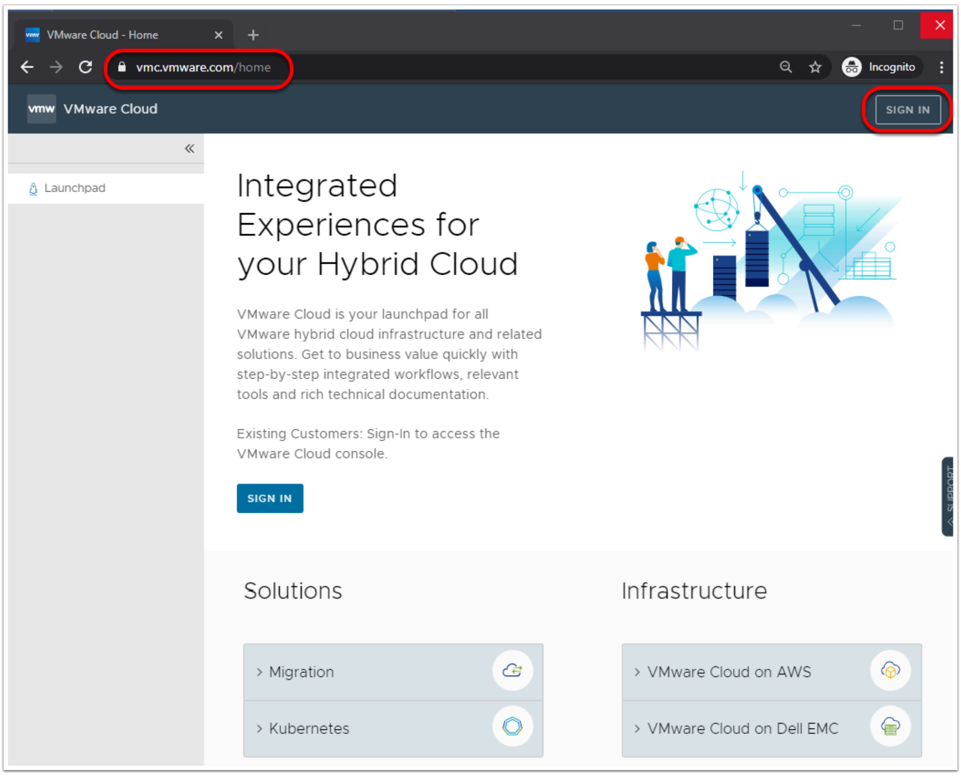
Lab 02 - Working with your SDDC

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.



Integrated Experiences for your Hybrid Cloud

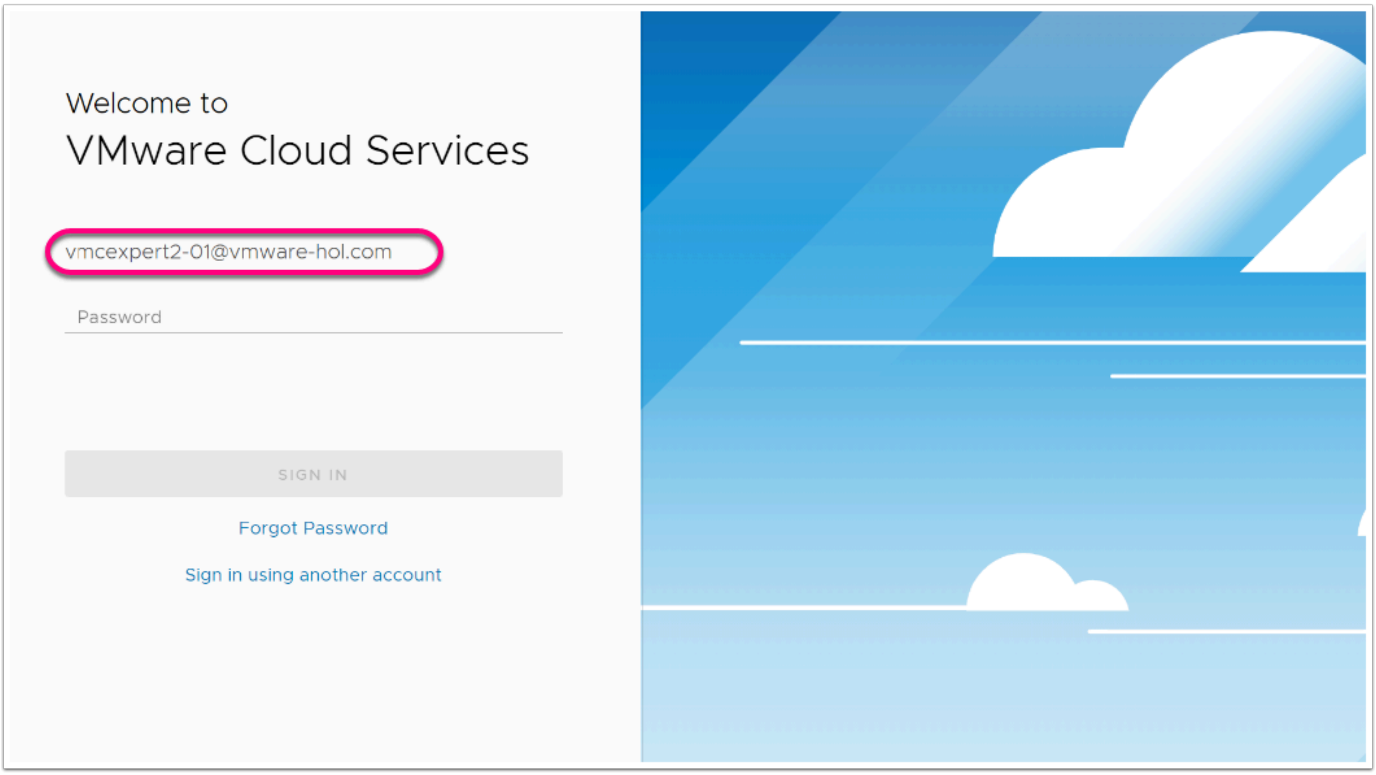
VMware Cloud is your launchpad for all VMware hybrid cloud infrastructure and related solutions. Get to business value quickly with step-by-step integrated workflows, relevant tools and rich technical documentation.

Existing Customers: Sign-In to access the VMware Cloud console.

SIGN IN

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

1. From your Desktop/laptop launch your preferred browser
   NOTE: In tests, *Google Chrome* in *Incognito mode* worked best
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!**



Welcome to
VMware Cloud Services

vmcexpert2-01@vmware-hol.com

Password

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 first two Virtual Machines in your SDDC
NOTE: VMC Network Segments are backed by NSX-T Geneve Overlay Segments.

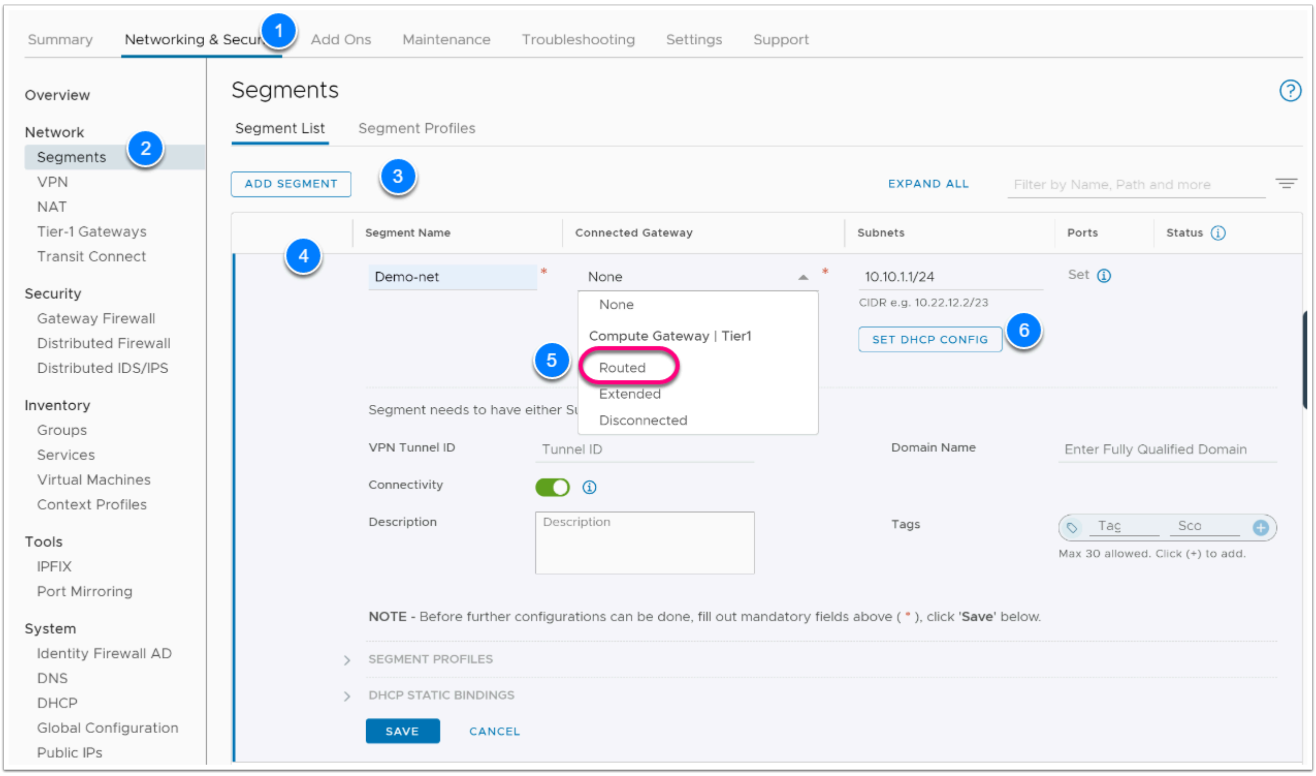
NSX-T Overlay-backed Segment

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. NSX-T Data Center 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.

VMware Cloud on AWS allows you to quickly and easily create new logical network segments on demand. Let’s create a new network segment in the SDDC.

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

1. Click the **Networking & Security** tab
2. click **Segments** to display the existing network segments.
3. Click on **ADD SEGMENT** to create a new network segment.
4. 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 the 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*
5. Click the **SET DHCP CONFIG** button to enable and configure DHCP in the pop up



Segment Name	Connected Gateway	Subnets	Ports	Status
Demo-net *	None *	10.10.1.1/24 CIDR e.g. 10.22.12.2/23	Set	

Segment needs to have either Su

VPN Tunnel ID: Tunnel ID

Domain Name: Enter Fully Qualified Domain

Connectivity

Description: Description

Tags: Tag Sco

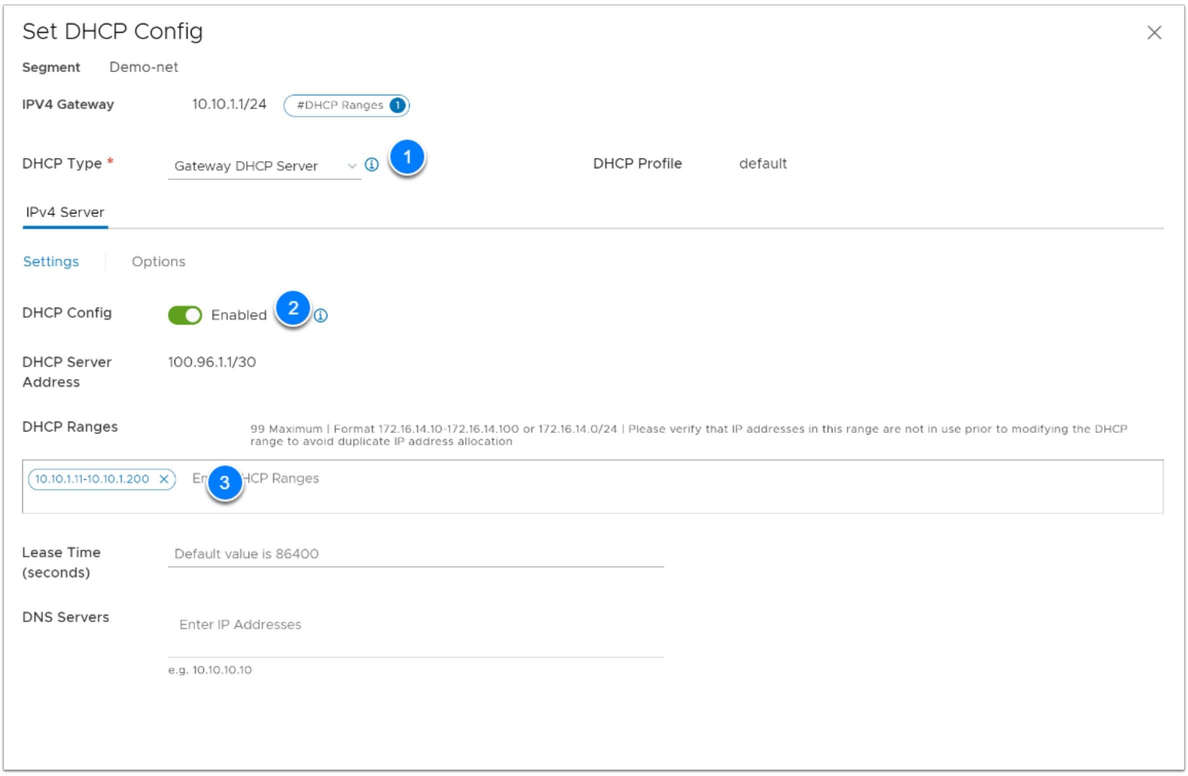
Max 30 allowed. Click (+) to add.

