published library immediately after the subscribed library is created, or to download only metadata for the items from the published library and later to download the full content of only the items you intend to use.

To ensure the contents of a subscribed library are up to date, the subscribed library automatically synchronizes to the source (published) library at regular intervals. You can also manually synchronize subscribed libraries.

You can use the option to download content from the source (published) library immediately or only when needed to manage your storage space.

Synchronization of a subscribed library that is set with the option to download all the contents of the published library immediately, synchronizes both the item metadata and the item contents. During synchronization, the library items that are new for the subscribed library are fully downloaded to the storage location of the subscribed library.

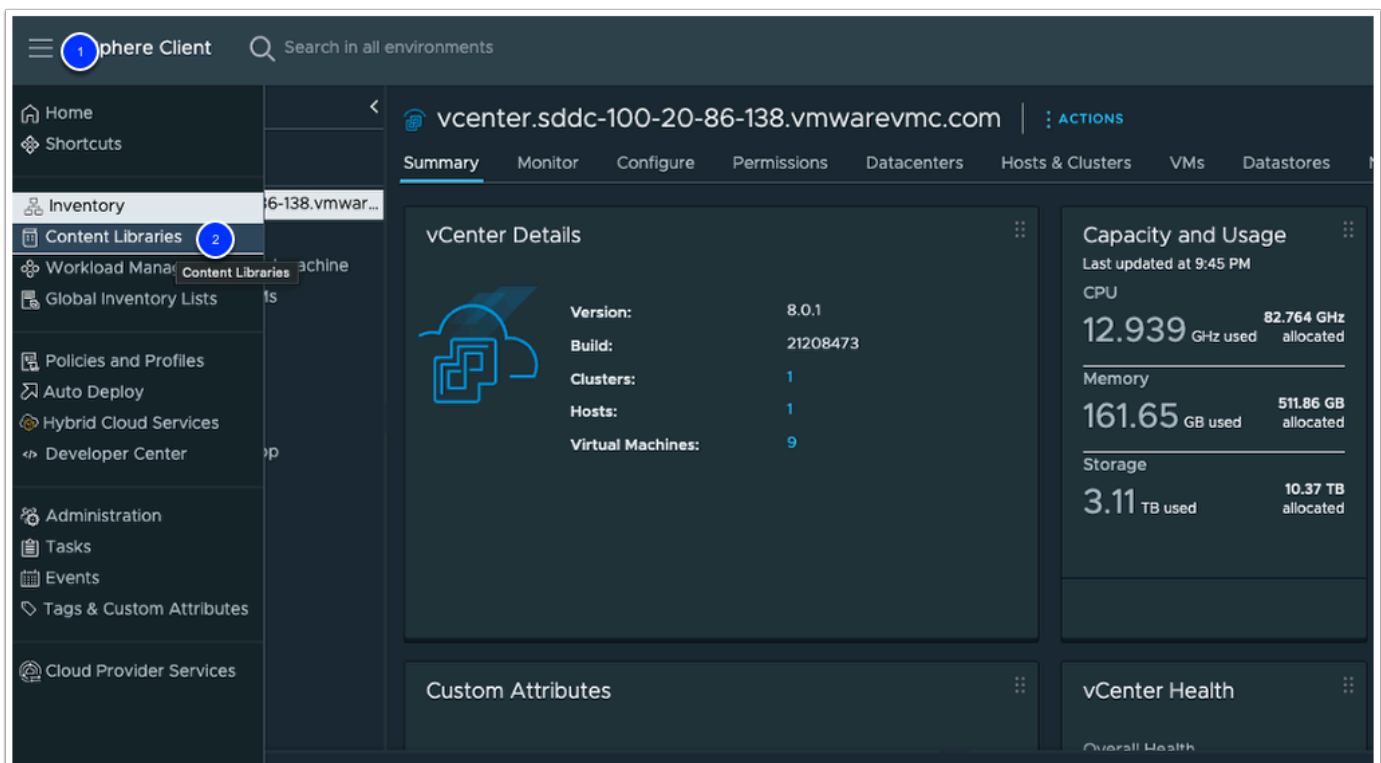
Synchronization of a subscribed library only downloads content when needed. It synchronizes the metadata for the library from the published library and does not

download the contents of the items. This saves storage space. If you need to use a library item, you need to synchronize that item. After you are done using the item, you can delete the item contents to free space on the storage. For subscribed libraries that are set with the option to download contents only when needed, synchronizing the subscribed library downloads only the metadata of all the items in the source published library, while synchronizing a library item downloads the full content of that item to your storage.

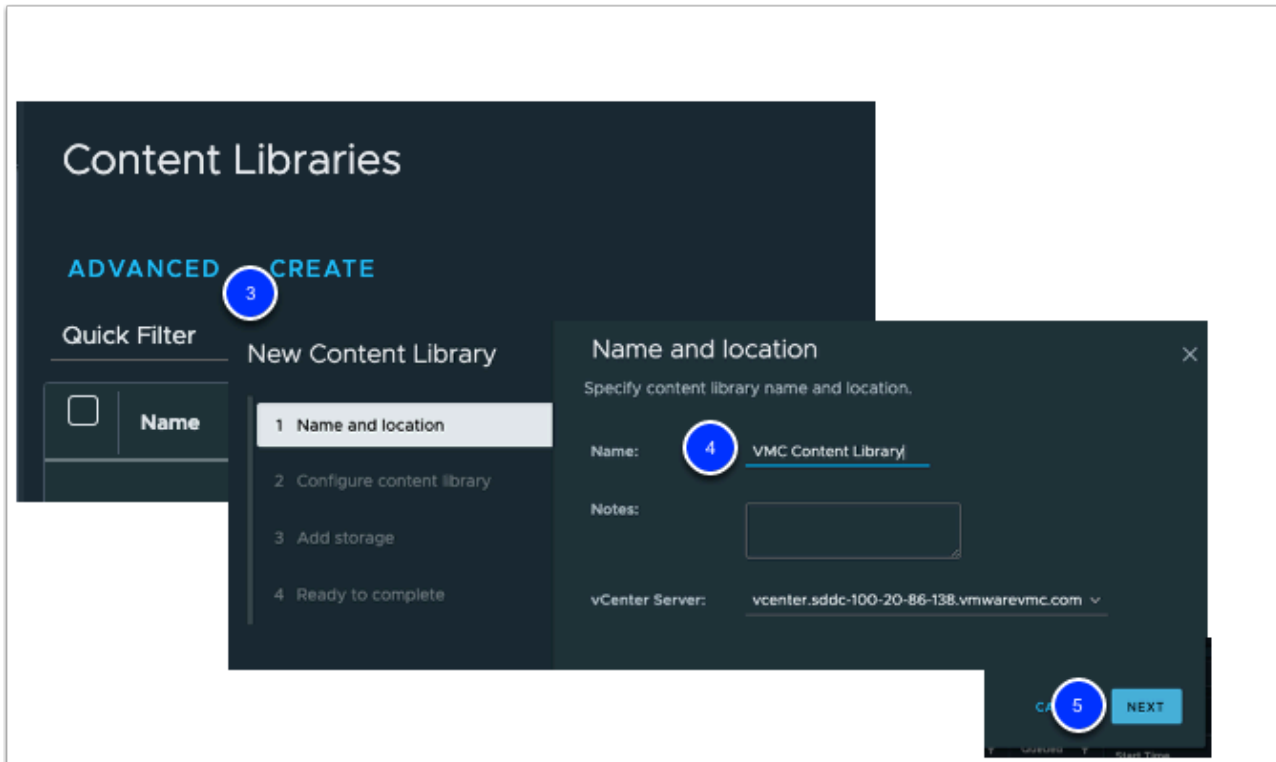
If you use a subscribed library, you can only utilize the content, but cannot contribute with content. Only the administrator of the published library can manage the templates and files.

A newly created VMC on AWS SDDC will have no Workload Virtual Machines pre-deployed, nor any of your corporate deployment images. Before you can begin deploying Virtual Machines based on your corporate-approved images into your SDDC you must first copy those images into the SDDC. One of the most effective ways to do so is to subscribe to a published vSphere Content Library. In this task, we will do just that.

1. In the Top Left of the page, click the **Menu Icon (3 dashes)** Also known as the "Hamburger Menu"
2. Click on **Content Libraries**



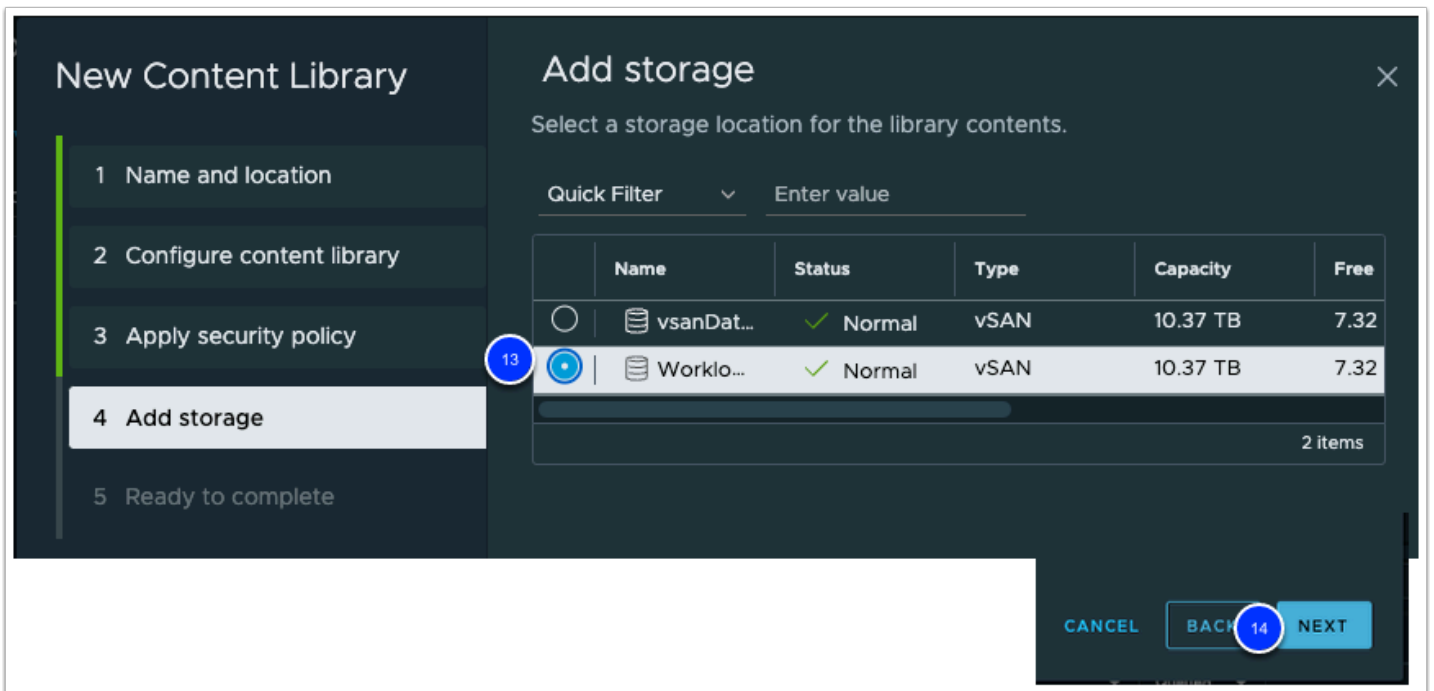
3. In your Content Library window, click **Create** to add a new Content Library
4. In the **Name and Location** section, enter **VMC Content Library** for the Name of the library. The other values should default to the appropriate selections.
5. Click the **NEXT** button.



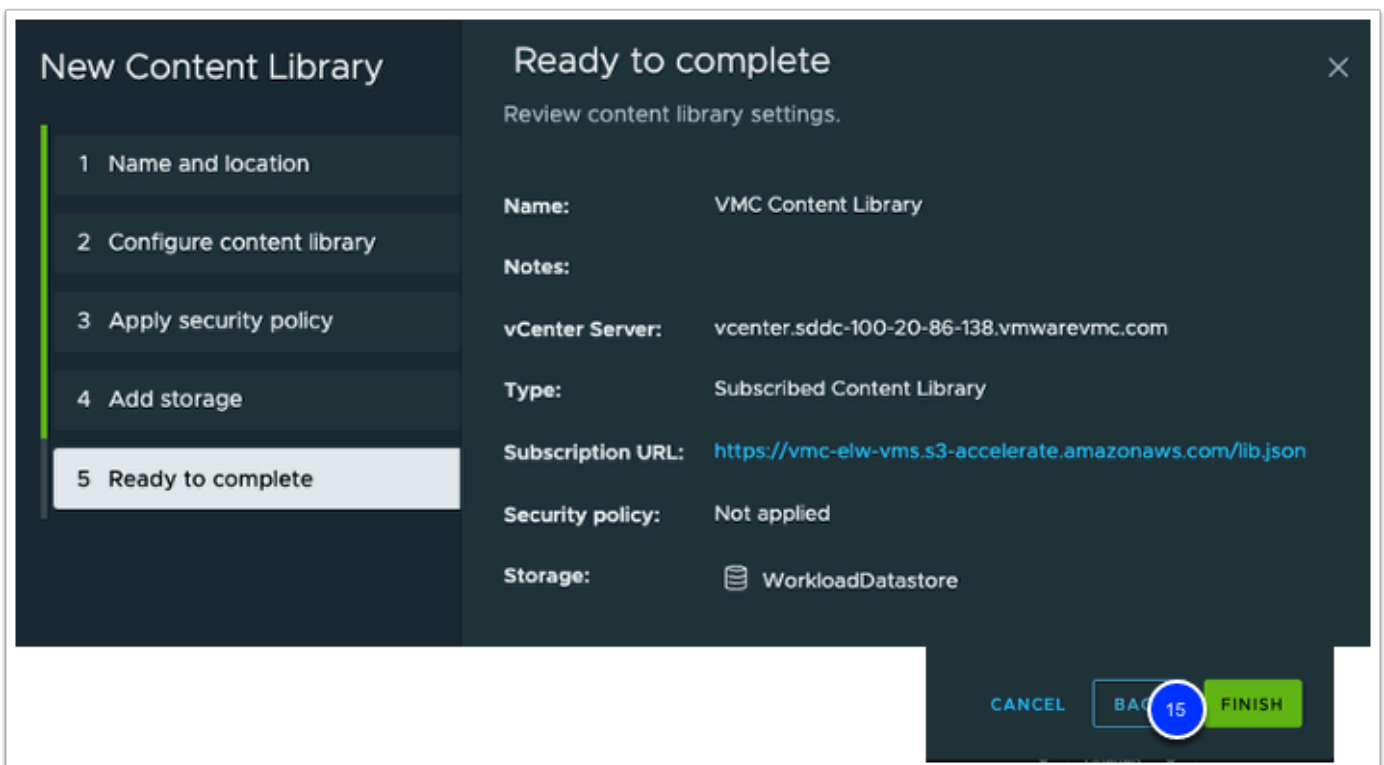
6. In the **Configure Content Library** section, select the radio button next to **Subscribed content library**.
7. Under **Subscription URL** enter the following: <https://vmc-elw-vms.s3-accelerate.amazonaws.com/lib.json>
8. **DO NOT** check the box next to **Enable Authentication**.
9. Make sure **Download content** is set to **immediately**.
10. Click **Next**
NOTE: If Prompted to accept the SSL Thumbprint, Click **Yes**.