NOTE - Before further configurations can be done, fill out mandatory fields above (*), click 'Save' below.

6. On the pop up slide the **"DHCP CONFIG"** slider to **Enable** DHCP
7. Enter **10.10.XX.11-10.10.XX.200** for the **DHCP IP Range**. (Where **XX** is your student number, for students(1-9) do not include the a leading 0) i.e. 10.10.1.11-10.10.1.200
   This is the range of IP addresses the DHCP server will grant to workloads attached to the network.
   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.

If you have a student number in the single digits, you must omit the leading zero. (ie 10.10.8.11)

8. Leave the other fields as their default values. As before ensure the bubble turns blue and not red.
   - DHCP Type: **Gateway DHCP Server**
   - DHCP Profile: **Default**
   - Lease Time: **Leave Blank**
   - DNS Servers: **Leave Blank**



Set DHCP Config

Segment Demo-net

IPV4 Gateway 10.10.1.1/24 #DHCP Ranges 1

DHCP Type * Gateway DHCP Server

DHCP Profile default

IPv4 Server

Settings | Options

DHCP Config Enabled

DHCP Server Address 100.96.1.1/30

DHCP Ranges

99 Maximum | Format 172.16.14.10-172.16.14.100 or 172.16.14.0/24 | Please verify that IP addresses in this range are not in use prior to modifying the DHCP range to avoid duplicate IP address allocation

10.10.1.11-10.10.1.200 ✕ En HCP Ranges

Lease Time (seconds) Default value is 86400

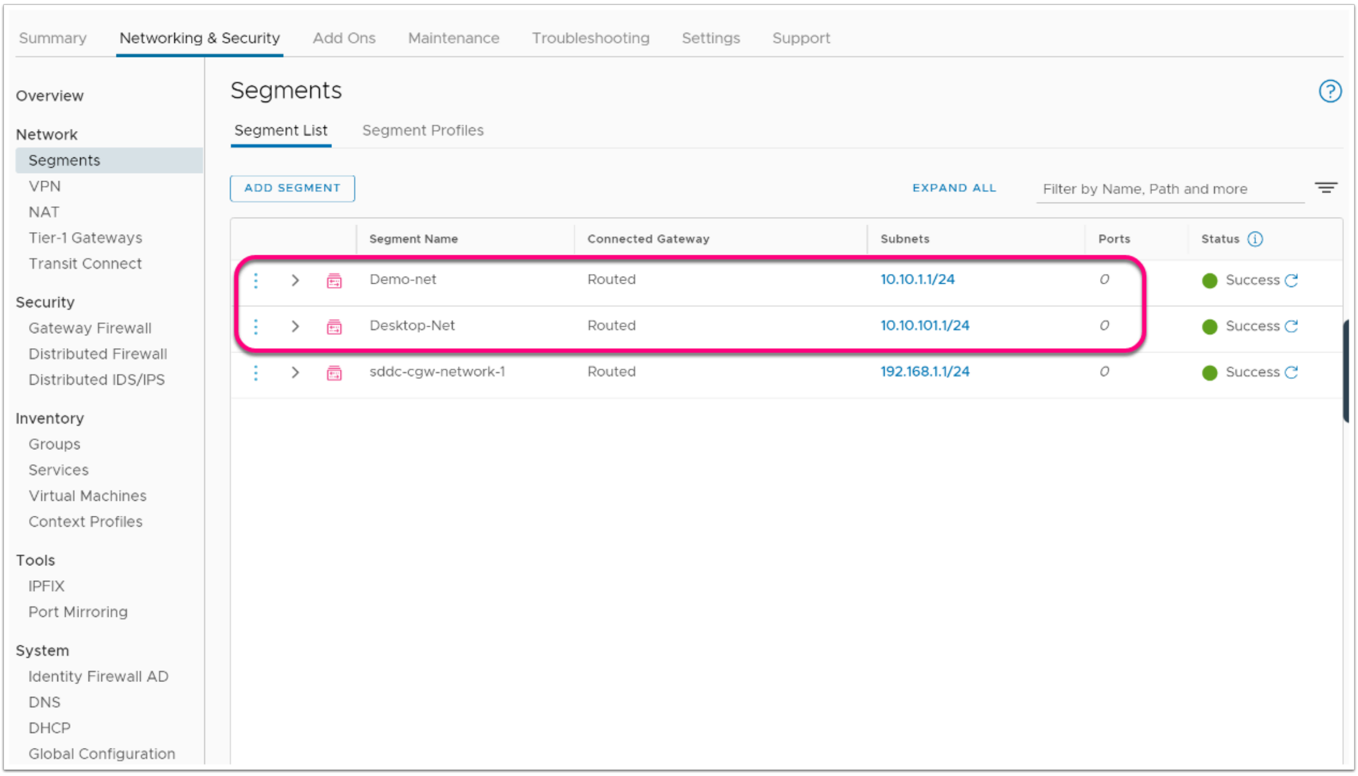
DNS Servers Enter IP Addresses

e.g. 10.10.10.10

9. Click **Apply**
10. 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**
11. When prompted to continue configuring the segment, Click **NO**
12. Repeat the steps 1 - 8 using the information below to create a 2nd virtual network segment in the SDDC
    - Segment Name: Desktop-Net
    - 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 Config: Enabled
      - 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):
        - 8.8.8.8
        - 192.168.110.10

Verify Network Segment Configuration

1. 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.



Segment Name	Connected Gateway	Subnets	Ports	Status
Demo-net	Routed	10.10.1.1/24	0	● Success
Desktop-Net	Routed	10.10.101.1/24	0	● Success
sddc-cgw-network-1	Routed	192.168.1.1/24	0	● Success

Task 2 - Configure Firewall rule for vCenter Access

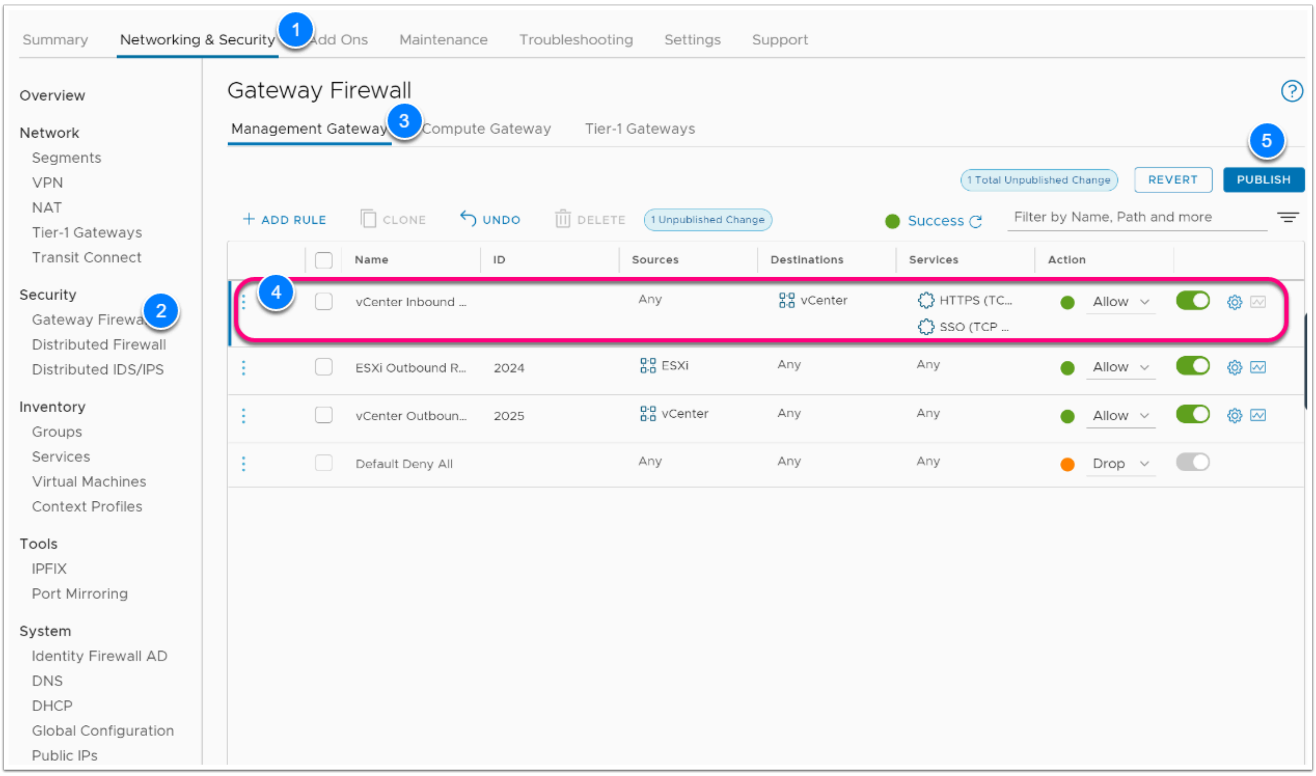
By default, all inbound firewall traffic into the SDDC is denied in VMware Cloud on AWS. In order to access vCenter from your Desktop/Laptop or any other external device, you will need to configure a firewall rule allowing inbound access. The Management Gateway (MGW) controls access to vCenter, the ESXi 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 environment, we will open it to any IP address on the internet which is not recommended.**

As of the 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

1. Navigate to the VMC on AWS console > Student## SDDC > Settings > Network & Security Menu

2. Click on **Gateway Firewall** on the left-hand side of the screen.
3. If it is not already selected, click on **Management Gateway** to create firewall rules that allow access to management components in the SDDC.
4. Click **+ ADD RULE** to add a new rule to the edge gateway. A row titled new rule should appear.
5. Click the “New Rule” text from the “Name” column and change it to ***vCenter Inbound Rule***.
6. Leave the Source set as **Any**.
7. Hover over the new rule's "**Destinations**" column, then click the **blue Edit button** to edit the destination field.
8. On the Pop Up, click the radio button next to **System Defined Groups**.
9. Select the Radio-button next to **vCenter**.
10. Click **Apply** to save the destination information in the rule.
11. Hover over the new rule's "**Services**" column, then click the **blue Edit button ,** select **HTTPS (TCP 443) & SSO (TCP 7444)** to allow access to the vCenter server.
12. Publish the rules by clicking **PUBLISH** button to activate the Firewall rule.



Name	ID	Sources	Destinations	Services	Action
vCenter Inbound ...		Any	vCenter	HTTPS (TC... SSO (TCP ...	Allow
ESXi Outbound R...	2024	ESXi	Any	Any	Allow
vCenter Outboun...	2025	vCenter	Any	Any	Allow
Default Deny All		Any	Any	Any	Drop

vCenter should now be accessible from anywhere on the internet. In the next section, we will access vCenter via the HTML5 client to begin the deployment and configuration of virtual machines.

Task 2.1 - Log into VMware Cloud on AWS vCenter

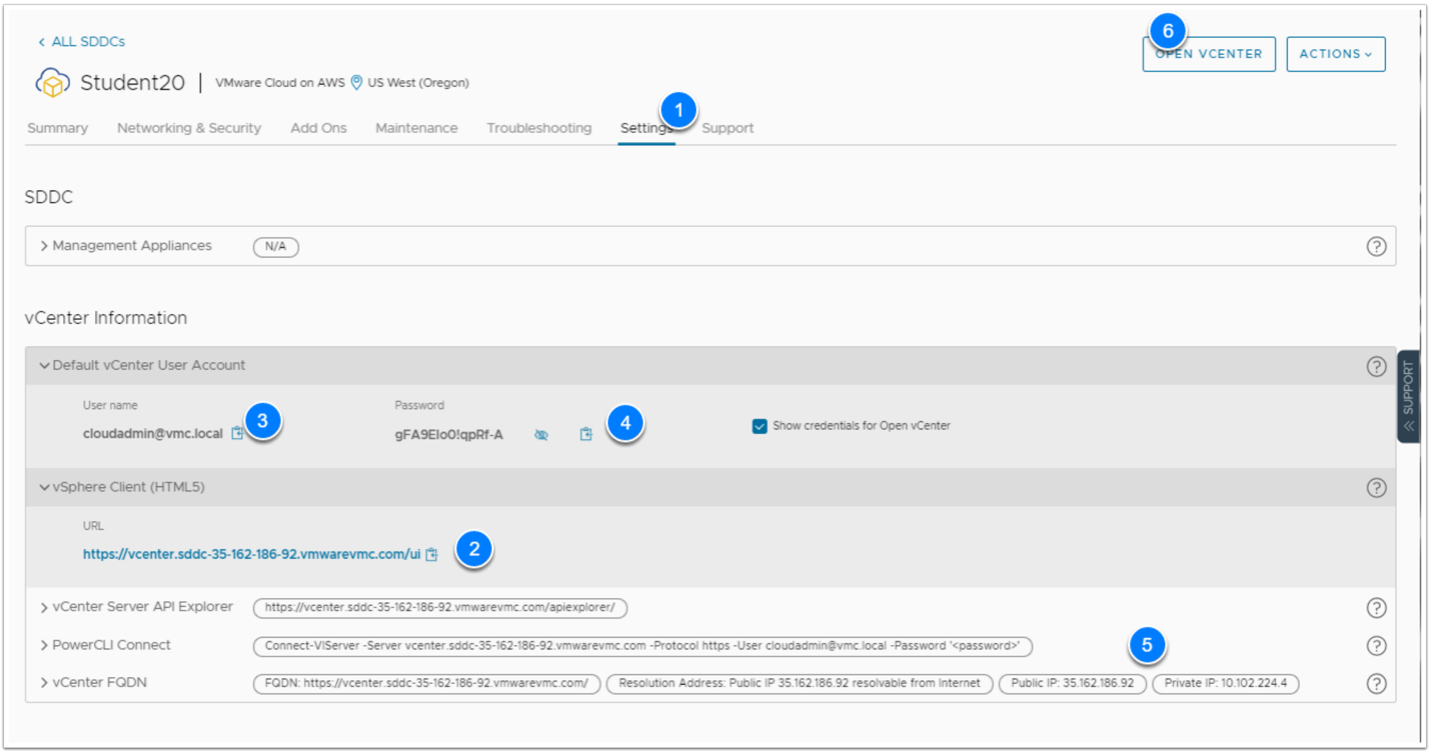
Now that the firewall rule has been modified to allow external access to vCenter, we would be able to log in, but before doing so, we need to first gather the following pieces of information from our VMC Console:

- vCenter (FQDN and/or IP)

- Default Cloud Admin Account
- Default Cloud Admin Password

To access this information

1. Click the **Settings** tab
2. Expand the **Default vCenter User Account** and **vSphere Client (HTML5)** sections
3. Copy the following values to the provided excel workbook, you will use them to log into vCenter and be using them again soon in task 2.2. If you need to find these items in the future this is where you find them.
   - vSphere Client (HTML5) URL
   - User Name
   - Password



‹ ALL SDDCs

Student20 | VMware Cloud on AWS US West (Oregon)

OPEN VCENTER ACTIONS

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

SDDC

› Management Appliances N/A

vCenter Information

⌄ Default vCenter User Account

User name: cloudadmin@vmc.local

Password: gFA9EIo0!qpRf-A

☑ Show credentials for Open vCenter

⌄ vSphere Client (HTML5)

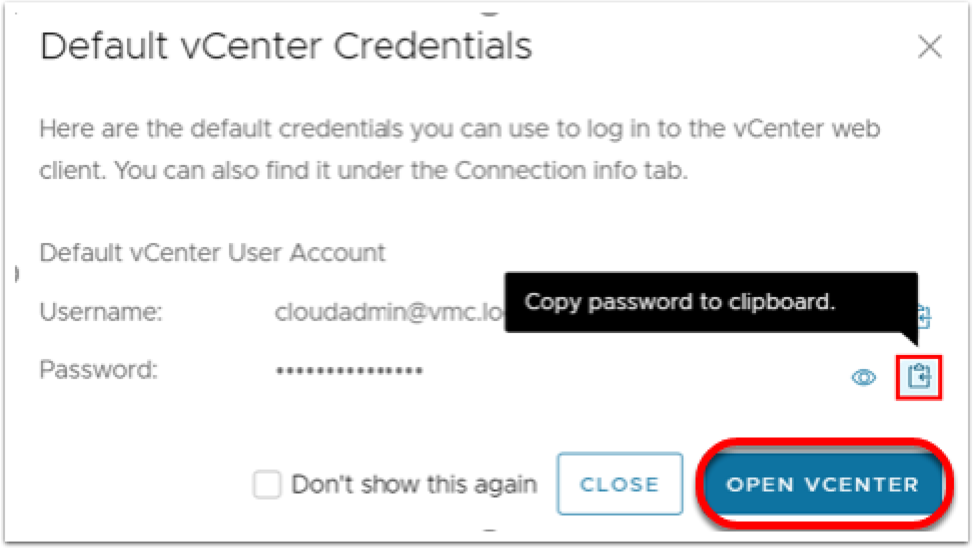
URL: https://vcenter.sddc-35-162-186-92.vmwarevmc.com/ui

› vCenter Server API Explorer https://vcenter.sddc-35-162-186-92.vmwarevmc.com/apiexplorer/

› PowerCLI Connect Connect-VIServer -Server vcenter.sddc-35-162-186-92.vmwarevmc.com -Protocol https -User cloudadmin@vmc.local -Password '<password>'

› vCenter FQDN FQDN: https://vcenter.sddc-35-162-186-92.vmwarevmc.com/ Resolution Address: Public IP 35.162.186.92 resolvable from Internet Public IP: 35.162.186.92 Private IP: 10.102.224.4

4. At the top right of the page, click **OPEN VCENTER**
5. On the Pop Up, click on the **SHOW CREDENTIALS Button**
6. Click the Clipboard **icon** next to Password to copy the administrative user password to your clipboard.



Default vCenter Credentials

Here are the default credentials you can use to log in to the vCenter web client. You can also find it under the Connection info tab.

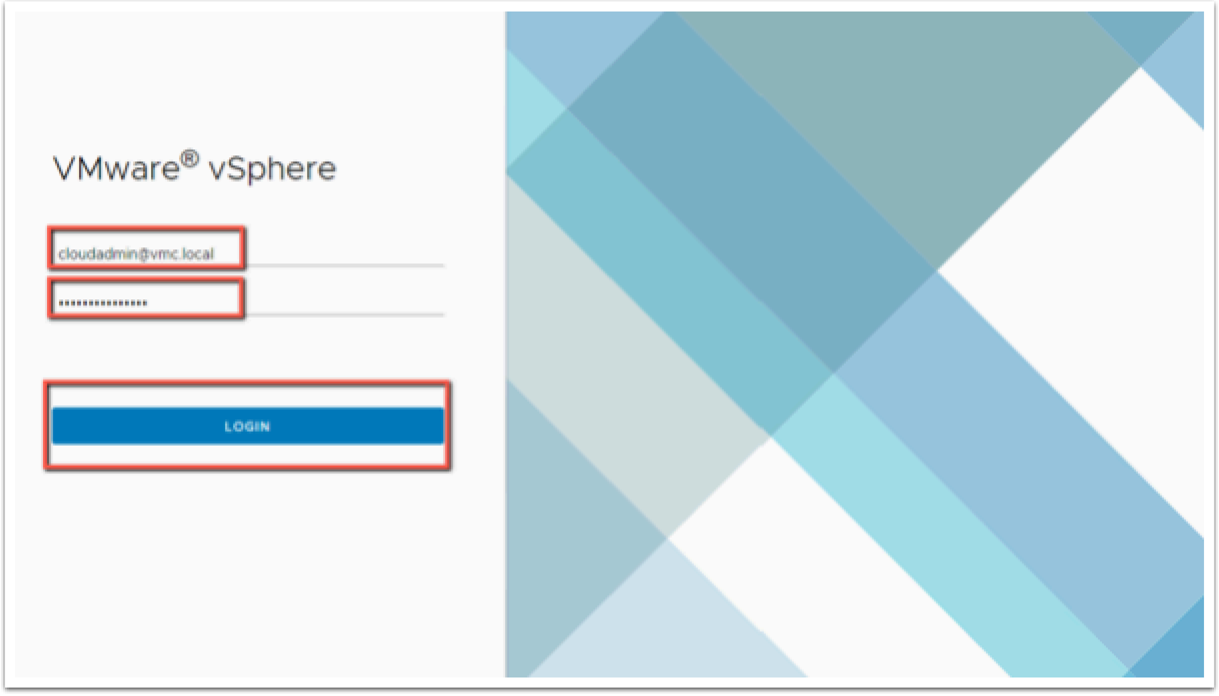
Default vCenter User Account

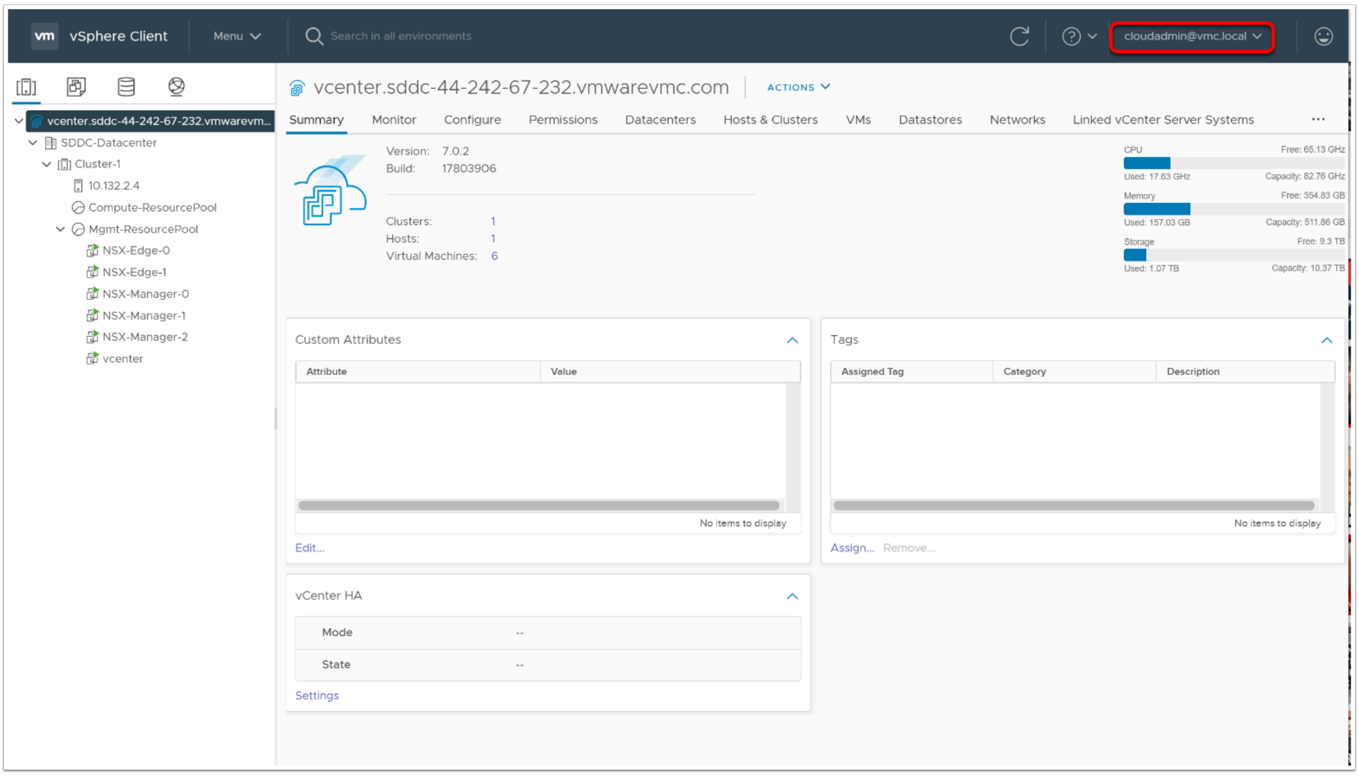
Username: cloudadmin@vmc.lo

Password: ••••••••••••••••

Task 2.2 - Log into the vSphere Client (HTML5)

1. Click the **OPEN VCENTER** button to open a connection to the vCenter HTML5 client.
2. In the example@domain.local field enter **cloudadmin@vmc.local**
3. Right-click in the **Password** field and paste the password copied in the previous step.
4. Click **LOGIN**.
5. On the Summary page Click **Reset to green** for any visible warnings and/or errors





Version: 7.0.2
Build: 17803906

Clusters: 1
Hosts: 1
Virtual Machines: 6

CPU Free: 65.13 GHz
Used: 17.63 GHz Capacity: 82.76 GHz
Memory Free: 354.83 GB
Used: 157.03 GB Capacity: 511.86 GB
Storage Free: 9.3 TB
Used: 1.07 TB Capacity: 10.37 TB

Attribute	Value

No items to display

Assigned Tag	Category	Description

No items to display

Mode	--
State	--

You are now logged in to your VMware Cloud on AWS SDDC vCenter Server as cloudadmin@vmc.local user.

Task 2.3 - 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.