11. On the **Apply Security Policy** Section, ensure that **Apply Security Policy** is **NOT checked**
12. Click **NEXT**

13. In the **Add Storage** section click on **WorkloadDatastore** for content library storage.
14. Click **NEXT**



15. In the **Ready to Complete** section verify that all the data matches the steps above then click **Finish**



💡 Depending the size and number of templates it can take a while to synchronize the content. We will proceed with task 5 while syncing. The sync of the "Photoapp-U"

virtual appliance must complete before moving to Task 6. You don't have to wait on "MonkeyIsland" & "VMC-Win10-Template" before proceeding to Task 6.

Task 5 - Create a Linux & Windows Customization Specification

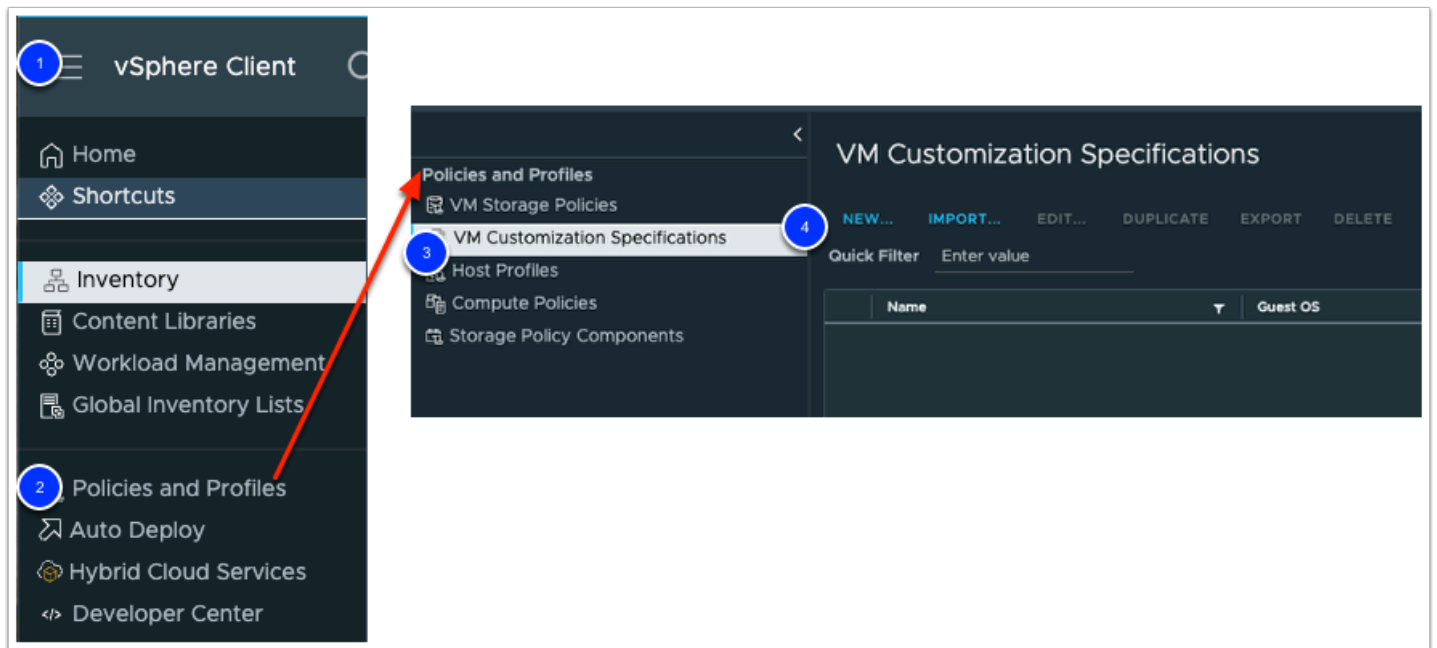
When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings.

Customizing guest operating systems can help prevent conflicts that can result if virtual machines with identical settings are deployed, such as conflicts due to duplicate computer names.

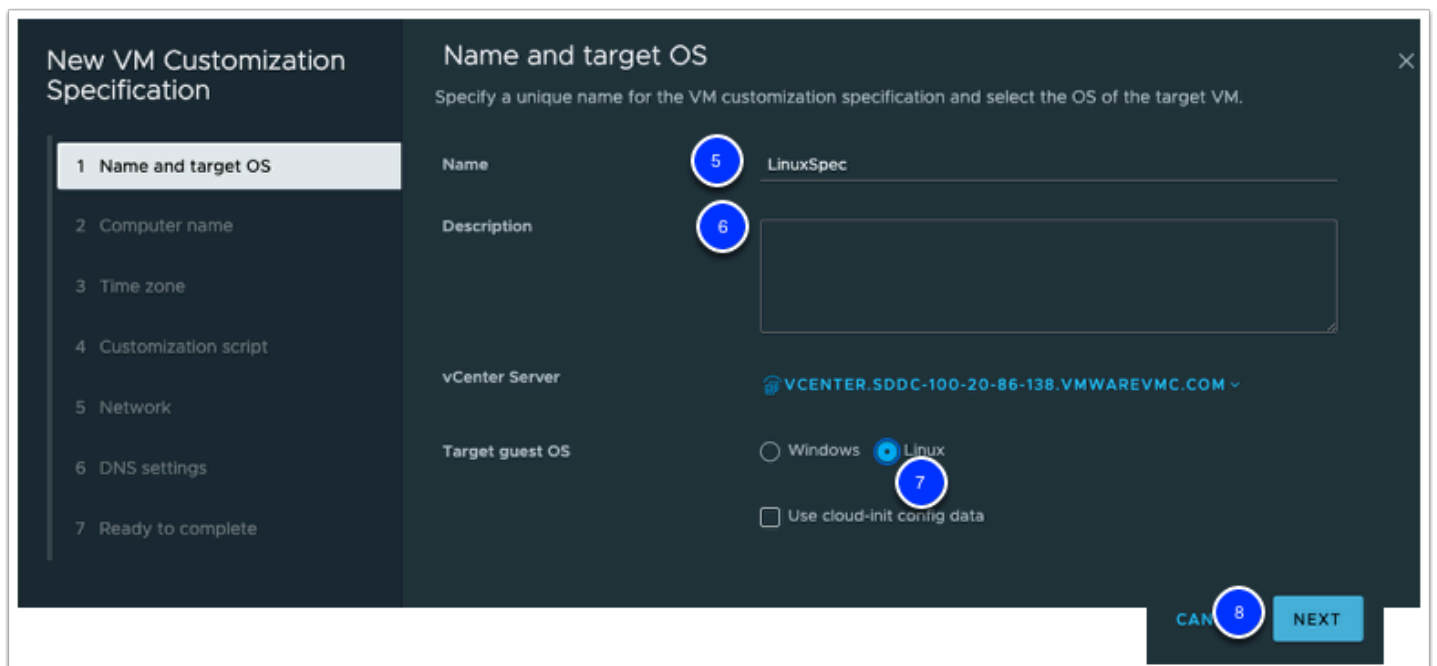
You can specify the customization settings by launching the Guest Customization wizard during the cloning or deployment process. Alternatively, you can create customization specifications, which are customization settings stored in the vCenter Server database. During the cloning or deployment process, you can select a customization to apply to the new virtual machine.

Use the Customization Specification Manager to manage customization specifications you create with the Guest Customization wizard.

1. From within vSphere client, click **Menu**.
2. In the menu dropdown click on **Policies and Profiles**.
3. Click the **VM Customization Specifications** menu item
4. Click on **New** to add a new Linux Customization Specification



5. **Name:** **LinuxSpec**
6. Optionally enter a **Description**.
7. Select the radio button for **Linux** next to **Target guest OS**.
8. Click **NEXT**



9. In the **Computer Name** section click the radio button next to **Use the virtual machine name**.
10. **Domain name:** **corp.local**
11. Click **Next**

Computer name

Specify a computer name that will identify this virtual machine on a network.

9 ☒ Use the virtual machine name i

☐ Enter a name in the Clone/Deploy wizard

☐ Enter a name

☐ Append a unique numeric value. i

☐ Generate a name using the custom application configured with the vCenter Server

Argument

Domain name 10

CANCEL 11 BACK NEXT

12. In the **Time Zone** section select **US** for **Area**
13. Location: **Eastern**
14. Click **Next**

Time zone

Specify a time zone for the virtual machine.

Area 12

Location

- Alaska
- Aleutian
- Arizona
- Central
- East-Indiana
- 13
- Hawaii
- Indiana-Starke
- Michigan
- Mountain
- Pacific
- Pacific-New
- Samoa

Hardware clock set to ☒ UTC ☐ Local time

CANCEL 14 BACK NEXT

15. Click **Next** to Skip the Customization Script page

16. On the **Network** section ensure the radio button next to **Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces** is selected.
17. Click **Next**

18. On the **DNS settings** section enter **8.8.8.8** for the Primary DNS server.
19. Enter **8.8.4.4** for the Secondary DNS server.
20. For the DNS Search paths enter **corp.local**.
21. Click the **Add** button to add the **corp.local** domain to the DNS search path. Verify that it was added.
22. Click **Next** to continue

DNS settings

Specify the DNS and domain information for the virtual machine.

DNS Servers

Primary DNS server

18

8.8.8.8

Secondary DNS server

19

8.8.4.4

Tertiary DNS server

DNS Search Paths

20

cor DNS search path

21

ADD

MOVE UP

MOVE DOWN

DELETE

corp.local

1 item

CANCEL

BACK

22

NEXT

23. Review your entries and click on the **Finish** button

Ready to complete

Review your settings before submitting.

Name	LinuxSpec
Description	
vCenter Server	vcenter.sddc-100-20-86-138.vmwarevmc.com
Target guest OS	Linux
Computer name	Use Virtual Machine name
Domain name	corp.local
Time zone	US/Eastern
	Hardware clock: Set to UTC
Customization script	Do not use customization script
Network type	Standard
DNS servers	8.8.8.8 (Primary)
	8.8.4.4 (Secondary)
DNS search paths	corp.local

CANCEL

BACK

23

FINISH

💡 Try to complete the steps below from memory, but if you have trouble use the steps above in task 2.4 modified with the following fields to create a Customization Specification for Microsoft Windows Virtual Machines

Note: Leave the default selection for any fields not mentioned below

24. **REPEAT STEPS** to create a Windows Customization Specification:

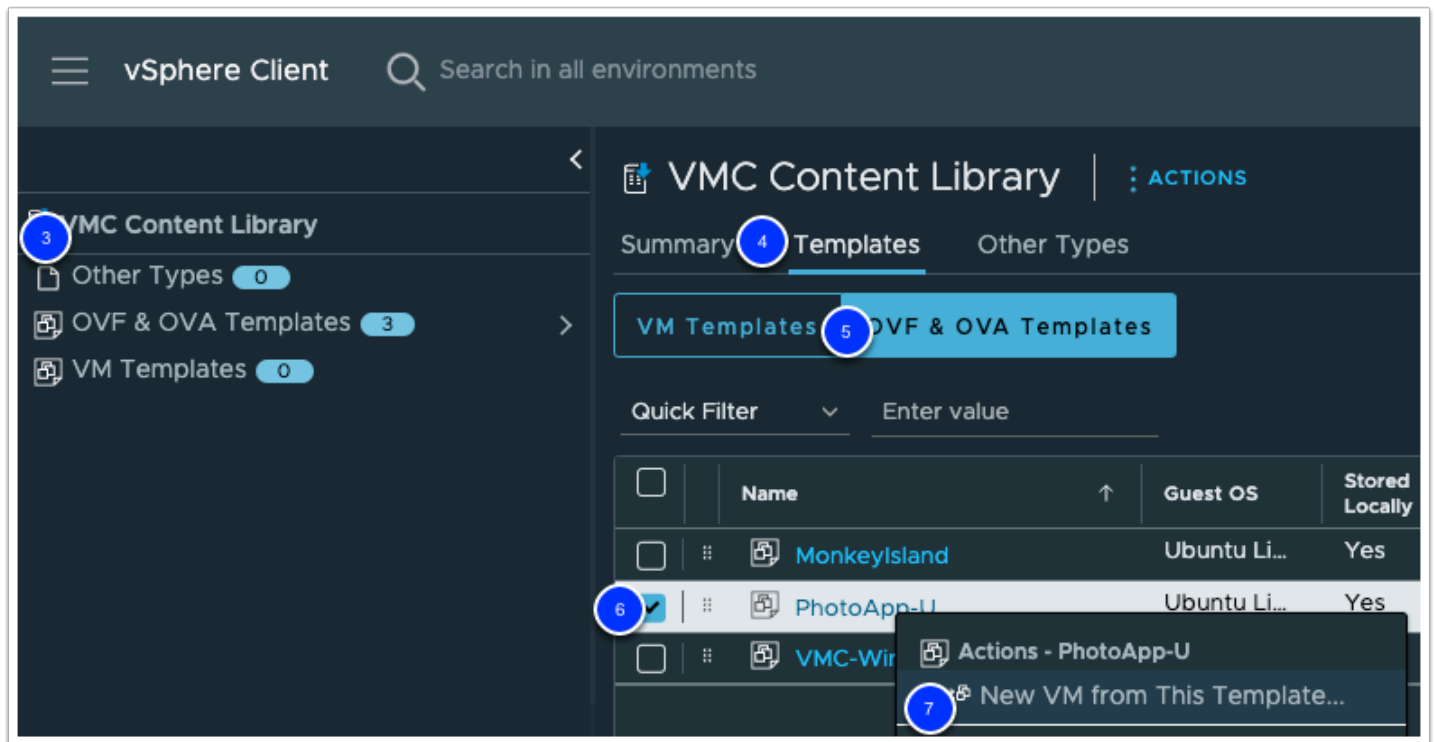
- Name and Target OS Page
 - **Name:** **WindowsSpec**
 - **Target guest OS:** **Windows**
- Registration Information Page
 - **Owner Name:** **(Your Name)**
 - **Owner Organization:** **(Your Organization)**
- Computer Name Page
 - **Computer Name:** **Select - Use the virtual machine name**
- Windows License Page
 - **Product Key** - Leave empty and click **NEXT**
- Administrator Password Page
 - **Password:** **VMware1!**
- Time Zone page
 - **Time Zone:** **(Select your timezone)**
- Click **Next**, leave defaults through the **Commands to Run Once, Network, Workgroup or Domain**. Then click **Finish** on the "ready to complete" section.