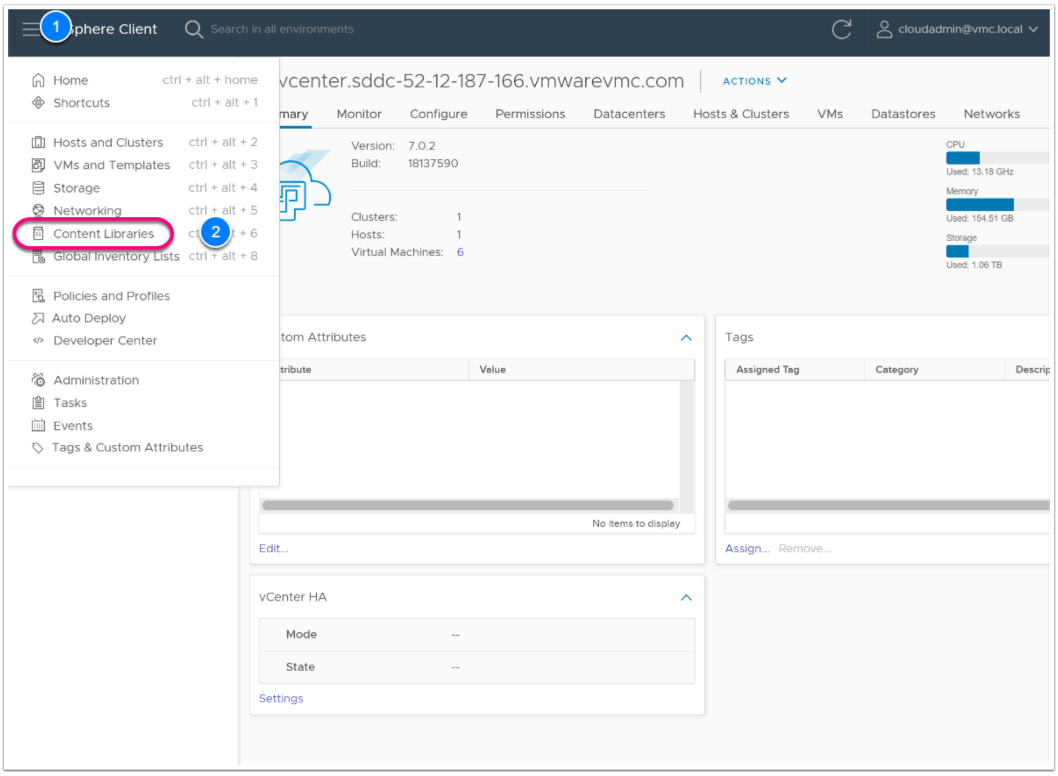
Synchronization of a subscribed library that is set with the option to download all the contents of the published library immediately, synchronizes both the item metadata and the item contents. During synchronization, the library items that are new for the subscribed library are fully downloaded to the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

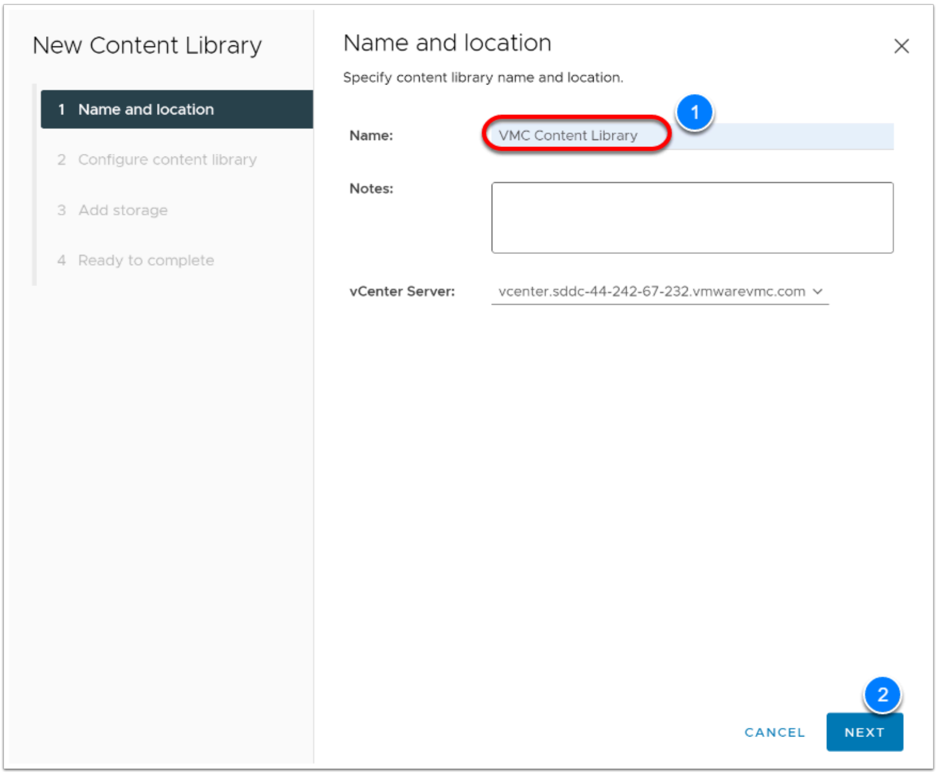
If you use a subscribed library, you can only utilize the content, but cannot contribute with content. Only the administrator of the published library can manage the templates and files.

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 | Hamburger Menu Icon)**
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.



New Content Library

Name and location

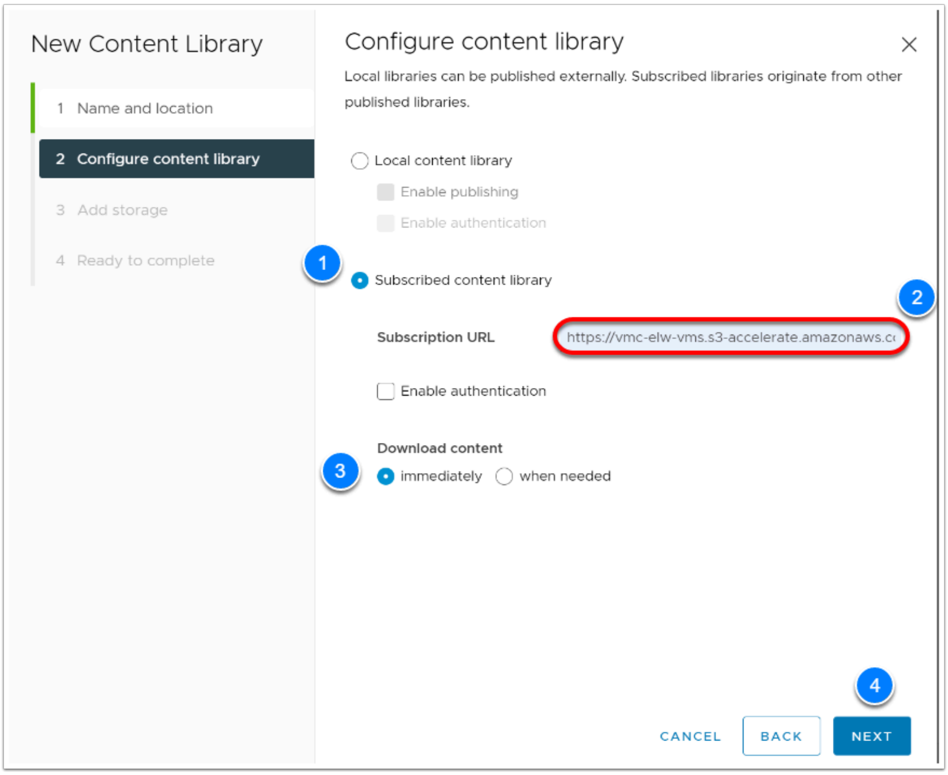
Specify content library name and location.

Name: VMC Content Library

Notes:

vCenter Server: vcenter.sddc-44-242-67-232.vmwarevmc.com

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. Leave the checkbox **unchecked** next to **Enable Authentication**.
9. Make sure **Download content** is set to **immediately**.
10. Click **Next** to continue.
    NOTE: If Prompted to accept the SSL Thumbprint, Click **Yes**.



New Content Library

1 Name and location

2 Configure content library

3 Add storage

4 Ready to complete

Configure content library

Local libraries can be published externally. Subscribed libraries originate from other published libraries.

○ Local content library

□ Enable publishing

□ Enable authentication

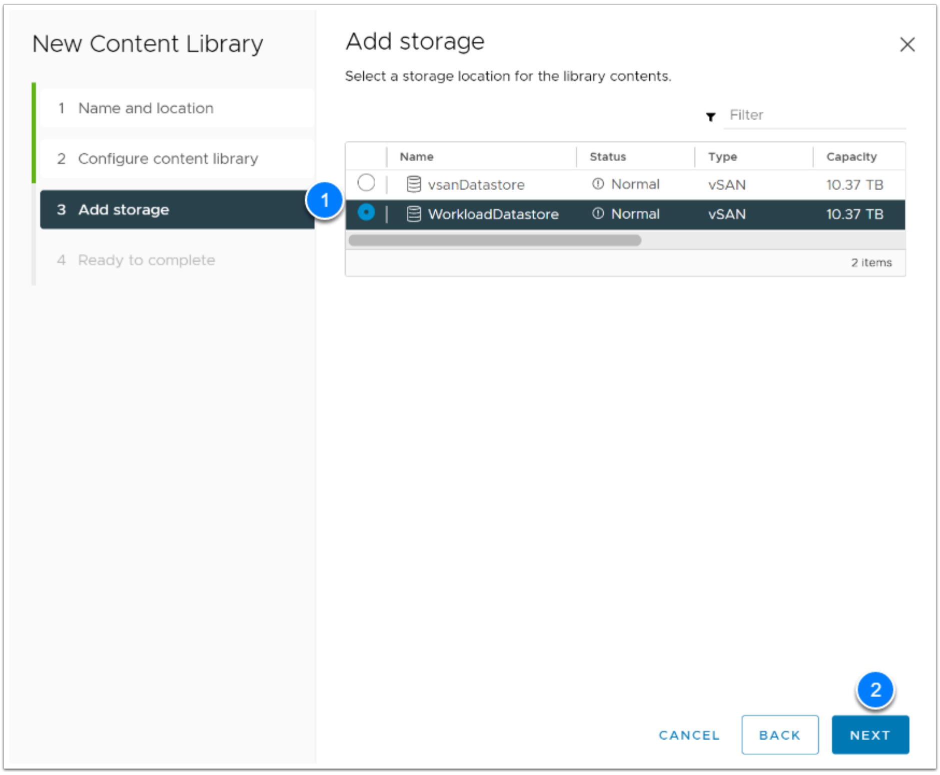
● Subscribed content library

Subscription URL: https://vmc-elw-vms.s3-accelerate.amazonaws.c

□ Enable authentication

Download content: ● immediately ○ when needed

11. On the **Apply Security Policy** Section, Click **NEXT**
12. In the **Add Storage** section click on **WorkloadDatastore** for content library storage.
13. Click the **Next** button.
14. In the **Ready to Complete** section verify that all the data matches the steps above then click **Finish**



New Content Library

1 Name and location

2 Configure content library

3 Add storage

4 Ready to complete

Add storage

Select a storage location for the library contents.

	Name	Status	Type	Capacity
○	vsanDatastore	Normal	vSAN	10.37 TB
●	WorkloadDatastore	Normal	vSAN	10.37 TB

2 items

Note: Depending the size and number of templates it can take a while to synchronize the content. This content library should only take a few minutes to synchronize. We will proceed with task 2.4 to allow time to synchronize. The sync of the "photoapp-u" virtual appliance must complete before moving to task 3. You don't have to wait on MonkeyIsland & VMC-Win10-Template before proceeding to Task 3.

Task 2.4 - Create a Linux & Windows Customization Specification

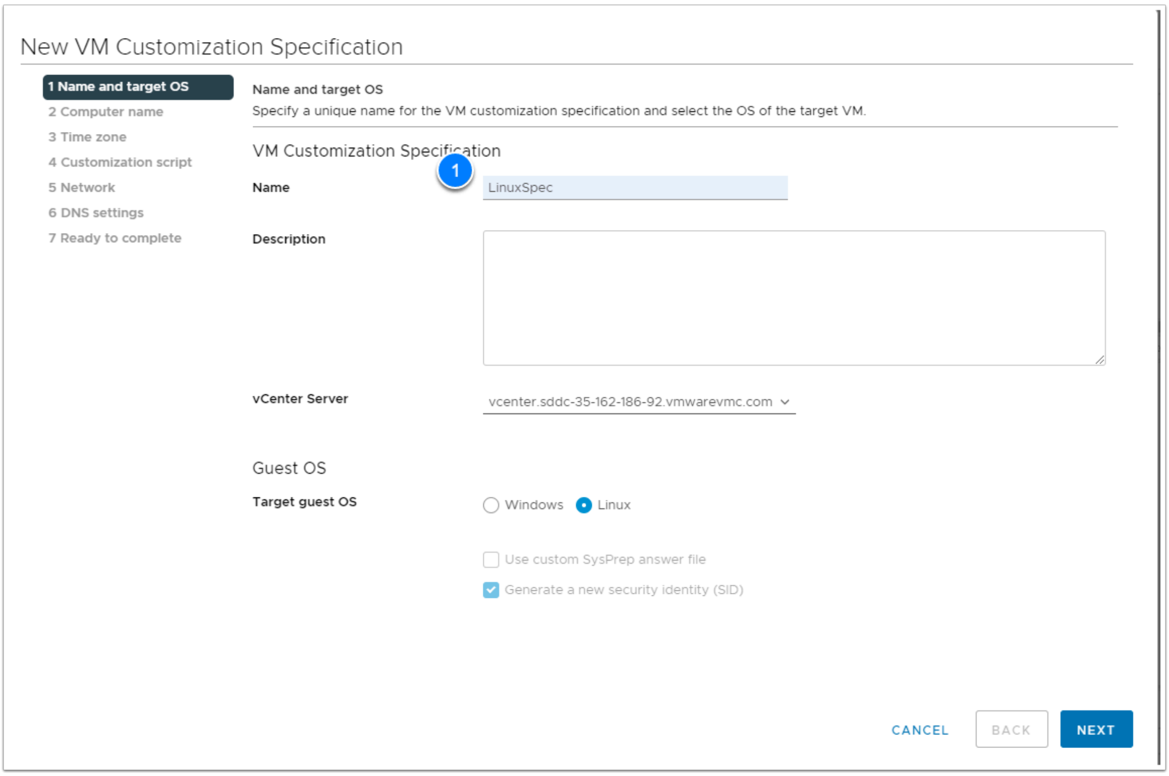
When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings.

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. Enter a **Name** for the Linux Customization Specification (**LinuxSpec** in this example).
6. Optionally enter a **Description**.
7. Select the radio button for **Linux** next to **Target guest OS**.
8. click the **Next** button to continue.



New VM Customization Specification

Name and target OS

Specify a unique name for the VM customization specification and select the OS of the target VM.

VM Customization Specification

Name: LinuxSpec

Description:

vCenter Server: vcenter.sddc-35-162-186-92.vmwarevmc.com

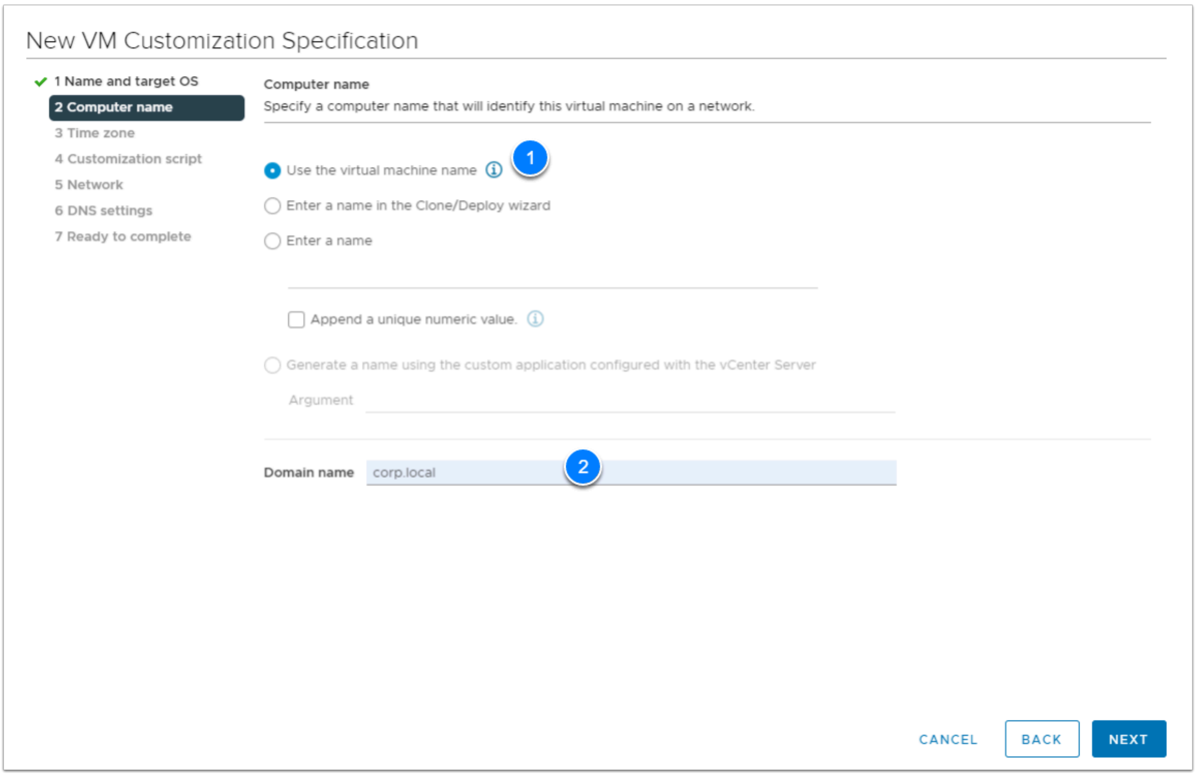
Guest OS

Target guest OS: ○ Windows ● Linux

□ Use custom SysPrep answer file

☑ Generate a new security identity (SID)

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



New VM Customization Specification

Computer name

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

● Use the virtual machine name ⓘ

○ Enter a name in the Clone/Deploy wizard

○ Enter a name

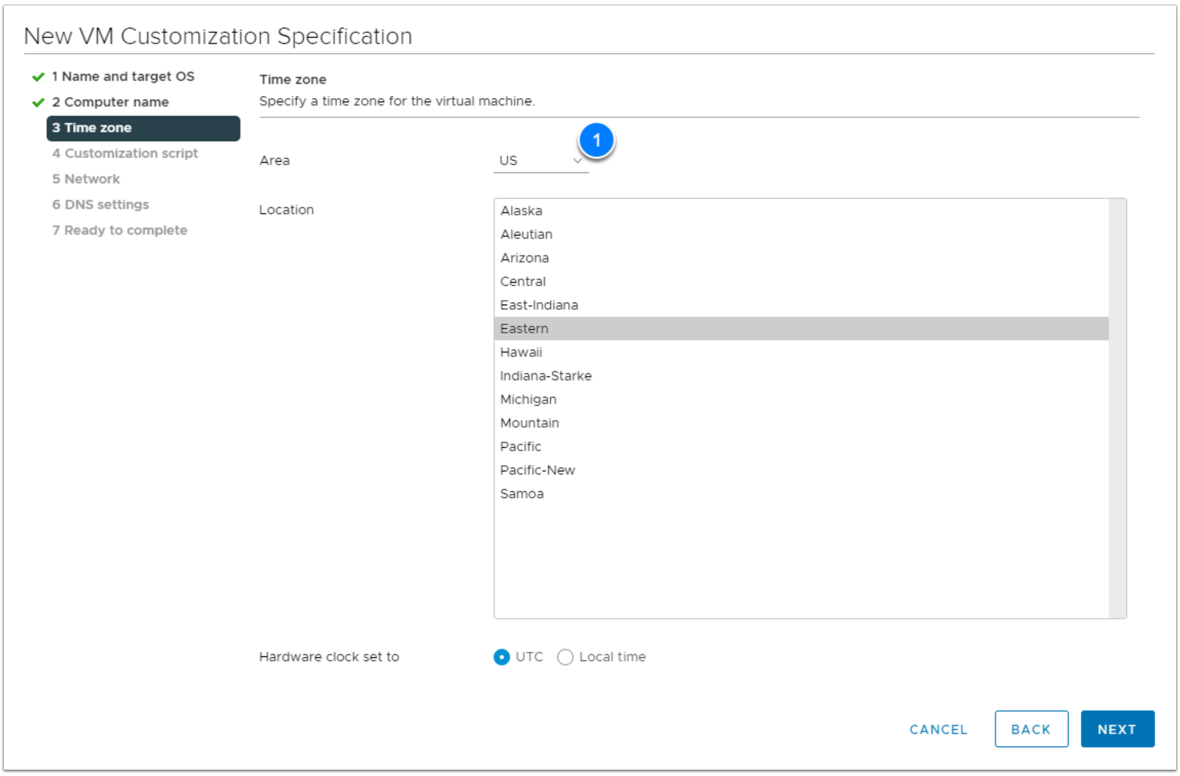
□ Append a unique numeric value. ⓘ

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

Argument

Domain name: corp.local

12. In the **Time Zone** section select the appropriate **Area** by clicking on the arrow next to the drop-down field. We are using the **US** for this lab.
13. Select the appropriate **Location**. You can use **Eastern**
14. Click the **Next** button to continue.
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 in all network interfaces** is selected.
17. Click **Next** to continue.



New VM Customization Specification

✓ 1 Name and target OS
✓ 2 Computer name
3 Time zone
4 Customization script
5 Network
6 DNS settings
7 Ready to complete

Time zone

Specify a time zone for the virtual machine.

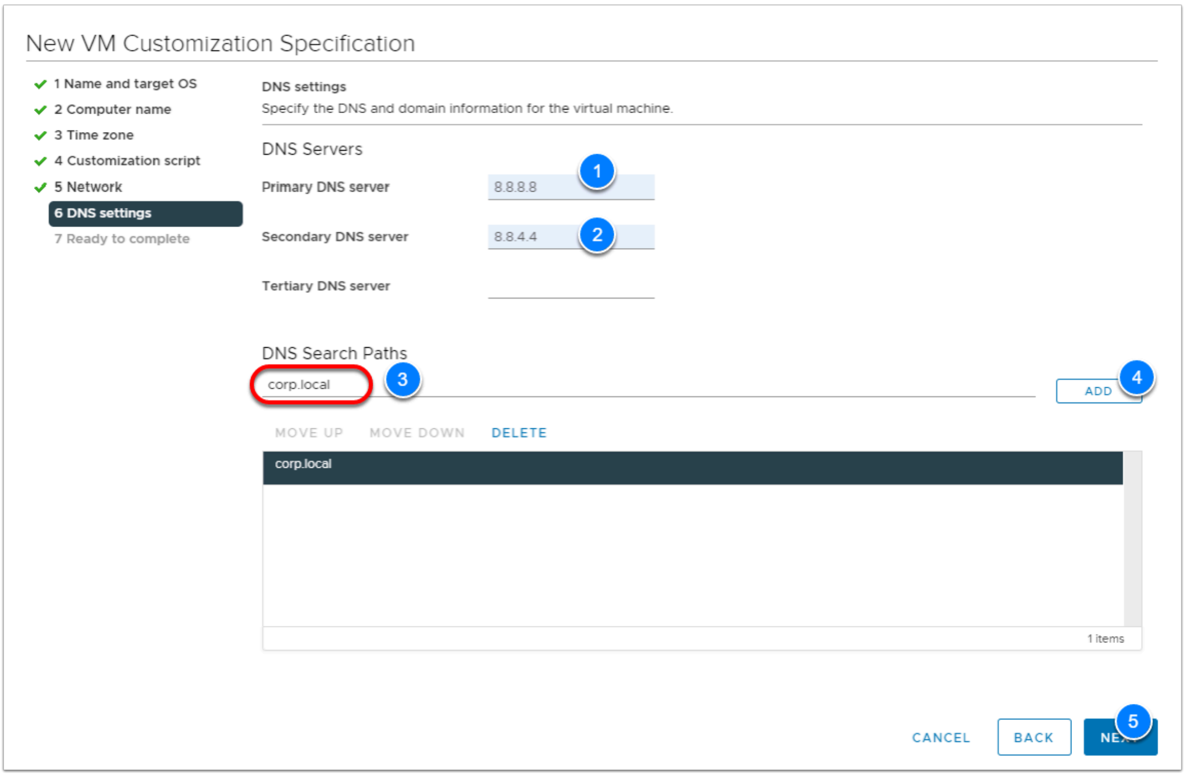
Area: US

Location: Alaska, Aleutian, Arizona, Central, East-Indiana, Eastern (selected), Hawaii, Indiana-Starke, Michigan, Mountain, Pacific, Pacific-New, Samoa

Hardware clock set to: ● UTC ○ Local time

18. On the **DNS settings** sections enter **8.8.8.8** for the Primary DNS server.
    - Enter **8.8.4.4** for the Secondary DNS server.
    - For the DNS Search paths enter corp.local.
    - Click the **Add** button to add the **corp.local** domain to the DNS search path. Verify that it was added.

19. Click **Next** to continue
20. Review your entries and click on the **Finish** button.



New VM Customization Specification

DNS settings

Specify the DNS and domain information for the virtual machine.

DNS Servers

Primary DNS server: 8.8.8.8

Secondary DNS server: 8.8.4.4

Tertiary DNS server:

DNS Search Paths: corp.local

corp.local

1 items

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

- 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**

- Administrator Password Page
  - Password: **VMware1!**

- Time Zone page
  - Time Zone: **(Select your timezone)**

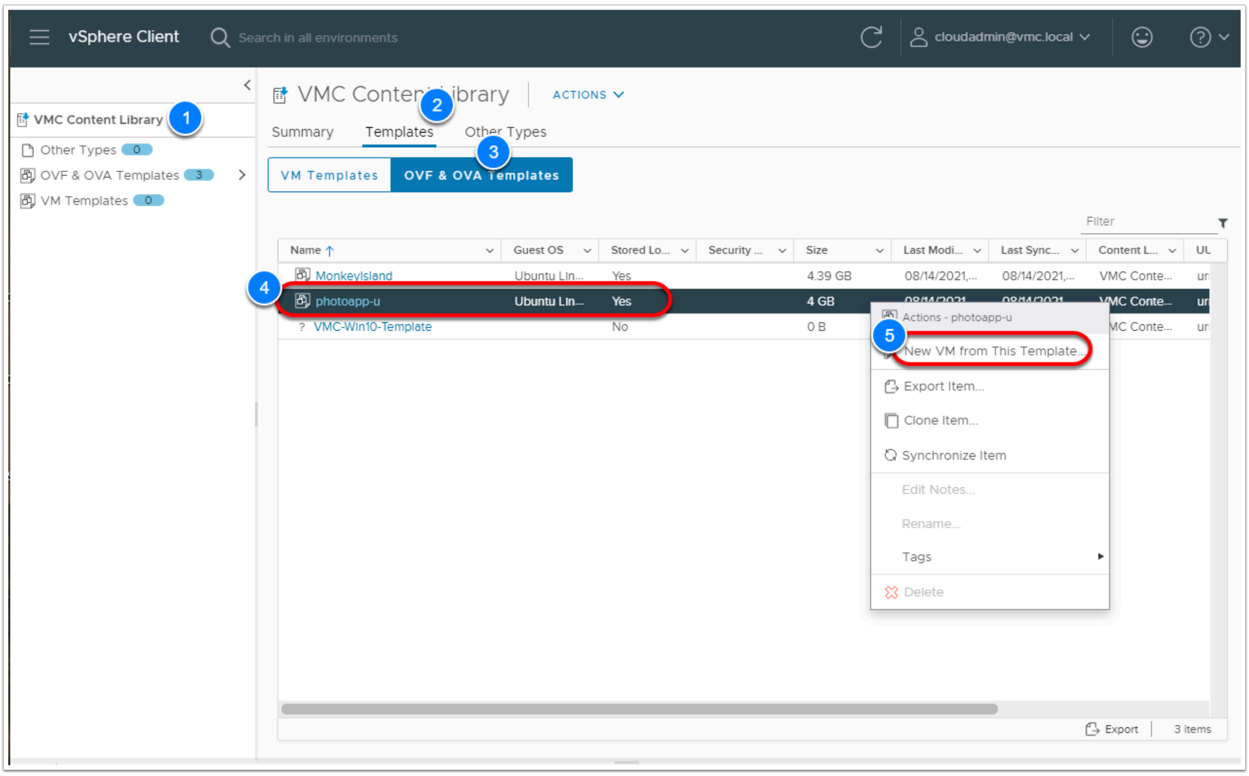
- Click Next and leave defaults through the Commands to Run Once, Network, Workgroup or Domain. Then click Finish on the “ready to complete” section.