Task 6 - Deploy Virtual Machine from template

In the vSphere client window already opened, you will deploy a Virtual Machine from a template in the content library. You'll then clone the deployed Virtual Machine to create a second VM. In both cases you will use the Customization Specification you created in task 2 to modify the Operating System configuration.

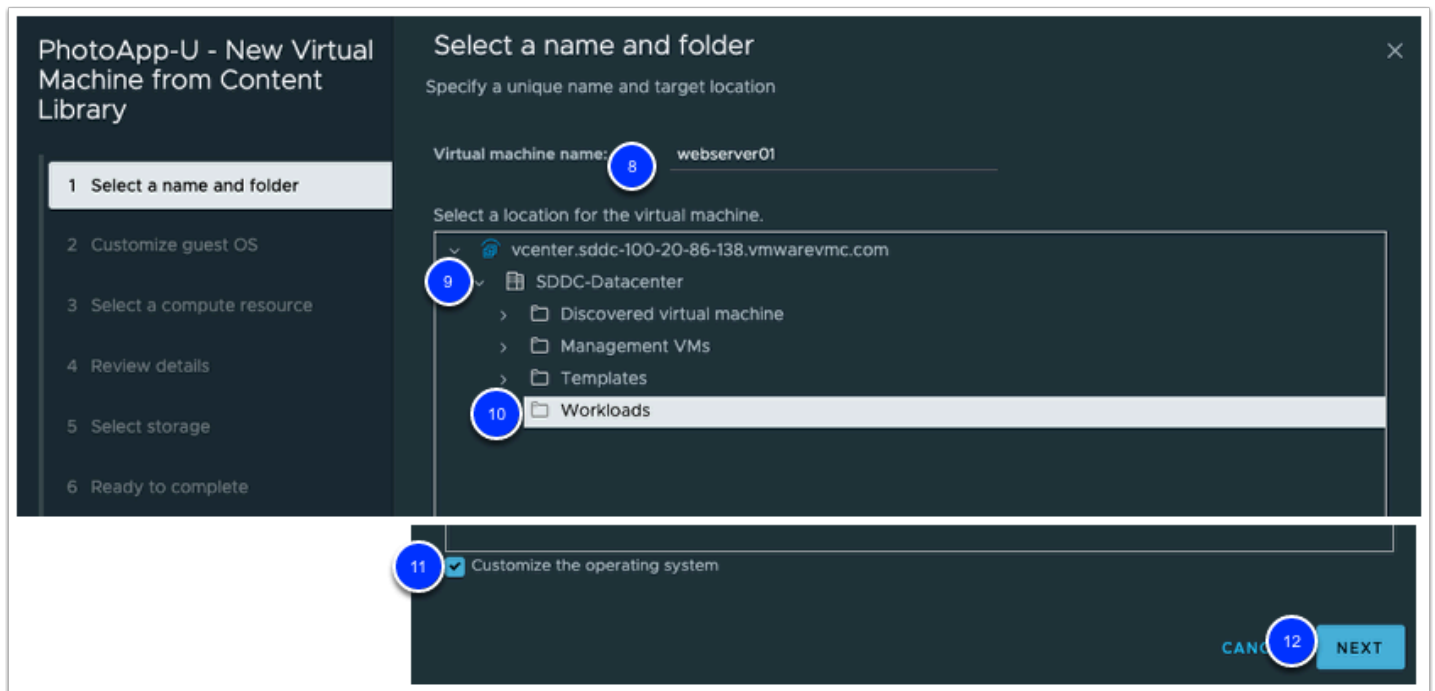
1. Click **Menu**.
2. Click on **Inventory --> Content Libraries**.
3. Click on the **VMC Content Library** that was previously synchronized.
4. Click the **Templates** tab to access the template synchronized in the content library.
5. Click the **OVF & OVA Templates** tab

6. Right-click on the **Photoapp-U** template to expose the Actions menu.
7. Click on **New VM from This Template** to deploy a virtual machine from template.

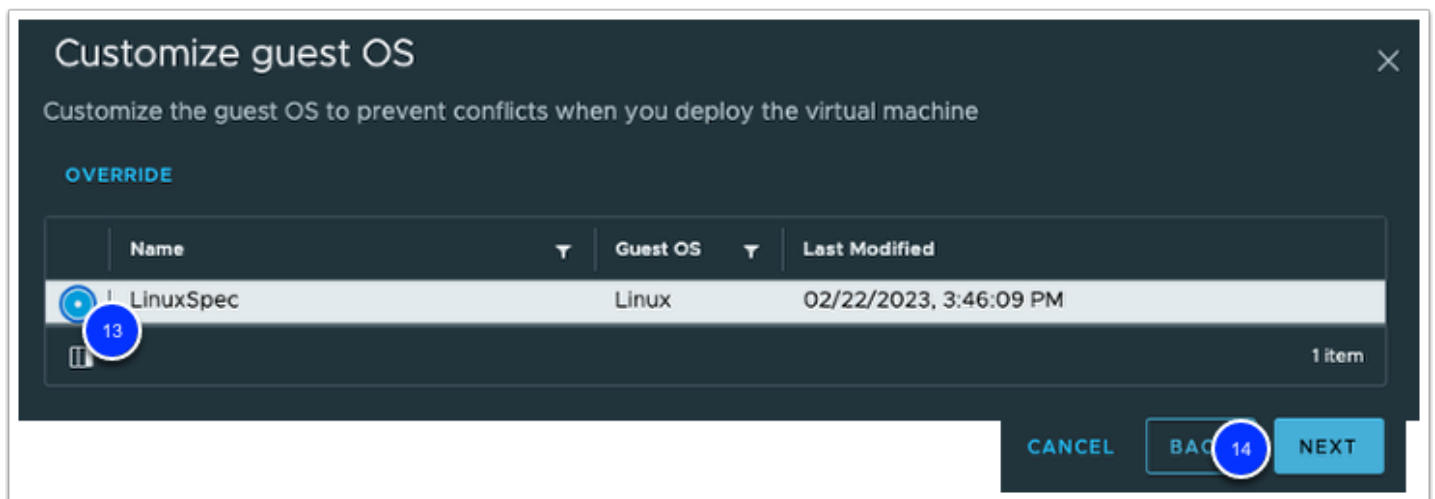


8. In the Select **Name and Folder** section enter **webserver01** for the virtual machine name.
9. Click the **arrow** next to **SDDC-Datacenter** to expose the folders available.
10. Click the **Workloads** folder.
11. Select the checkbox next to **Customize the operating system**.
12. Click **Next** to continue

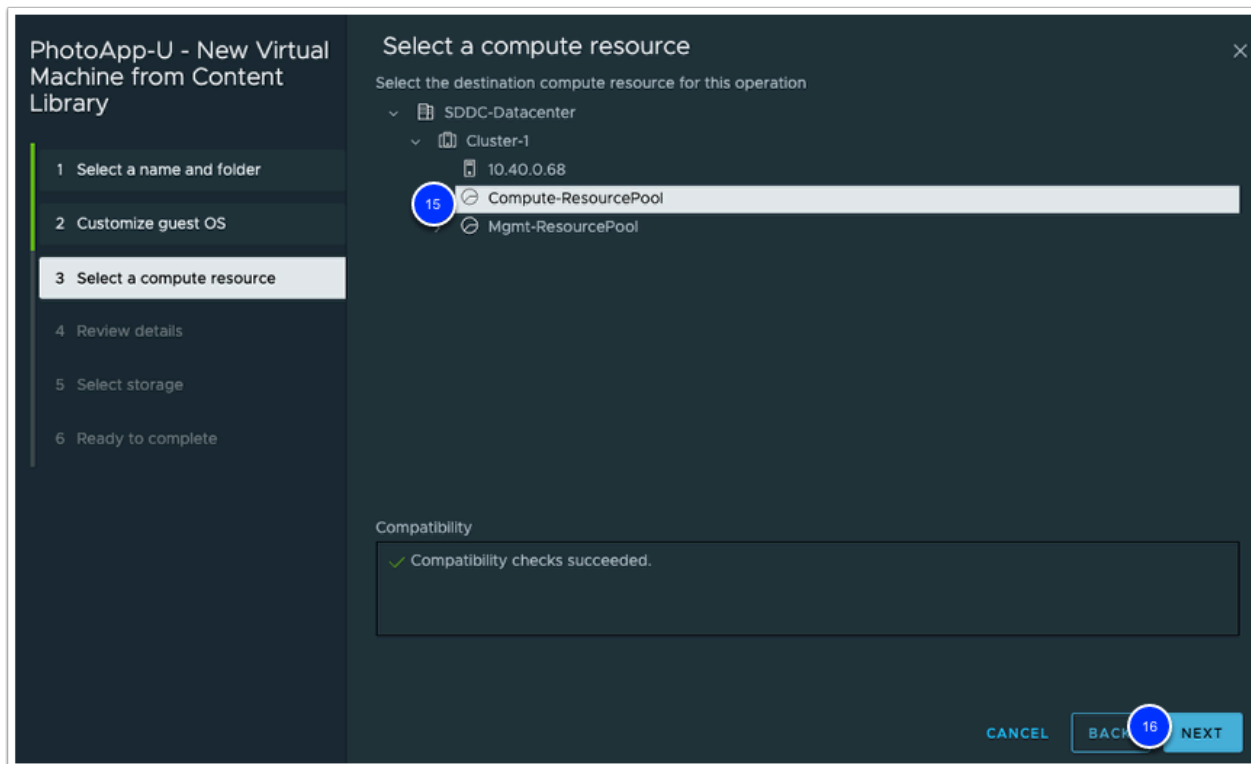
💡 In VMware Cloud on AWS customer workloads should be placed in the **Workloads** folder.



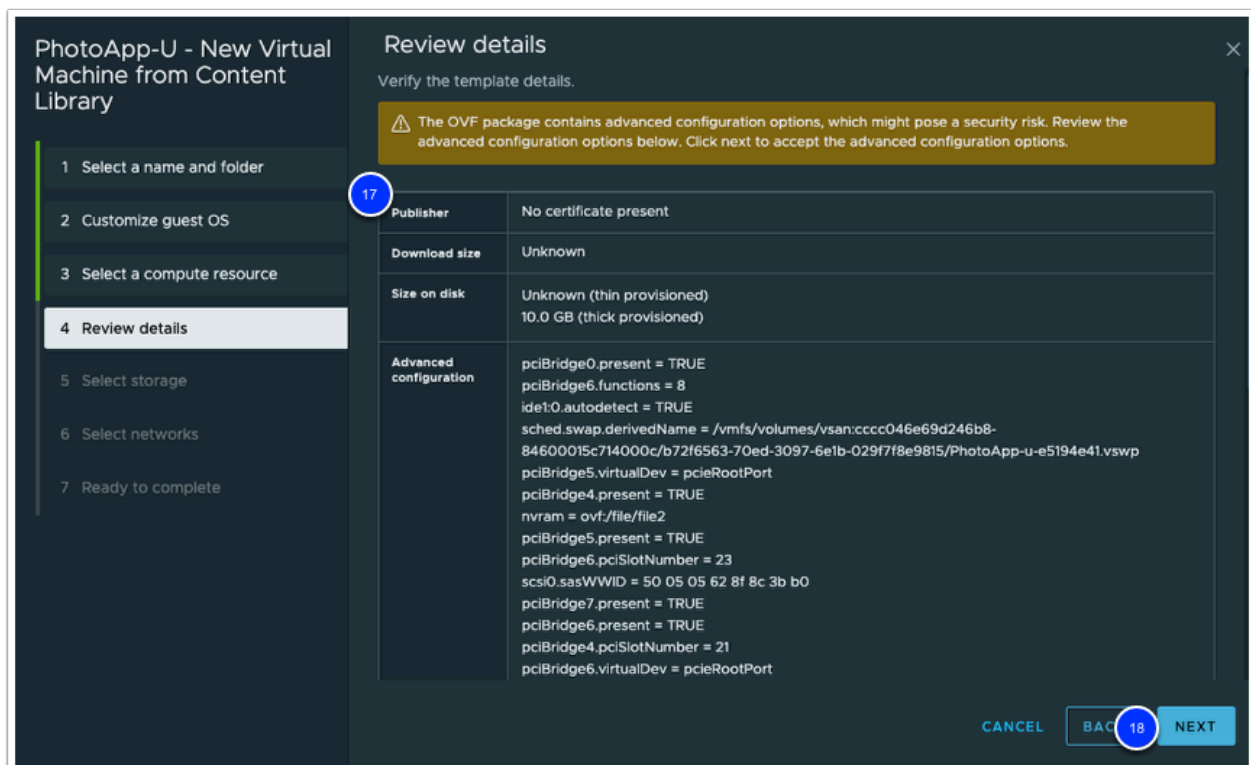
13. On the Customize guest OS page, select **LinuxSpec** customization specification.
14. Click **Next** to continue.



15. In the **Select a Compute Resource** section, click the arrow next to **Cluster-1** to expose the resource pools available.
Select **Compute-ResourcePool**.
In VMware Cloud on AWS customer workloads should be placed in the **Compute-ResourcePool** (or a sub-pool).
16. Click **Next** to continue



17. Review the details of the template to be deployed. There may be a security warning displayed, but you can safely ignore that for the purpose of this lab.
18. Click **Next** to continue.



19. In **Select Storage** Click **WorkloadDatastore** to select the datastore where the virtual machine will be provisioned.

20. Click **Next** to continue

💡 Each VMware Cloud on AWS SDDC will include two datastores in order to separate management and customer workloads. All customer workloads must be placed in the datastore named WorkloadDatastore

Select storage

Select the storage for the configuration and disk files

BATCH CONFIGURE **CONFIGURE PER DISK GROUP**

☐ Encrypt this virtual machine ⓘ

Select virtual disk format As defined in the VM storage policy ▾

VM Storage Policy **Datastore Default ▾**

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Plac
<input type="radio"/>	vsanDatastore	--	10.37 TB	6.22 TB	7.29 TB	vSAN	Loc
<input checked="" type="radio"/>	WorkloadDatastore...	--	10.37 TB	3.08 TB	7.29 TB	vSAN	Loc

Items per page 10 ▾ 2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **20** **NEXT**

21. Click the drop-down below **Destination Network** to select the network for the virtual machine.

22. Click **Browse...**, then Select **Demo-Net** the network previously created in Task 1.

23. Click **Next**

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Demo-Net	Demo-Net ▾

1 item

CANCEL **BACK** **23** **NEXT**

24. Review the information for accuracy and click **Finish** to deploy the virtual machine

⚠ It should take a couple of minutes for the virtual machine to deploy. Continue to the next task to clone this virtual machine to create a second web server.

PhotoApp-U - New Virtual Machine from Content Library

1 Select a name and folder
2 Customize guest OS
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Ready to complete

✓ Select a name and folder

Name	webserver01
Template name	PhotoApp-U
Folder	Workloads

✓ Customize guest OS

Guest OS customization specification	LinuxSpec
--------------------------------------	-----------

✓ Select a compute resource

Resource	Compute-ResourcePool
----------	----------------------

✓ Review details

Download size	Unknown
---------------	---------

✓ Select storage

Size on disk	10.0 GB
Storage mapping	1
All disks	Datastore: WorkloadDatastore; Format: As defined in the VM storage policy

✓ Select networks

Network mapping	1
Demo-Net	Demo-Net

CANCEL BACK FINISH

24

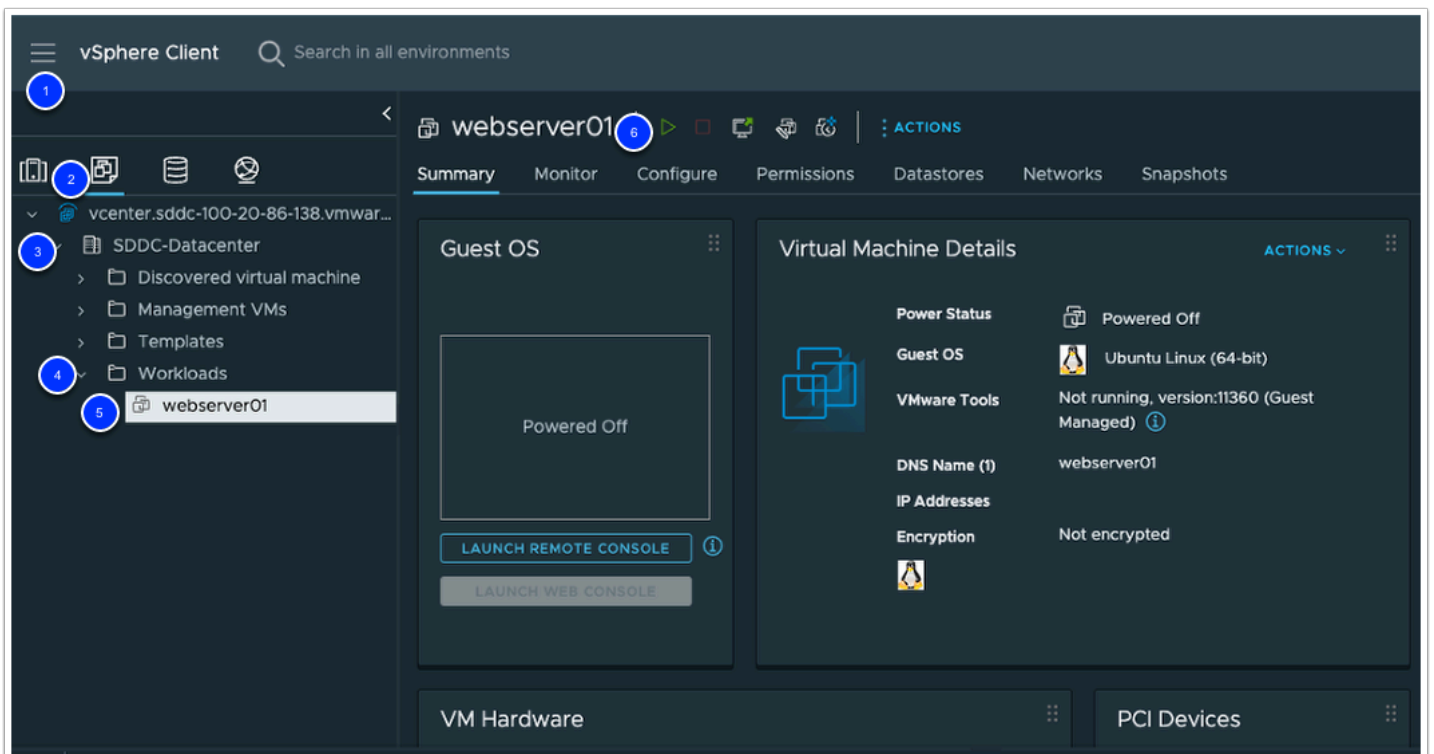
Task 7 - Clone a Virtual Machine

You will now create your second Virtual Machine by cloning the previously deployed Virtual machine (**webserver01**).

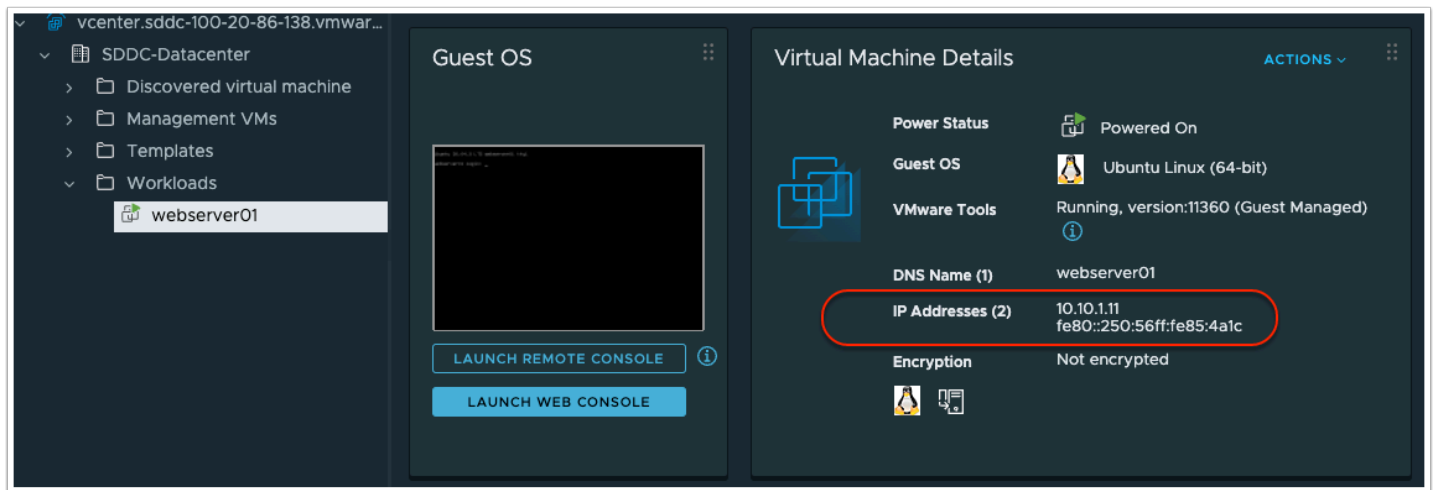
⚠ Validate the virtual machine deployment completed in the previous exercise by looking for the **Deploy OVF Template** task, verify it is Completed successfully. Once completed you may move on to the steps listed below. You will start by powering on the previously deployed VM to allow the OS customization to proceed. If the deployment failed please notify your instructor or go back through the steps listed in Task 3.1 again.

<input type="checkbox"/>	>	Customize virtual m...	webserver01	Completed	vpzd-extension-Oa449786...	2 ms	02/22/2023, 4:08:18...	02/22/2023, 4:08:19...	1 s
<input type="checkbox"/>	>	Check customizatio...	webserver01	Completed	vpzd-extension-Oa449786...	3 ms	02/22/2023, 4:08:18...	02/22/2023, 4:08:18...	5 ms
<input type="checkbox"/>	>	Transfer file(s)	10.40.0.68	Completed	vpzd-extension-Oa449786...	3 ms	02/22/2023, 4:08:10...	02/22/2023, 4:08:15...	4 s
<input type="checkbox"/>	>	Deploy OVF template	webserver01	Completed	vpzd-extension-Oa449786...	5 ms	02/22/2023, 4:07:5...	02/22/2023, 4:08:18...	22 s
<input type="checkbox"/>	>	com.vmware.ovfs.LI...	Compute-ResourcePo...	Completed	cloudadmin@vmc.local	87 ms	02/22/2023, 3:59:0...	02/22/2023, 4:08:19...	9 m 14 s

1. Click **Menu**.
2. Click on **VMs and Templates**.
3. Click the **arrow** next to **SDDC-Datacenter** to expose the sub-folders.
4. Click the **arrow** next to **Workloads** to expose **webserver01**
5. Click on the virtual machine **webserver01**
6. Click the **green arrow** at the top center of the screen to power on the VM



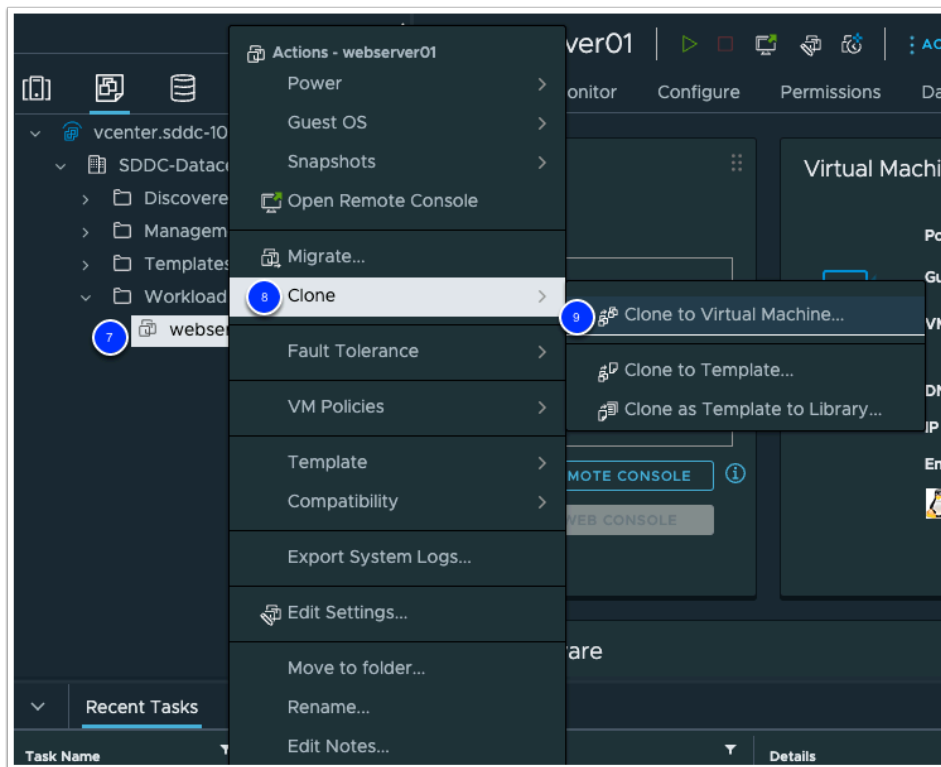
⚠ Note: Please wait until the virtual machine is fully powered on and has an IP before proceeding to the next step.



- ⚠ If webserver01 does not connect to the network and does not receive an IP address from DHCP, follow these steps. 1) Hit refresh on the page a few times. 2) Ensure the NIC is connected by right-clicking on webserver01 and then Edit Settings and make sure the checkbox next to Connected is selected.