Task 3 - Deploy Virtual Machines in VMC on AWS

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.

Task 3.1 - Deploy Virtual Machine from template

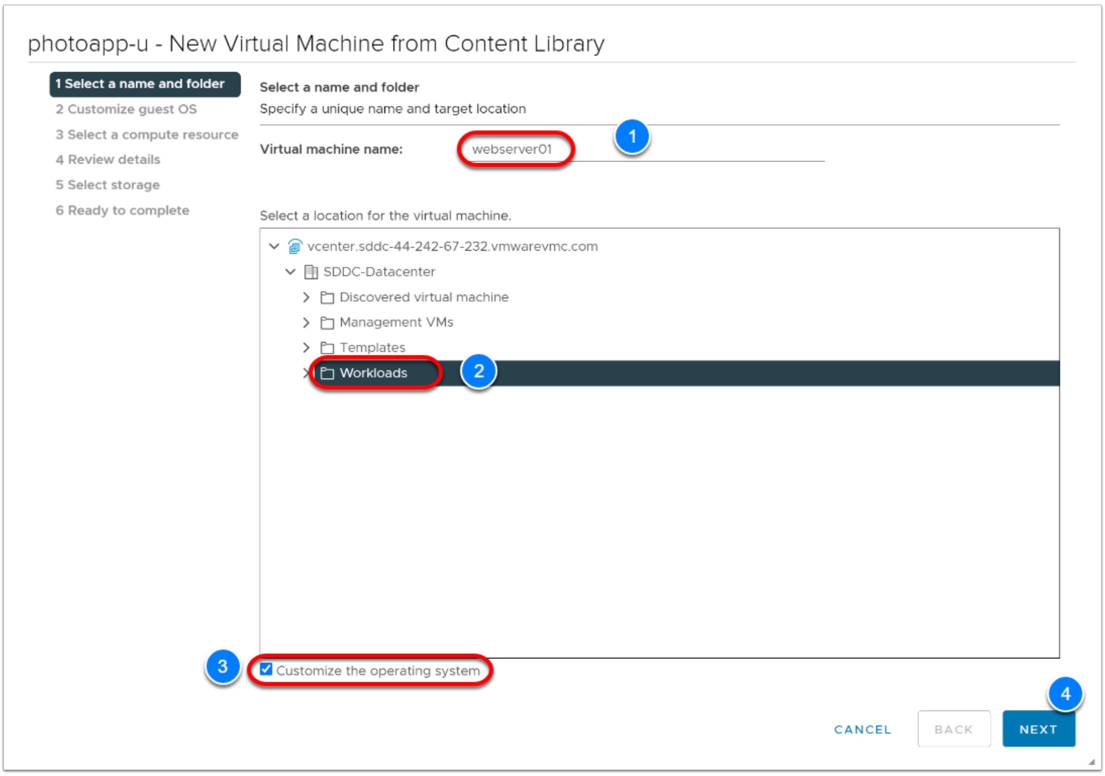
1. Click **Menu**.
2. Click on **Content Libraries**.
3. Click on the **VMC Content Library** that was previously synchronized.
4. Click the **Templates** tab to access the template synchronized in the content library.
5. Click the **OVF & OVA Templates** Tab
6. Right-click on the **photoapp-u** template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



Name	Guest OS	Stored Lo...	Security ...	Size	Last Modi...	Last Sync...	Content L...	UL
MonkeyIsland	Ubuntu Lin...	Yes		4.39 GB	08/14/2021,...	08/14/2021,...	VMC Conte...	ur
photoapp-u	Ubuntu Lin...	Yes		4 GB	08/14/2021	08/14/2021	VMC Conte...	ur
VMC-Win10-Template		No		0 B			MC Conte...	ur

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

11. Click the **Workloads** folder.
12. Select the checkbox next to **Customize the operating system**.
13. Click **Next** to continue
14. On the Customize guest OS page, select **LinuxSpec** customization specification.
15. Click **Next** to continue.



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 Ready to complete

Select a name and folder
Specify a unique name and target location

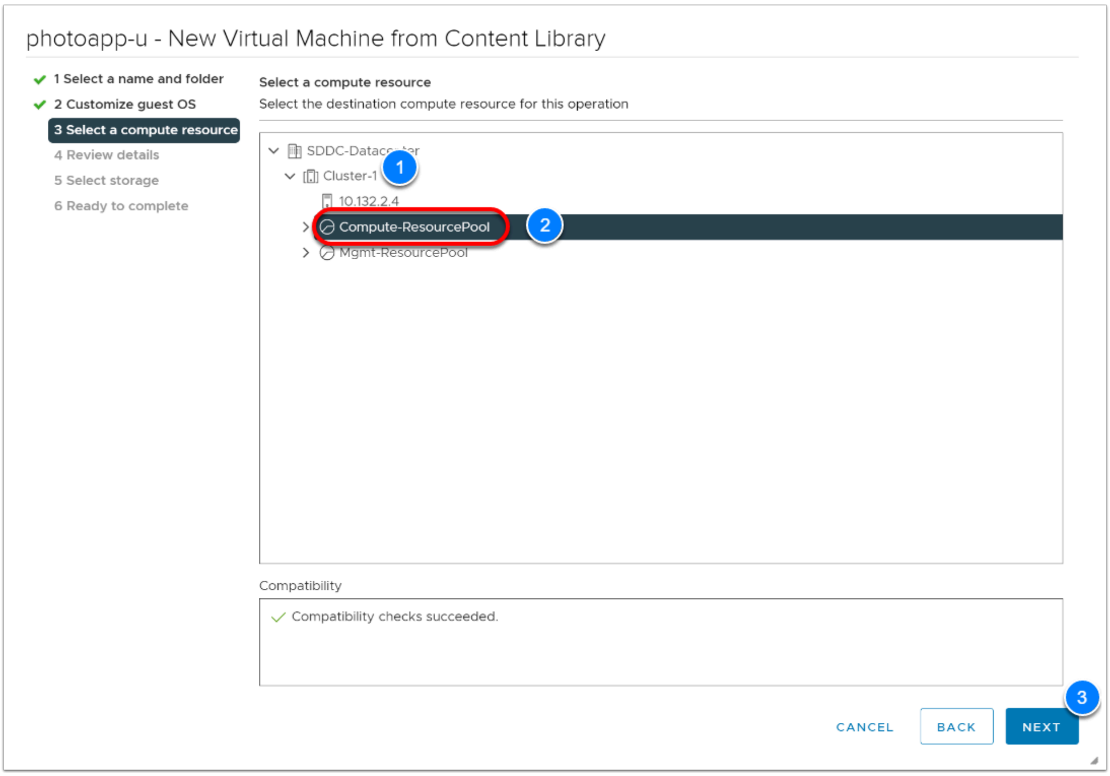
Virtual machine name: webserver01

Select a location for the virtual machine.

- vcenter.sddc-44-242-67-232.vmwarevmc.com
  - SDDC-Datacenter
    - Discovered virtual machine
    - Management VMs
    - Templates
    - Workloads

☑ Customize the operating system

16. In the **Select 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).
17. Click **Next** to continue



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 Ready to complete

Select a compute resource

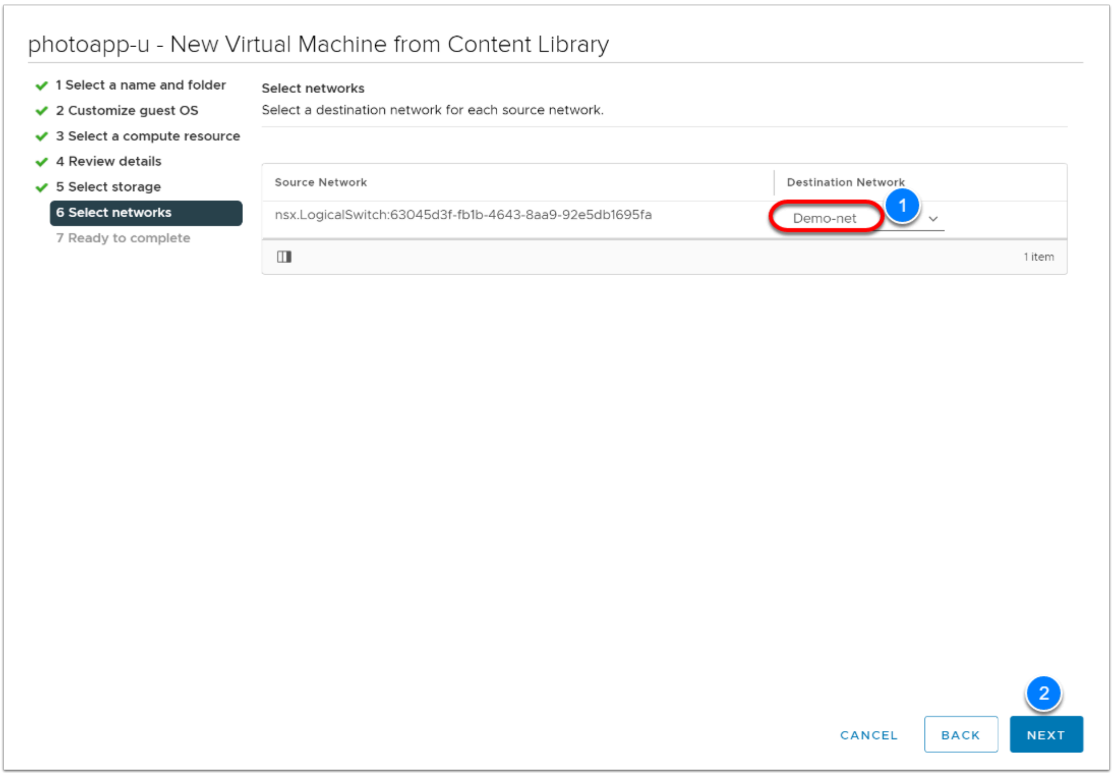
Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

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.

19. Click **Next** to continue.
20. In **Select Storage** Click **WorkloadDatastore** to select the datastore where the virtual machine will be provisioned.
    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
21. Click **Next** to continue
22. Click the drop-down below **Destination Network** to select the network for the virtual machine.
23. Click **Browse...**, then Select **Demo-Net** the network previously created in Task 1.
24. Click **Next** to continue.



photoapp-u - New Virtual Machine from Content Library

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nsx.LogicalSwitch:63045d3f-fb1b-4643-8aa9-92e5db1695fa	Demo-net

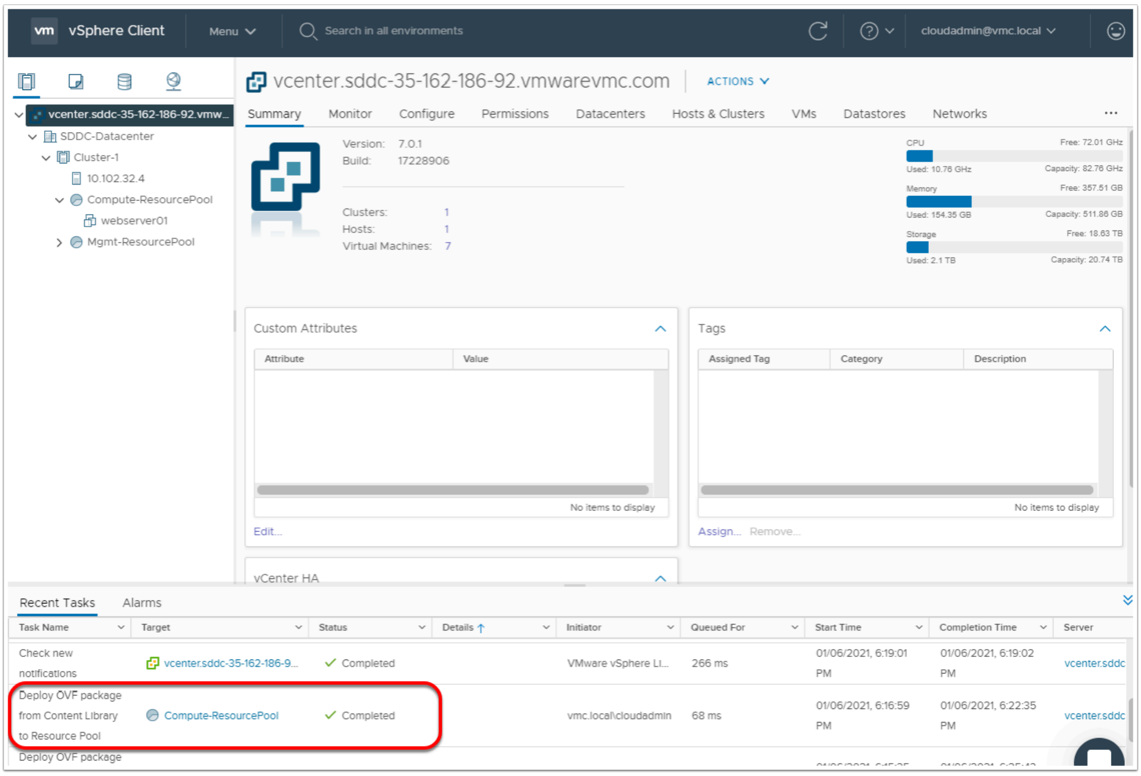
1 item

25. 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.