You may need to repeat this step for the cloned VM webserver02

7. Right-click on **webserver01** to expose the Actions menu.
8. Click on **Clone**
9. Click **Clone to Virtual Machine**



10. Next to **Virtual machine name** enter **webserver02**.
11. Click the **arrow** next to **SDDC-Datcenter** to expose the folders available.
12. Click the **Workloads** folder for the virtual machine location.
13. Click **Next** to continue.
14. Click the **arrow** next to **Cluster-1** to expose the resource pools available
15. Click on **Compute-ResourcePool** to ensure it is selected for the target virtual machine.
16. Click **Next** to continue.
17. Click on **WorkloadDatastore** to ensure it is selected as the destination for the virtual machine.
18. Click **Next** to continue.
19. Click the checkbox next to **Customize the operating system**.
20. Click the checkbox next to **Power on virtual machine after creation**.
21. Click **Next** to continue.
22. Select the **LinuxSpec** customization specification.
23. Click **Next** to continue.
24. Review the information for accuracy and click **Finish** to clone the virtual machine.

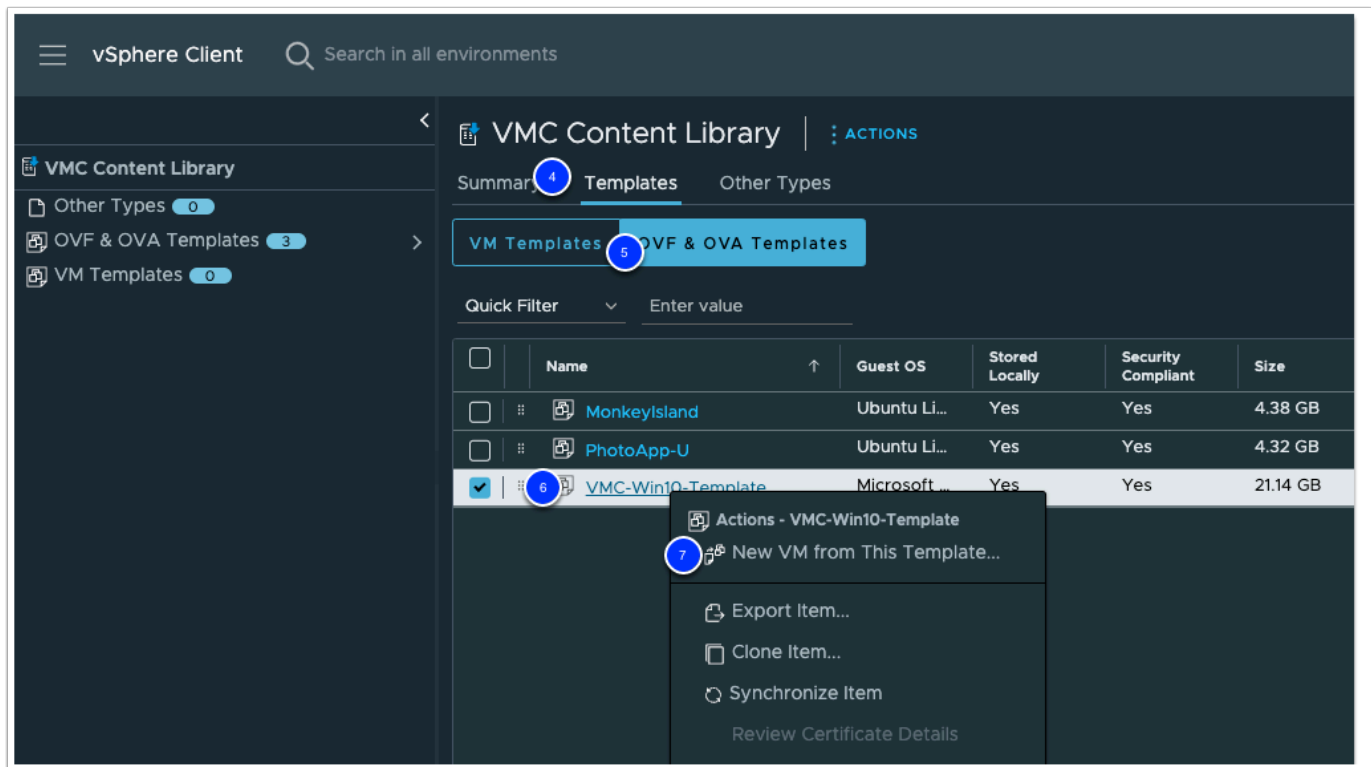


⚠ It should take a couple of minutes for the virtual machine to clone. Continue to the next exercises to deploy a windows VM and learn about securing workloads in VMware Cloud on AWS.

Task 8 - Deploy a Windows 10 Virtual Machine

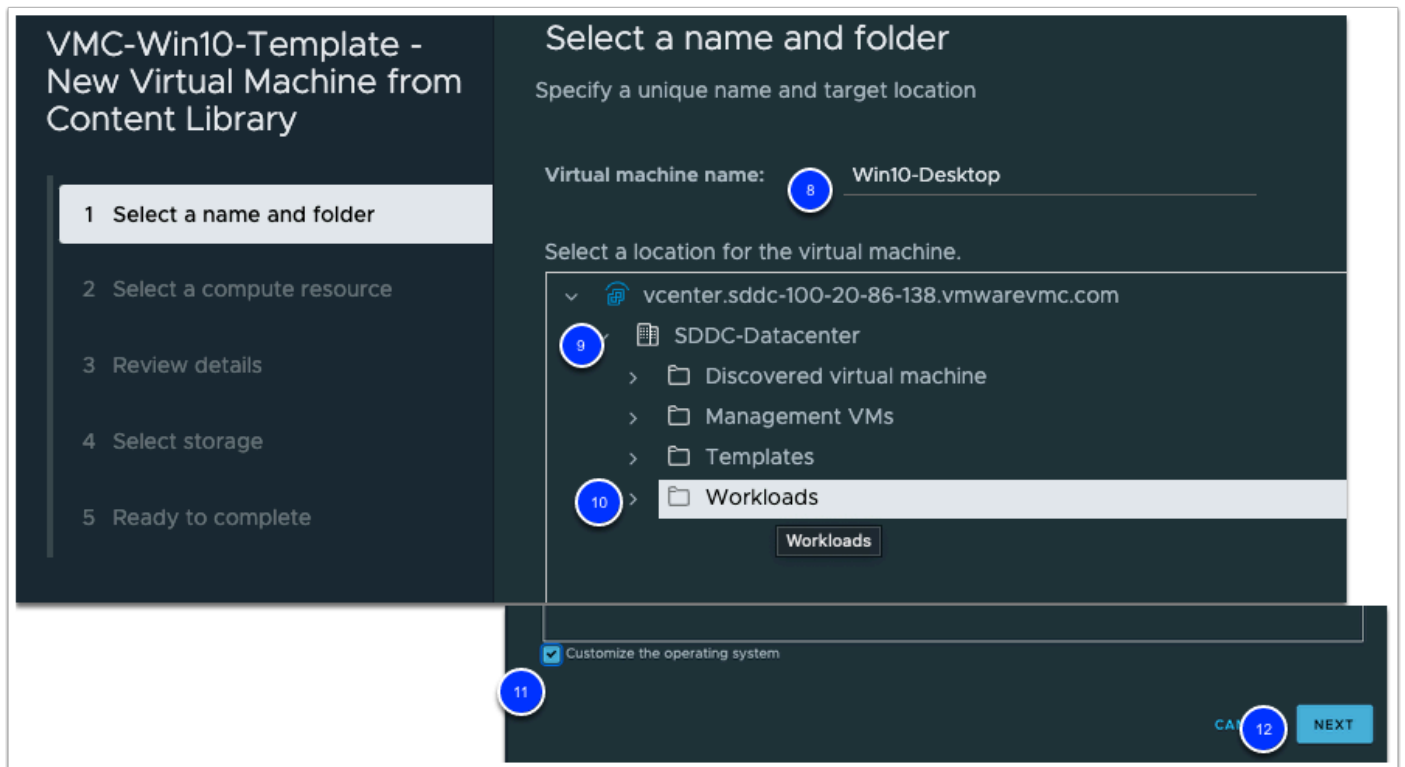
In this task you will deploy and customize a Windows 10 Virtual Machine from the VMC Content Library

1. Click the **Menu Icon** in the upper left.
2. Click on **Content Libraries**.
3. Click on the **VMC Content Library** that was previously synchronized.
4. Click the **Templates** tab to access the template synchronized in the content library.
5. Click the **OVF & OVA Templates** Tab
6. Right-click on the **VMC-Win10-Template** to expose the **Actions** menu.
7. Click on **New VM from This Template** to deploy a virtual machine from template.

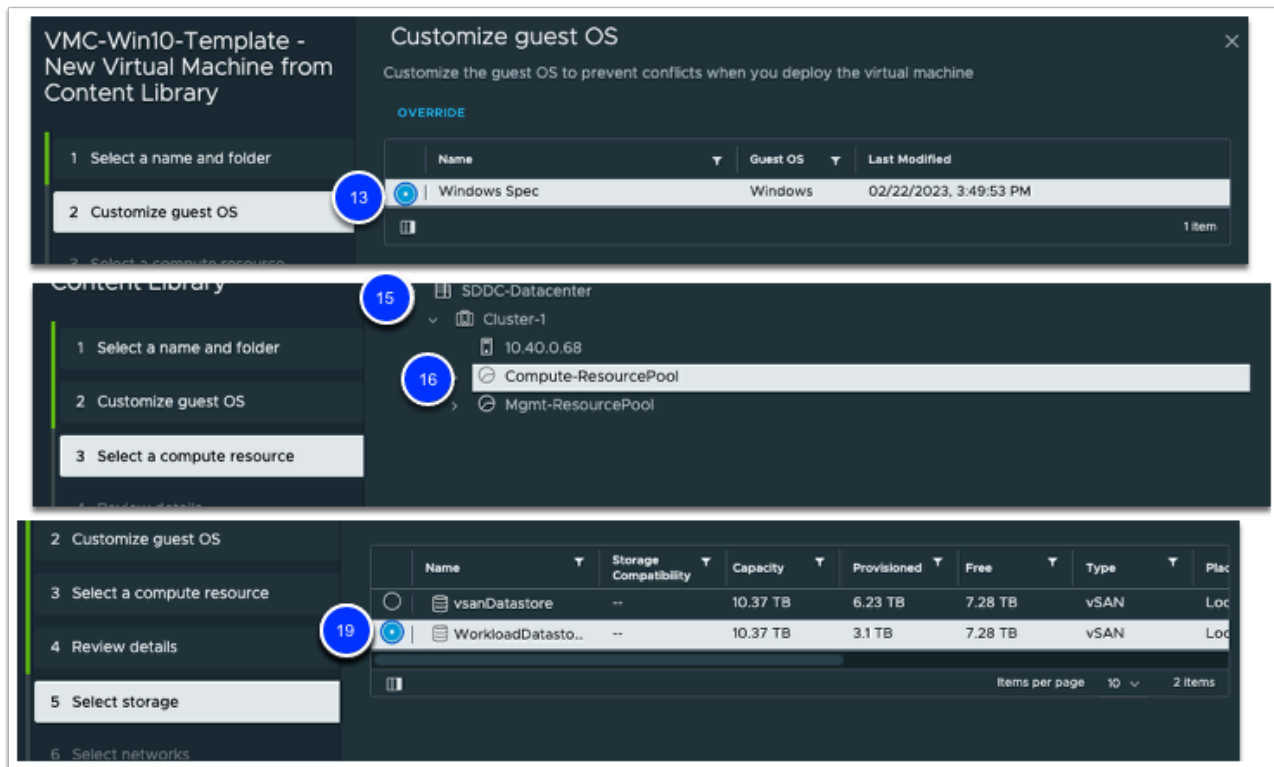


8. Enter **Win10-Desktop** for the virtual machine name.
9. Click the **arrow** next to SDDC-Datcenter to expose the folders available.
10. Click the **Workloads** folder.
11. Select the checkbox next to **Customize the operating system**.
12. Click **Next**

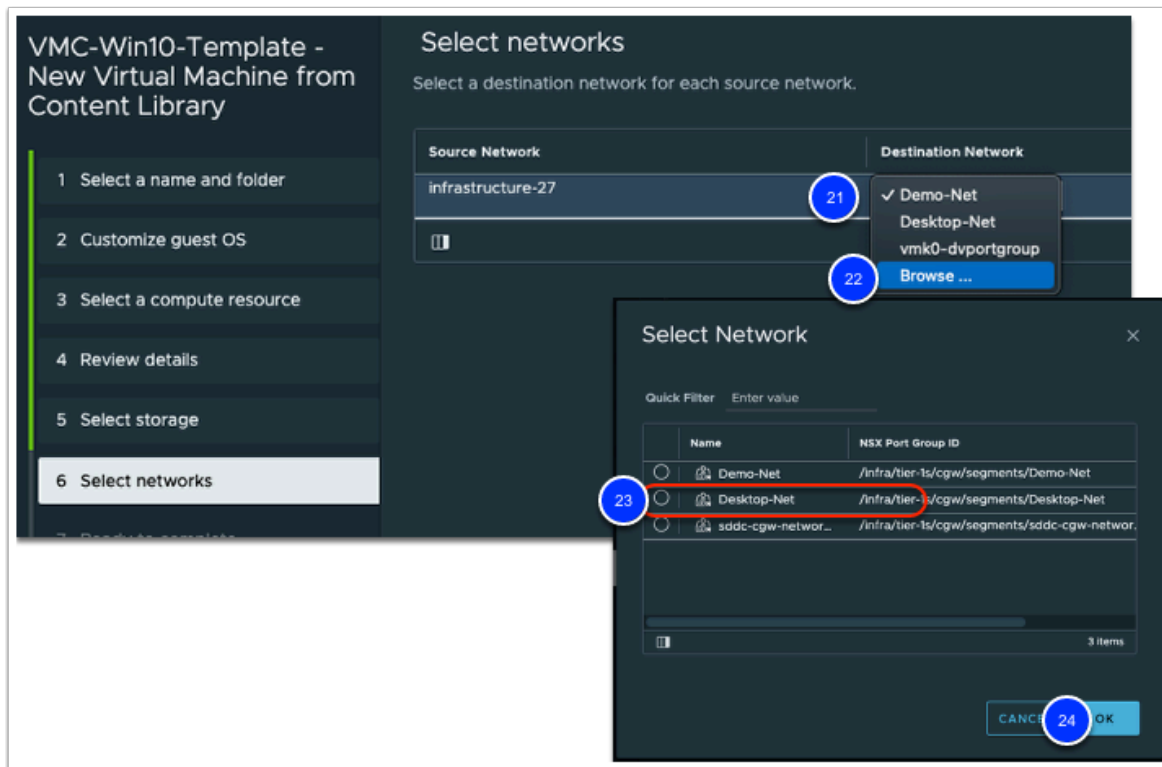
💡 In VMware Cloud on AWS customer workloads should be placed in the Workloads folder (or subfolder).



13. On the Customize guest OS page, select **WindowsSpec** customization specification.
14. Click **Next** to continue.
15. Click the arrow next to **Cluster-1** to expose the resource pools available.
16. Select **Compute-ResourcePool**.
17. Click **Next**
18. Click **Next** after reviewing details.
19. Click **WorkloadDatastore** to select the datastore where the virtual machine will be provisioned.
20. Click **Next**



21. Click the arrow below **Destination Network** to select the network for the virtual machine.
22. Click **Browse**
23. Choose **Desktop-Net** to select the network previously created.
24. Click OK
25. Click **Next** to continue.
26. Review the information for accuracy and click **Finish** to deploy the virtual machine



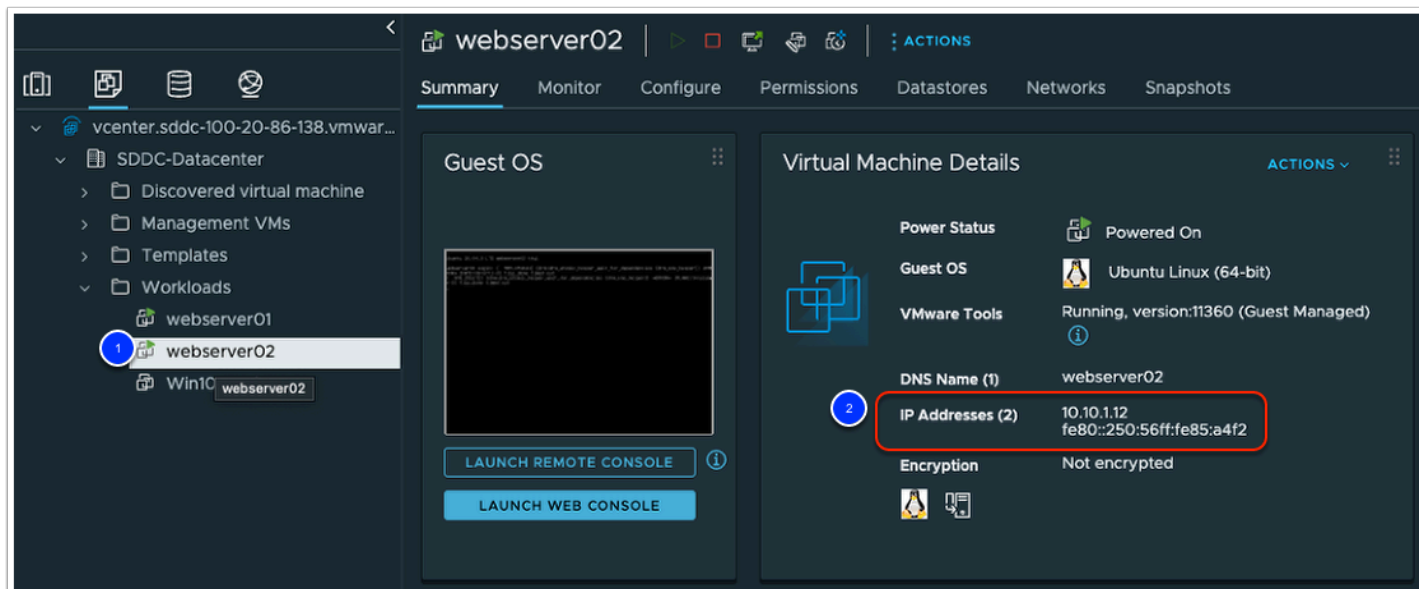
25. Power-on the Windows 10 desktop once the deployment is complete.

NOTE: You can expand the Recent Tasks & Events Pane at the bottom of the vSphere Client interface to view the deployment process/state

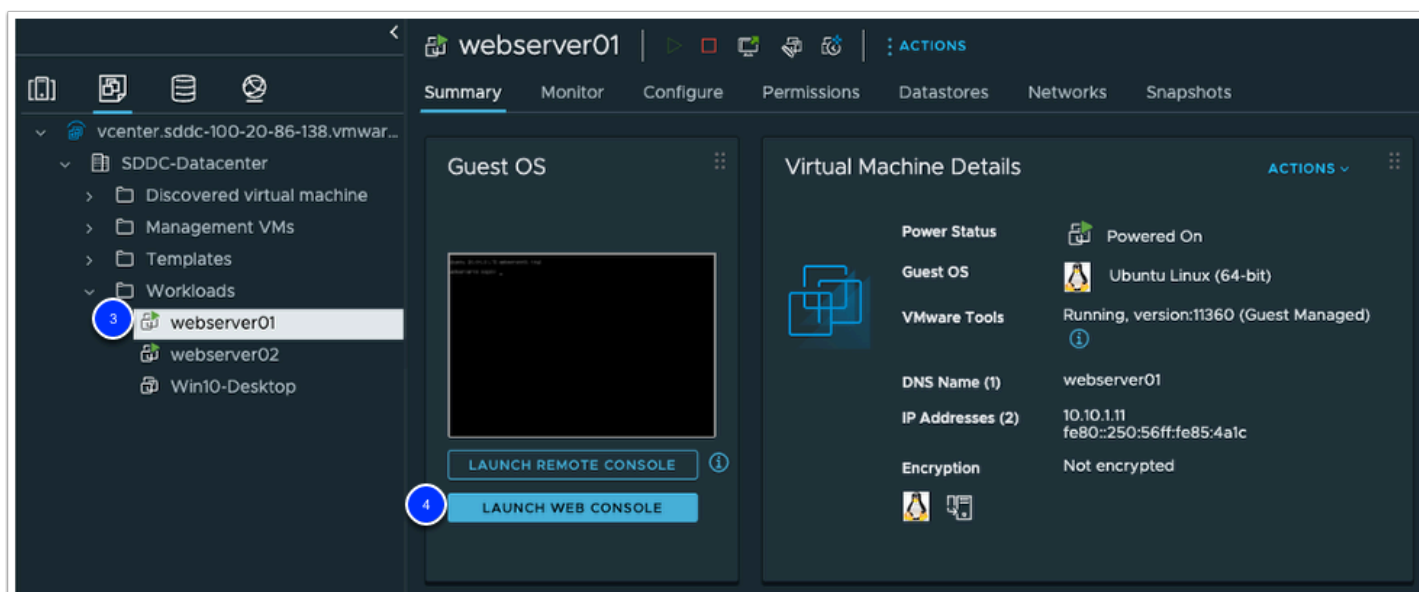
Task 9 - Test Connectivity between the Virtual Machines

In this exercise we will test the connectivity between webserver01 and webserver02, which we created in the previous exercises. You will need to open a console session to webserver01 to validate it can communicate with webserver02.

1. In the vSphere Client (HTML5) click on **webserver02** to bring it into focus. (You may need to Navigate to **Menu > Inventory > VMs and Templates**)
2. Note the IP address of **webserver02**



3. Click on **webserver01** to bring it into focus.
4. Click on **LAUNCH WEB CONSOLE**



5. At the login prompt enter **root** and press Enter.
6. At the password prompt enter **VMware1!** and press Enter.
7. At the console prompt, enter **ping -c3 <Your WebServer02 IP> i.e. 10.10.1.12** (you recorded webserver02 IP in step 5) and press **Enter**.
8. The third octet is based on student number and the last octet of the IP address in most cases it will be 12, but verify this in your configuration.
9. Verify the pings are successful.

```
to check for new updates (any) sudo apt update  
Last login: Fri Nov  4 11:50:32 EDT 2022 on tty1  
root@webserver01:~# ping -c3 10.10.1.12  
PING 10.10.1.12 (10.10.1.12) 56(84) bytes of data.  
64 bytes from 10.10.1.12: icmp_seq=1 ttl=64 time=1.28 ms  
64 bytes from 10.10.1.12: icmp_seq=2 ttl=64 time=0.331 ms  
64 bytes from 10.10.1.12: icmp_seq=3 ttl=64 time=0.247 ms  
  
--- 10.10.1.12 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2021ms  
rtt min/avg/max/mdev = 0.247/0.618/1.278/0.467 ms  
root@webserver01:~#
```

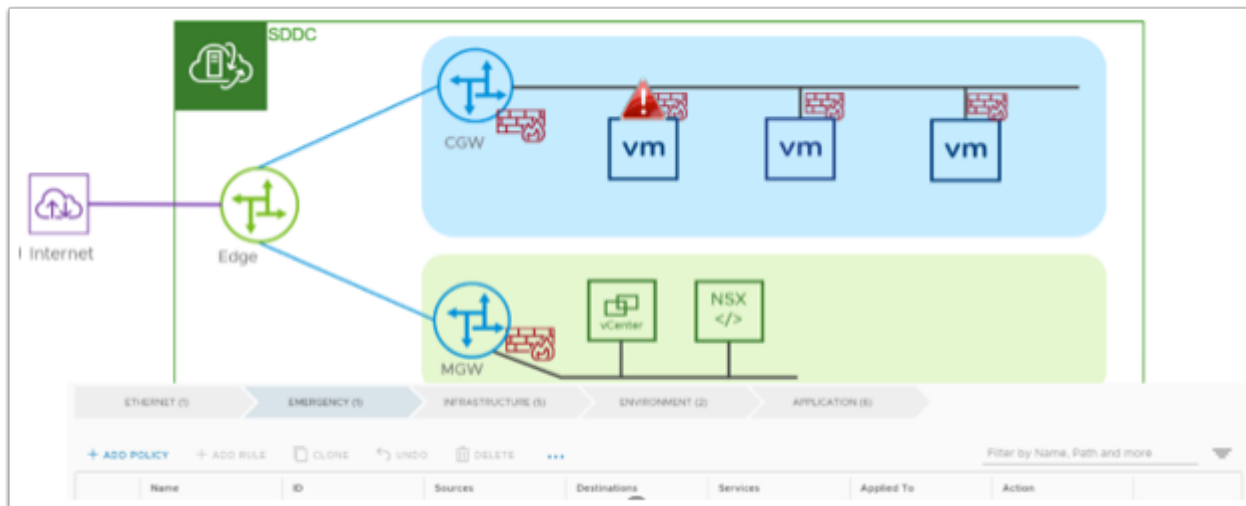
NOTE: Please leave this ping and console Window open for the next lesson. We will revisit it to verify the web servers can no longer communicate.

Task 10 - Configure Distributed Firewall Rules

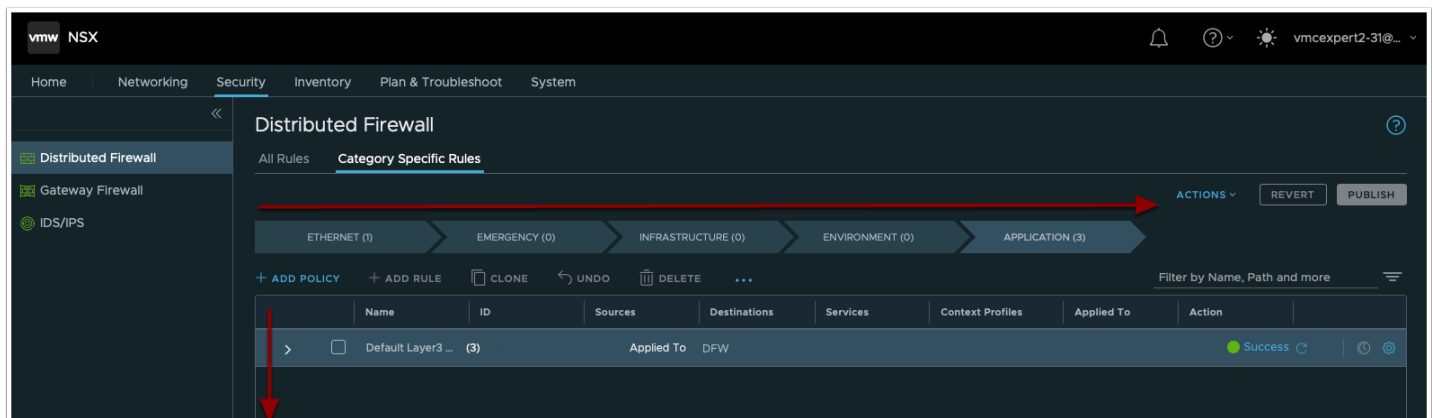
VMware Cloud on AWS Advanced Network Services is now available for new SDDC deployments.

Using VMware Cloud on AWS Advanced Network Services, users can implement micro-segmentation with Distributed Firewall. Granular security policies can be applied at the VM-level allowing for segmentation within the same L2 network or across separate L3 networks. This is shown in the diagram below.

All networking and security configuration is now done through the VMware Cloud on AWS console via the Networking & Security tab, including creating network segments. This provides ease of operations and management by having all networking and security access through the console.



From the below screenshot, you can see, in addition to the ability to create multiple sections, users can organize Distributed Firewall rules into groups (Emergency Rules, Infrastructure Rules, Environment Rules, and Application Rules). The categories are processed from left to right, the rules from the top down.