Task 3.2 - Clone a Virtual Machine

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



Version: 7.0.1
Build: 17228906

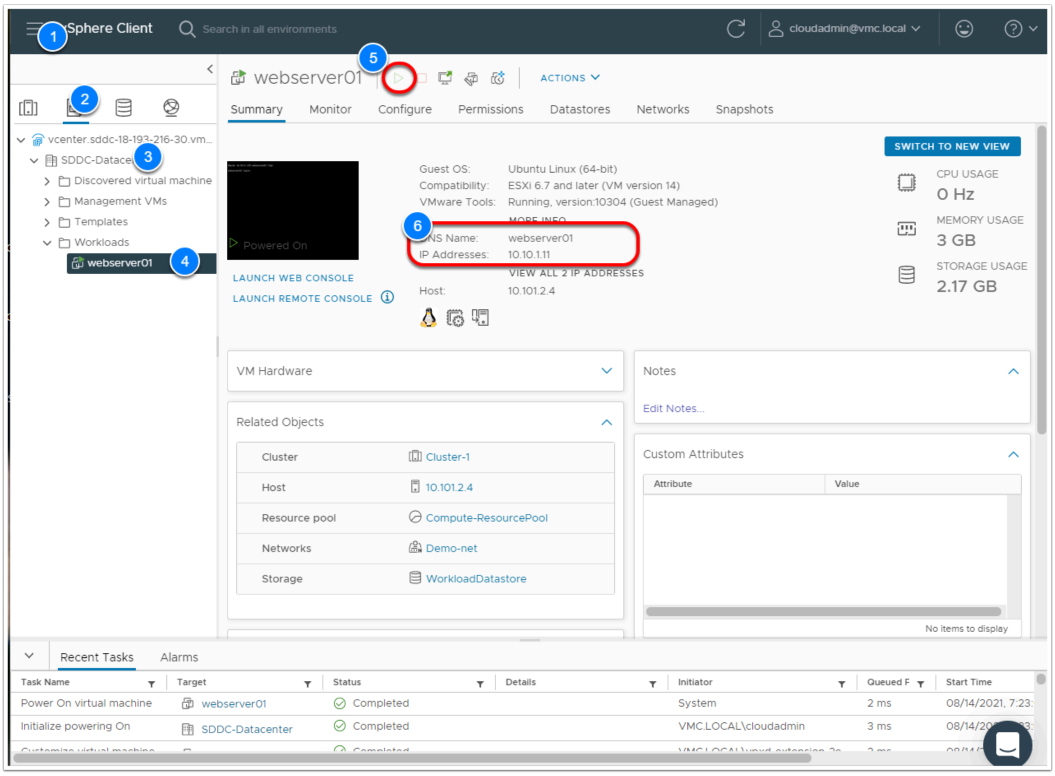
Clusters: 1
Hosts: 1
Virtual Machines: 7

CPU Free: 72.01 GHz, Used: 10.76 GHz, Capacity: 82.76 GHz
Memory Free: 357.51 GB, Used: 154.35 GB, Capacity: 511.86 GB
Storage Free: 18.63 TB, Used: 2.1 TB, Capacity: 20.74 TB

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Check new notifications	vcenter.sddc-35-162-186-9...	✓ Completed		VMware vSphere Li...	266 ms	01/06/2021, 6:19:01 PM	01/06/2021, 6:19:02 PM	vcenter.sddc
Deploy OVF package from Content Library to Resource Pool	Compute-ResourcePool	✓ Completed		vmc.local\cloudadmin	68 ms	01/06/2021, 6:16:59 PM	01/06/2021, 6:22:35 PM	vcenter.sddc
Deploy OVF package								

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.

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 execute the power on operation.



webserver01

Guest OS:	Ubuntu Linux (64-bit)
Compatibility:	ESXi 6.7 and later (VM version 14)
VMware Tools:	Running, version:10304 (Guest Managed)
DNS Name:	webserver01
IP Addresses:	10.10.1.11
Host:	10.101.2.4

CPU USAGE 0 Hz

MEMORY USAGE 3 GB

STORAGE USAGE 2.17 GB

Related Objects	
Cluster	Cluster-1
Host	10.101.2.4
Resource pool	Compute-ResourcePool
Networks	Demo-net
Storage	WorkloadDatastore

Attribute	Value

Task Name	Target	Status	Details	Initiator	Queued F	Start Time
Power On virtual machine	webserver01	Completed		System	2 ms	08/14/2021, 7:23:
Initialize powering On	SDDC-Datacenter	Completed		VMC.LOCAL\cloudadmin	3 ms	08/14/20

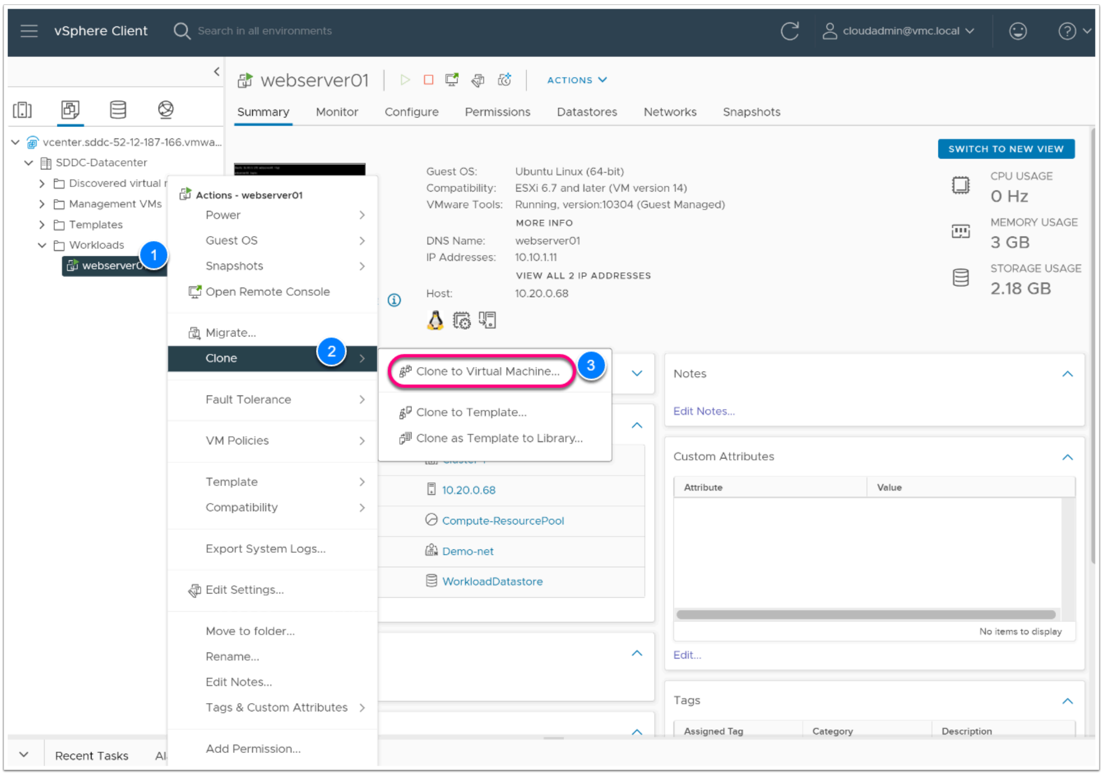
Note: Please wait until the virtual machine is fully powered on and has an IP before proceeding to the next step.

⚠ If the webserver 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**

3.2.1 - Clone Webserver01

1. Right-click on **webserver01** to expose the Actions menu.
2. Click on **Clone** to expose a secondary menu of options.
3. Click **Clone to Virtual Machine** to initiate the cloning wizard.



4. Next to **Virtual machine name** enter **webserver02**.
5. Click the **arrow** next to SDDC-Datacenter to expose the folders available.
6. Click the **Workloads** folder for the virtual machine location.
7. Click **Next** to continue.
8. Click the **arrow** next to Cluster-1 to expose the resource pools available
9. Click on **Compute-ResourcePool** to ensure it is selected for the target virtual machine.
10. Click **Next** to continue.
11. Click on **WorkloadDatastore** to ensure it is selected as the destination for the virtual machine.
12. Click **Next** to continue.

    We will now set the options for cloning. We will need to customize the operating system to change the server name and also power on the virtual machine after cloning is complete.

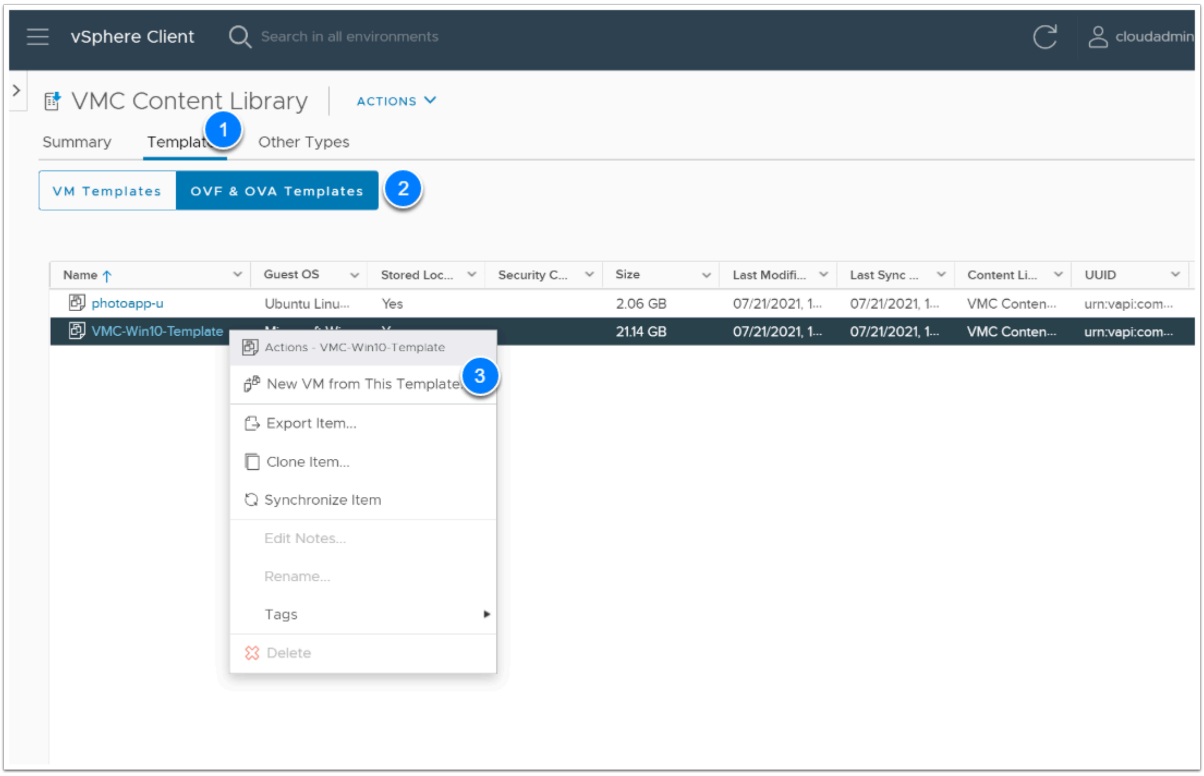
13. Click the checkbox next to **Customize the operating system**.
14. Click the checkbox next to **Power on virtual machine after creation**.
15. Click **Next** to continue.
16. Select the **LinuxSpec** customization specification.
17. Click **Next** to continue.
18. Review the information for accuracy 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 3.3 - Deploy a Windows 10 Virtual Machine

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

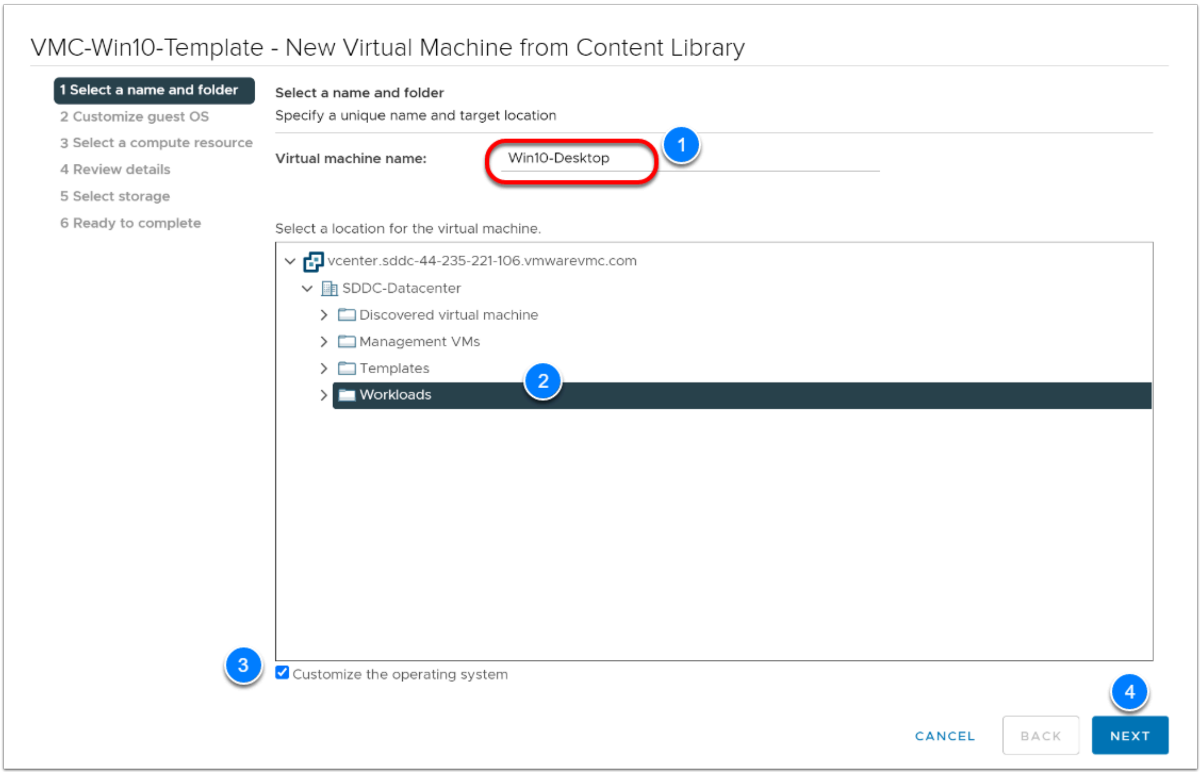
1. Click **Menu**.
2. Click on **Content Libraries**.
3. Click on the **VMC Content Library** that was previously synchronized.
4. Click the **Templates** tab to access the template synchronized in the content library.
5. Click the **OVF & OVA Templates** Tab
6. Right-click on the **VMC-Win10-Template**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



Name ↑	Guest OS	Stored Loc...	Security C...	Size	Last Modifi...	Last Sync ...	Content Li...	UUID
photoapp-u	Ubuntu Linu...	Yes		2.06 GB	07/21/2021, 1...	07/21/2021, 1...	VMC Conten...	urn:vapi:com...
VMC-Win10-Template	[illegible]	[illegible]		21.14 GB	07/21/2021, 1...	07/21/2021, 1...	VMC Conten...	urn:vapi:com...