In addition to the Distributed Firewall capabilities, grouping objects can now be leveraged within security policies. Security groups support the following grouping criteria/constructs:

- IP Address
- VM Instance
- Matching criteria of VM Name
- Matching Criteria of Security Tag

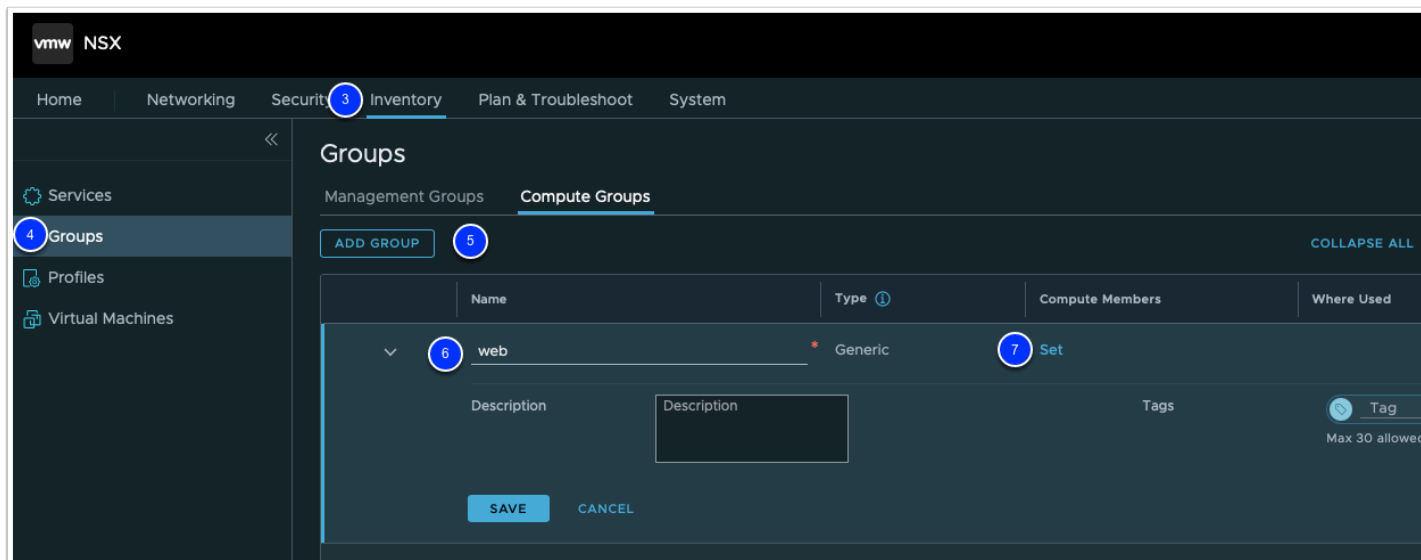
💡 As shown below, Security Groups can be created under **Compute Groups** or **Management Groups**. **Compute Groups** can be used in **DFW** and **CGW** firewall policies and **Management Groups** can be used under **MGW** firewall policies. Management Groups only support IP addresses as these groups are infrastructure based. Predefined Management Groups already exist for vCenter, ESXi hosts, and NSX Manager. Users can also create groups here based on IP address for on-premises ESXi hosts, vCenter, and other management appliances.

Task 10.1 - Create a Dynamic Security Group

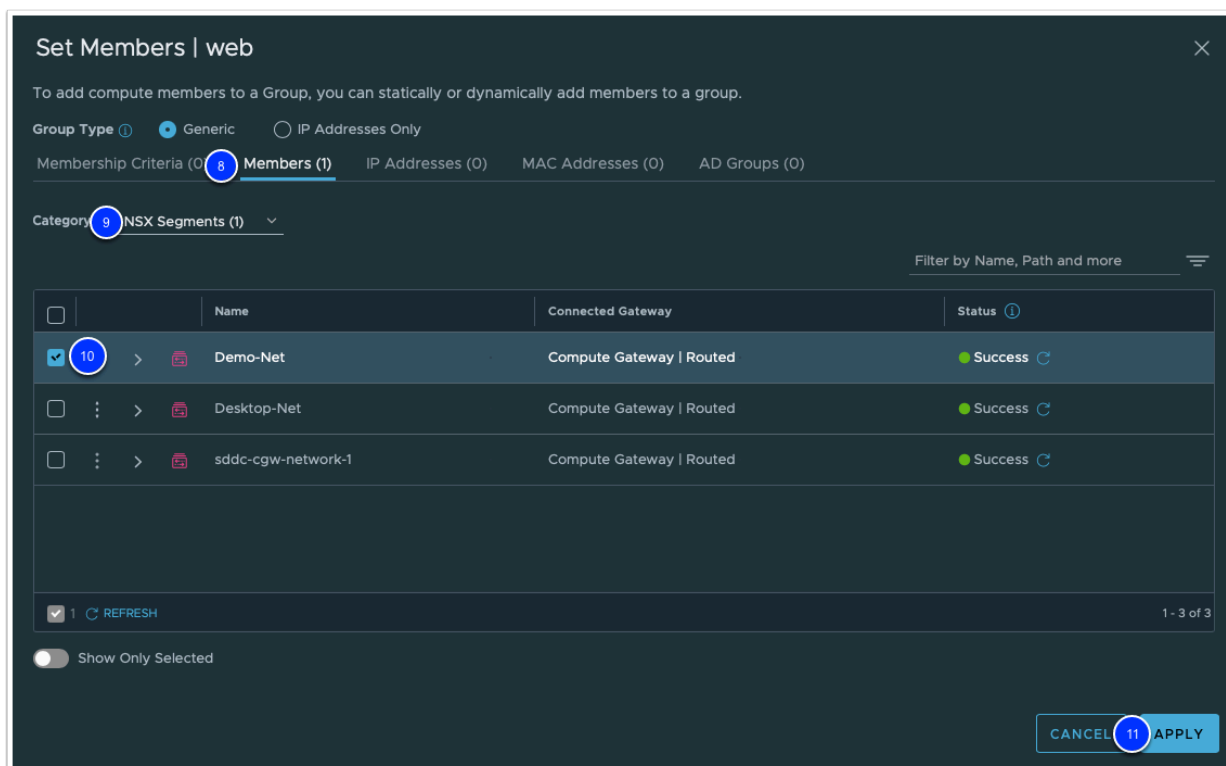
Groups can be used in VMware Cloud on AWS Advanced Network Services to group virtual machines and simplify rule-based configuration. In this exercise, we will group the two web servers into a group and then create a firewall rule to block communication between them. In a properly architected traditional application, there is usually no need for servers in the web tier to communicate.

We will now create a group of web servers based on the dynamic security tag we applied earlier.

1. If your NSX Manager UI tab is active then go to step #3. If you already closed NSX Manager tab then Select your SDDC, if you aren't currently within it, then click **View Details**
2. Click the **OPEN NSX MANAGER** button and click **ACCESS VIA THE INTERNET** to connect to NSX Manager UI. Wait till page with NSX Manager will be loaded and you will see **Home - Overview** dashboard.
3. Choose **Inventory** tab
4. Click on **Groups** on the left hand side of the screen.
5. Click on **Compute Groups**, then **Add Group**
6. Under **Name** enter **web** for the name of the group.
7. Click **Set**

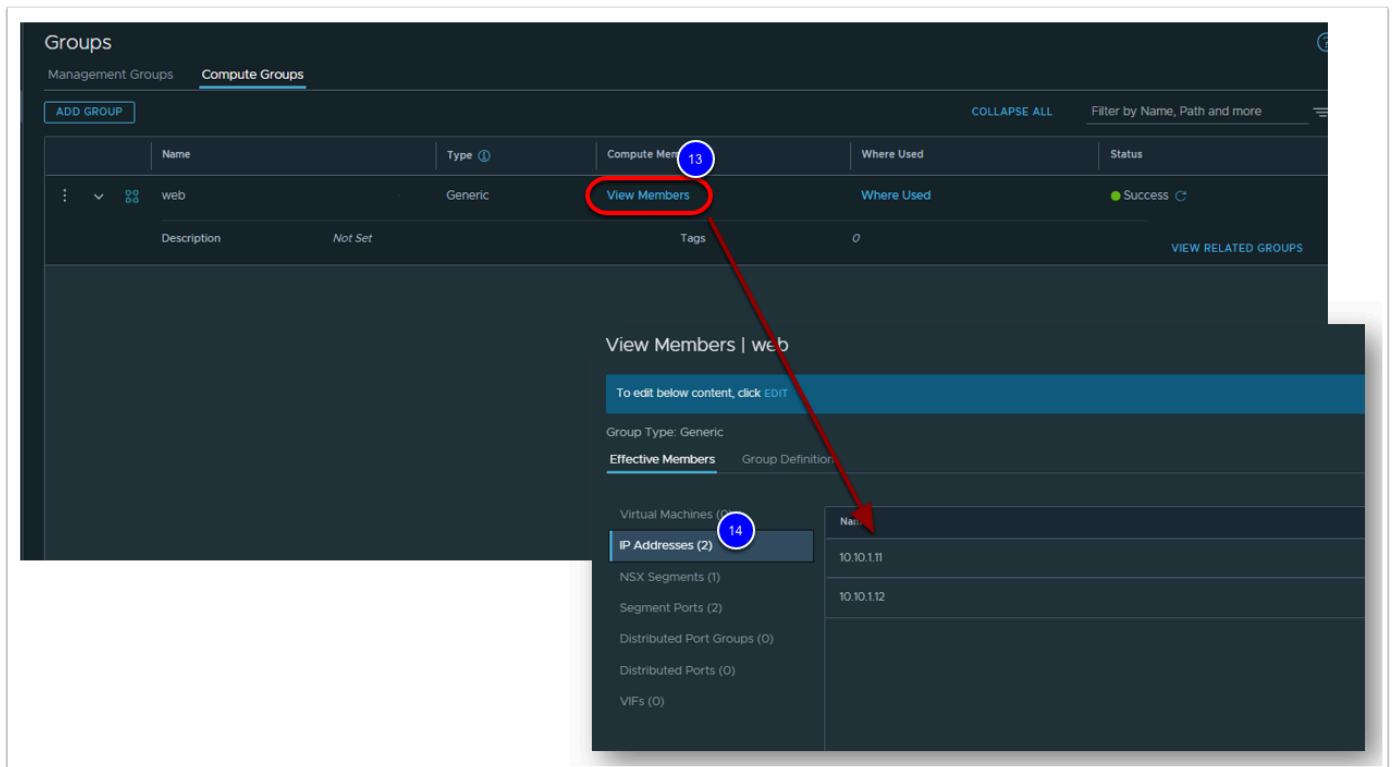


8. Click on **Members** tab.
9. Select **NSX Segments**, in the category dropdown list
10. Select the "**Demo-Net**" Segment. **NOTE:** This is the 1st of the 2 Segments you created in Task 1
11. Click **APPLY**
12. Click **SAVE**



13. Validate that both **webserver01** and **webserver02** appear in the group membership, by clicking **View Members**.

14. Click **IP Addresses**
15. Confirm the existence of your Web Servers in the group and Click **Close** to exit popup once complete



⚠ If both VMs are not present, go back and verify that you selected the correct Segment, also confirm that your Web Server VMs are properly deployed and connected to the Demo-Net segment. Common errors encountered include selection of the wrong segment or VMs, VMs not connected to the selected segment, or naming the segment something other than "Demo-Net as instructed.

Task 10.2 - Create Distributed Firewall Policy


Now that we have created our dynamic group, let's create a firewall rule to block access between the web servers.

1. Select the **Security** tab
2. Click **Distributed Firewall** on the left-hand side of the screen.
3. On the Arrow Shaped menu, click the **Application** bar.
4. Click **+ADD POLICY** to create a new section for the rule. This functionality allows you to group rules logically to make operating the environment simpler.


5. Click the **"New Policy"** text in the name column, Type **Web Tier**.
6. Click the **Checkbox** next to the **Web Tier** section.
7. Click **+ADD RULE** in the menu above the rules.
8. Under **Name**, Type **Block Web To Web**.
9. Under **Sources** hover over **any** and select the **blue edit** button.
10. In the popup click the **checkbox** next to **Web**.
11. Click **Apply**
12. Under Destinations, hover over **any** and select the **blue edit** button.
13. In the popup window click the **checkbox** next to **Web**.
14. Click **Apply**
15. Under **Action**, click the **drop-down** and select **Reject**.
16. Click the **Gear** at the far right of the rule
17. Move the **Slider** to the right to enable logging
18. Click **APPLY**
19. Click **Publish** to commit the rule and begin blocking traffic between the web servers.

💡 By setting the action for our east-west (internal) traffic to REJECT, we ensure that our users and applications will immediately know if an address or port is prohibited instead of waiting for a timeout. This will speed up the response to pings, and improve application response times if they are trying to perform an action that is prohibited.

The screenshot displays the VMware NSX Distributed Firewall configuration interface. The main panel shows the 'Category Specific Rules' section with a table of rules. The rule 'Block Web To Web' is highlighted, showing its configuration: Name: Block Web To Web, Sources: web, Destinations: web, Action: Reject, and a green status indicator. The 'Settings' panel on the right shows the 'Logging' section with the 'Enable' checkbox checked. The 'Set Source' and 'Set Destination' panels at the bottom show the selection of 'web' for both source and destination groups. Red arrows indicate the sequence of steps: 1. Clicking 'ADD POLICY', 2. Selecting 'Web Tier', 3. Clicking 'ADD RULE', 4. Selecting 'Block Web To Web', 5. Clicking the 'Sources' column, 6. Selecting 'web' in the 'Set Source' panel, 7. Clicking the 'Destinations' column, 8. Selecting 'web' in the 'Set Destination' panel, 9. Clicking the 'Action' column, 10. Selecting 'Reject' in the 'Settings' panel, 11. Clicking the 'Enable' checkbox, 12. Clicking 'APPLY', and 13. Clicking 'PUBLISH'.

 It might take a couple of seconds for the rule to be published. You can click the refresh button next to the rule to ensure the rule status turns from yellow to green.

Task 10.3 - Confirm Success of the DFW Policy

 You should still have a console session to **webserver01** active. If not, launch the web console again and run the ping command.

1. Click the Chrome Tab for **webserver01**.
2. Ping the IP address for webserver02 you noted previously. You can also press the up arrow then enter to run the last command if you still had the console active.

```
ping -c3 10.10.xx.xx
```

 Click to copy

```
root@webserver01:~# ping -c3 10.10.1.12
PING 10.10.1.12 (10.10.1.12) 56(84) bytes of data.
From 10.10.1.12 icmp_seq=1 Destination Host Prohibited
From 10.10.1.12 icmp_seq=2 Destination Host Prohibited
From 10.10.1.12 icmp_seq=3 Destination Host Prohibited

--- 10.10.1.12 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2047ms
root@webserver01:~#
```

The pings should have stopped responding meaning that the distributed firewall rules have been correctly applied. This simple demonstration should give you an idea of the power of the distributed firewall.

Now, let's ping the gateway address of the Desktop-net segment (10.10.1xx.1, where **xx** is your student number). You can reference your Desktop-net segment subnet gateway address from Task 1, Step 12.

3. Ping the gateway of Desktop-Net segment. Your ping test should succeed.

```
ping -c3 10.10.1xx.1
```

📄 Click to copy

! WARNING: If this pinging the Desktop-net gateway fails you need to double-check your Distributed firewall rule. Consult the rule definition, review your distributed firewall rule and make the necessary changes. If the firewall rule is not corrected it will negatively impact the results of Lab 3.

See your instructor for assistance if needed.

```
root@webserver01:~# ping -c3 10.10.101.1
PING 10.10.101.1 (10.10.101.1) 56(84) bytes of data.
64 bytes from 10.10.101.1: icmp_seq=1 ttl=64 time=0.214 ms
64 bytes from 10.10.101.1: icmp_seq=2 ttl=64 time=0.164 ms
64 bytes from 10.10.101.1: icmp_seq=3 ttl=64 time=0.158 ms

--- 10.10.101.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.158/0.178/0.214/0.025 ms
```

Task 11 - Visibility & Operations

The Activity Log contains a history of significant actions in your organization, such as SDDC deployments and removals, as well as notifications sent by VMware for events such as SDDC upgrades and maintenance.

All operations (UI or API) that occurs within VMware Cloud AWS (VMC), including but not limited to SDDC creation, deletion, updates, network configurations, user authorization/access, etc. is all captured as part of the Activity Log in the VMC Console. Within the Activity Log, you can view the type of operation, the time the operation occurred, the applicable SDDC as well the user of the operation and all of these fields can be filtered out further.

In this task we will take a look at the activity log, we will also look at Log Insight Cloud for more details and logs

1. In the left pane of your VMC on AWS SDDC Console, Click **Activity Log**
You would see a number of SDDC activities recorded, such as:

- SDDC Created
- HCX deployed
- etc..

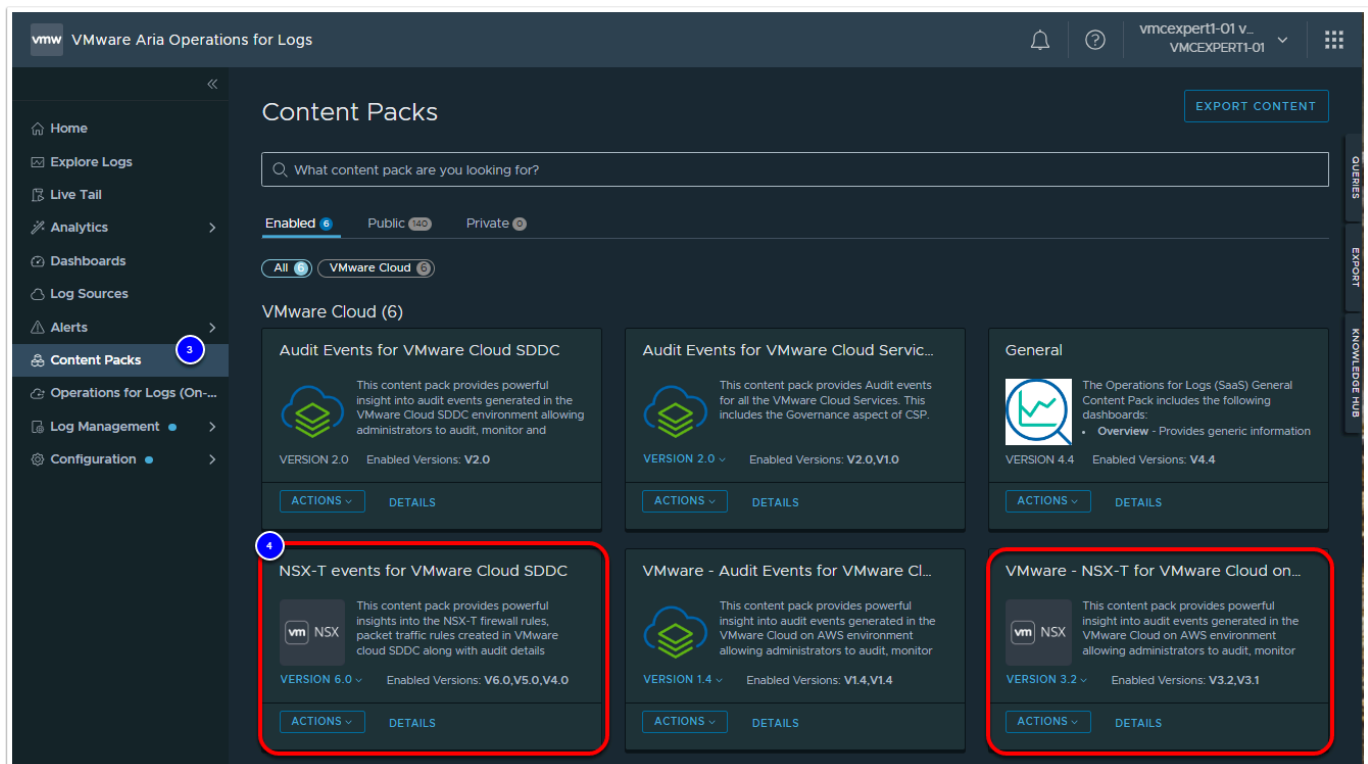
2. Click the **VMware Aria Operations for Logs** link at the top of the page

Event Name	Time	Deployment Type	Resource Type	Resource Name	Task Owner
Updating Management VM	6/5/23, 10:01 AM	AWS	SDDC		
Updating Management VM	6/5/23, 10:00 AM	AWS	SDDC		
Updating Management VM	6/5/23, 10:00 AM	AWS	SDDC		
SDDC Provisioning	6/4/23, 5:07 PM	AWS	SDDC		
SDDC Provisioning	6/4/23, 5:05 PM	AWS	SDDC		
SDDC Group Deletion	5/26/23, 11:04 AM	AWS	SDDC		
SDDC Removal of External AWS Account	5/26/23, 11:03 AM	AWS	SDDC		

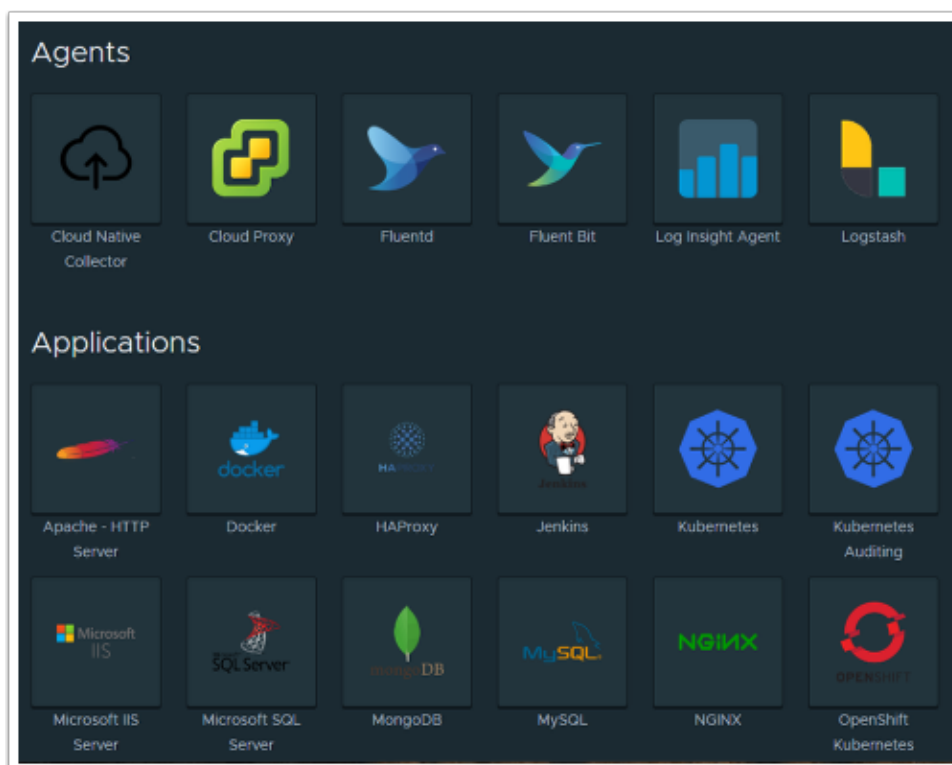
We'll now take a look at Aria Operations for Logs where we will be able to see log entries providing more details and from multiple sources.

3. In the left pane Click **Content Packs**
4. Confirm the following content packs are enabled and if not enable them
 - **NSX-T events for VMware Cloud SDDC**
 - **NSX-T for VMware Cloud on AWS**
5. Look through the list of other Content Packs you can enable for vRealize Log Insight Cloud

 Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs



6. In the left Pane, Click **Log Sources**, to see all of the sources log insight cloud supports



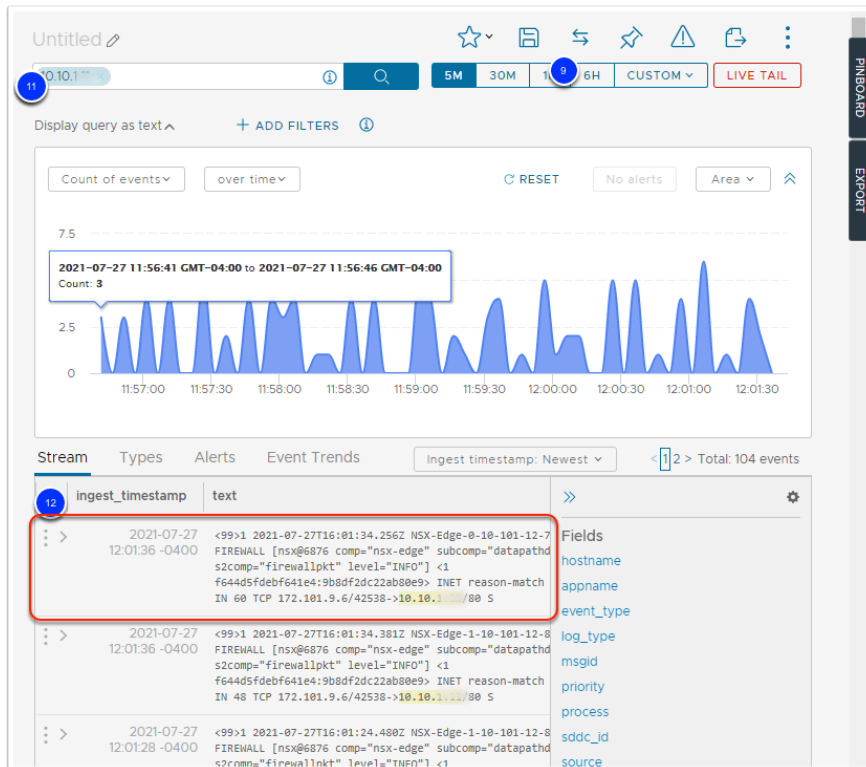
7. In the Left Pane, Click **Dashboards**

8. Scroll down and click **Distributed Firewall - Traffic**

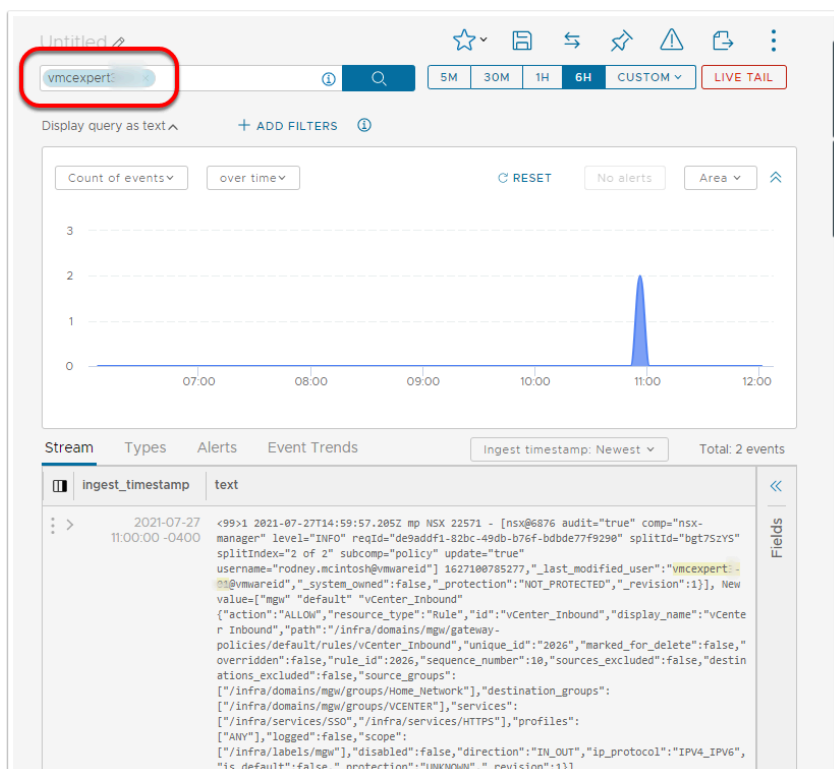
9. Adjust the time scope to **6H**

10. Click **Explore Log**, in the left pane

11. In the search bar type in the <IP address of your webserver01> (10.10.x.x)
12. Notice the firewall log entries from your earlier pings



12. Also search for your SDDC user account (**vmcexpert#-xx**) to see audit events for the user account



Conclusion

In this module, we explored the setup of configuration of a VMware Cloud on AWS SDDC including utilizing the content library, deploying virtual machines, modifying firewall rules and working with virtual machines