8. Enter **Win10-Desktop** for the virtual machine name.

9. Click the **arrow** next to SDDC-Datacenter to expose the folders available.
   In VMware Cloud on AWS customer workloads should be placed in the Workloads folder (or subfolder).
10. Click the **Workloads** folder.
11. Select the checkbox next to **Customize the operating system**.
12. Click **Next** to continue



VMC-Win10-Template - New Virtual Machine from Content Library

Select a name and folder

Specify a unique name and target location

Virtual machine name: Win10-Desktop

Select a location for the virtual machine.

vcenter.sddc-44-235-221-106.vmwarevmc.com
SDDC-Datacenter
Discovered virtual machine
Management VMs
Templates
Workloads
1
2
3
4

☑ Customize the operating system

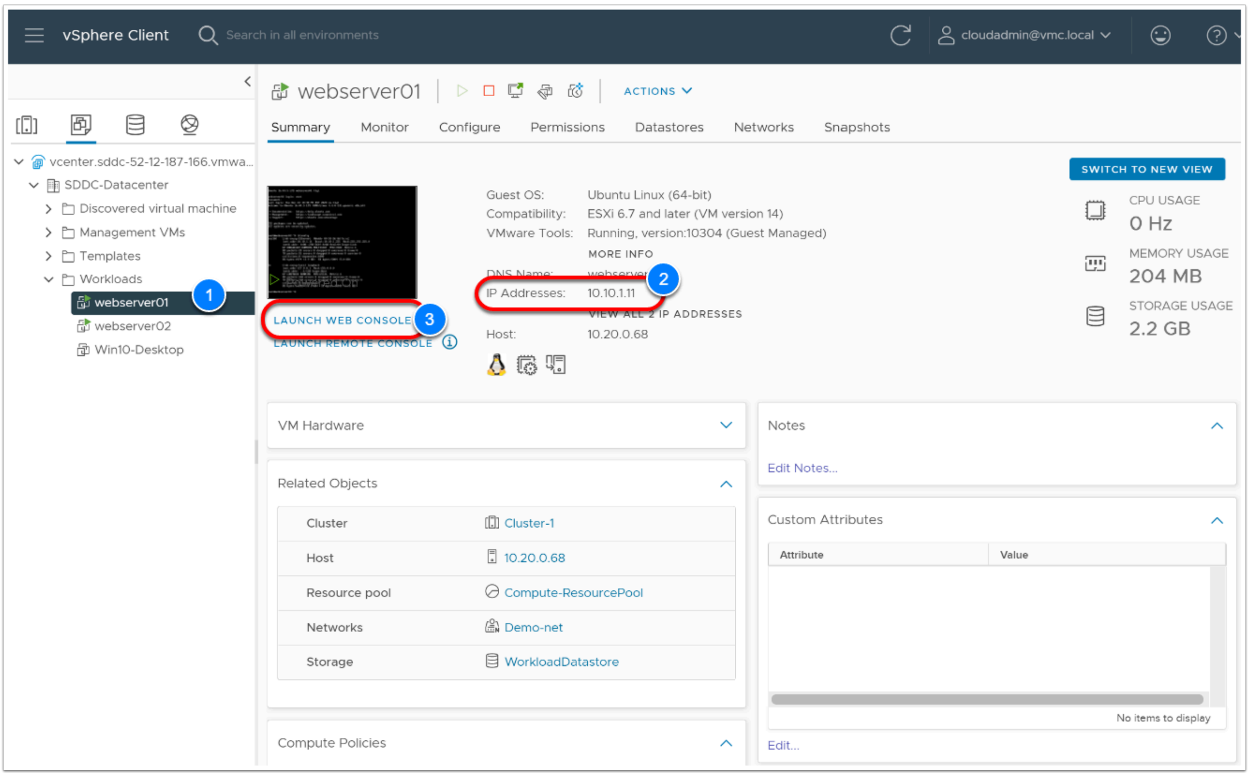
14. On the Customize guest OS page, select **WindowsSpec** customization specification.
15. Click **Next** to continue.
16. Click the arrow next to **Cluster-1** to expose the resource pools available.
    In VMware Cloud on AWS customer workloads should be placed in the **Compute-ResourcePool** (or subpool).
17. Select **Compute-ResourcePool**.
18. Click **Next** to continue
19. Click **Next**
20. Click **WorkloadDatastore** to select the datastore where the virtual machine will be provisioned.
21. Click **Next** to continue
22. Click the arrow below **Destination Network** to select the network for the virtual machine.
23. Click **Desktop-Net** to select the network previously created.
24. Click **Next** to continue.
25. Review the information for accuracy and click **Finish** to deploy the virtual machine

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

Task 3.4 - 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 **Webserver01** to bring it into focus. (You may need to Navigate to Menu > VMs and Templates)
2. Take note of the **IP Address** for webserver01 in the middle of the screen
3. Click **LAUNCH WEB CONSOLE**. The console should open in a new browser tab



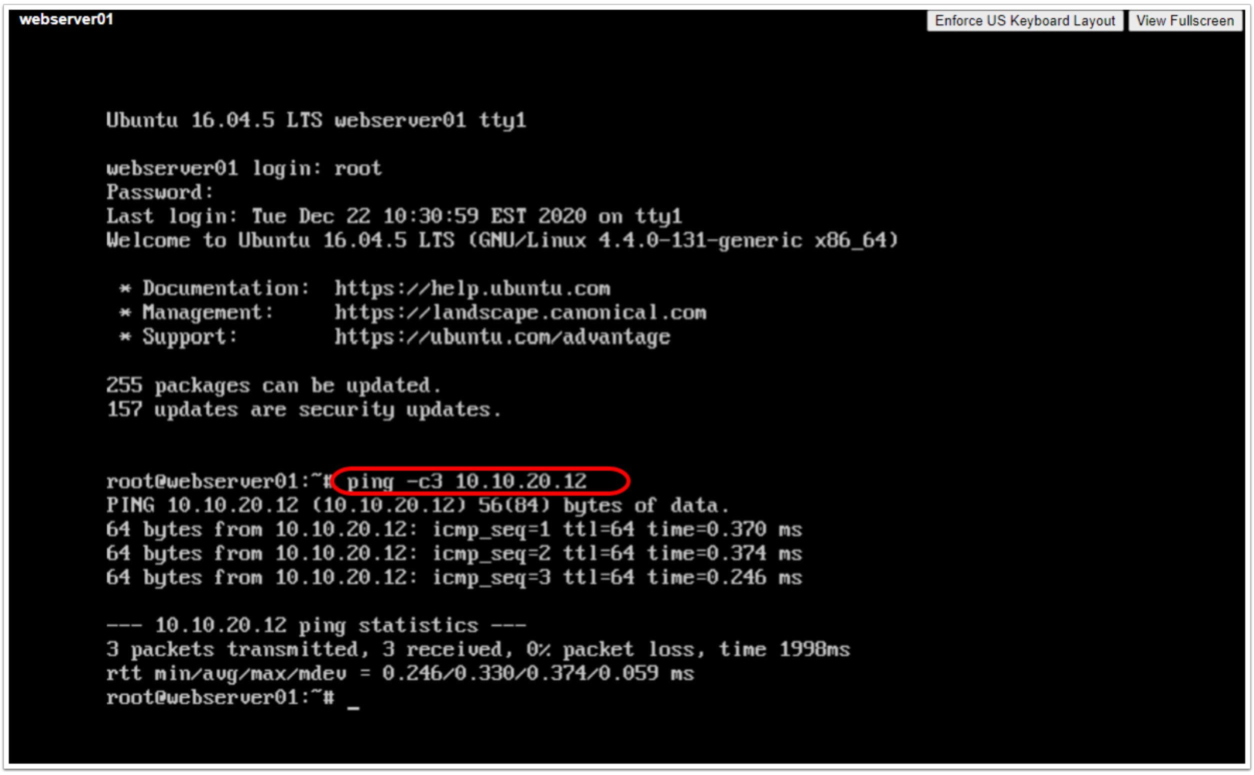
Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:10304 (Guest Managed)
DNS Name: webserver
IP Addresses: 10.10.1.11
Host: 10.20.0.68

CPU USAGE 0 Hz
MEMORY USAGE 204 MB
STORAGE USAGE 2.2 GB

Cluster	Cluster-1
Host	10.20.0.68
Resource pool	Compute-ResourcePool
Networks	Demo-net
Storage	WorkloadDatastore

Attribute	Value

3. Go back to the vSphere Client browser tab
4. Select **webserver02**
5. Take note of the **IP Address** for webserver02 in the middle of the screen. This will be needed in the next step.
6. Click the **Chrome Tab** of the console session for webserver01 to bring it back into focus.
7. At the login prompt enter **root** and press Enter.
8. At the password prompt enter **VMware1!** and press Enter.
9. 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**.
   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.
10. Verify the pings are successful.



```
Ubuntu 16.04.5 LTS webserver01 tty1

webserver01 login: root
Password:
Last login: Tue Dec 22 10:30:59 EST 2020 on tty1
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

255 packages can be updated.
157 updates are security updates.


root@webserver01:~# ping -c3 10.10.20.12
PING 10.10.20.12 (10.10.20.12) 56(84) bytes of data.
64 bytes from 10.10.20.12: icmp_seq=1 ttl=64 time=0.370 ms
64 bytes from 10.10.20.12: icmp_seq=2 ttl=64 time=0.374 ms
64 bytes from 10.10.20.12: icmp_seq=3 ttl=64 time=0.246 ms

--- 10.10.20.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.246/0.330/0.374/0.059 ms
root@webserver01:~# _
```

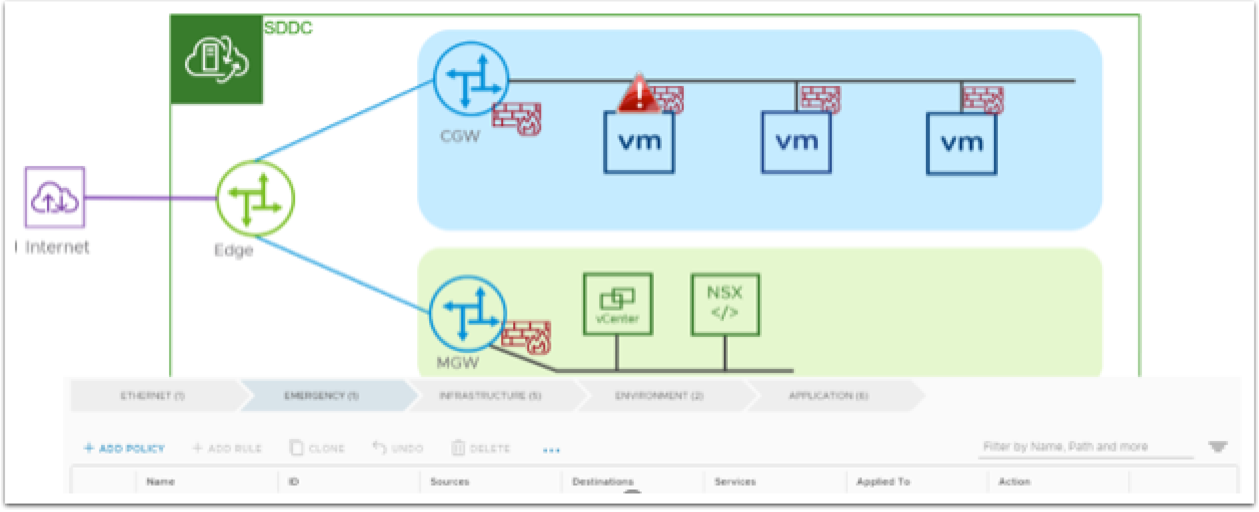
NOTE: Please leave this ping and console Window open for the next lesson. We will revisit it to verify the web servers can no longer communicate.

Task 3.5 - Configure VMC on AWS Advanced Network Services

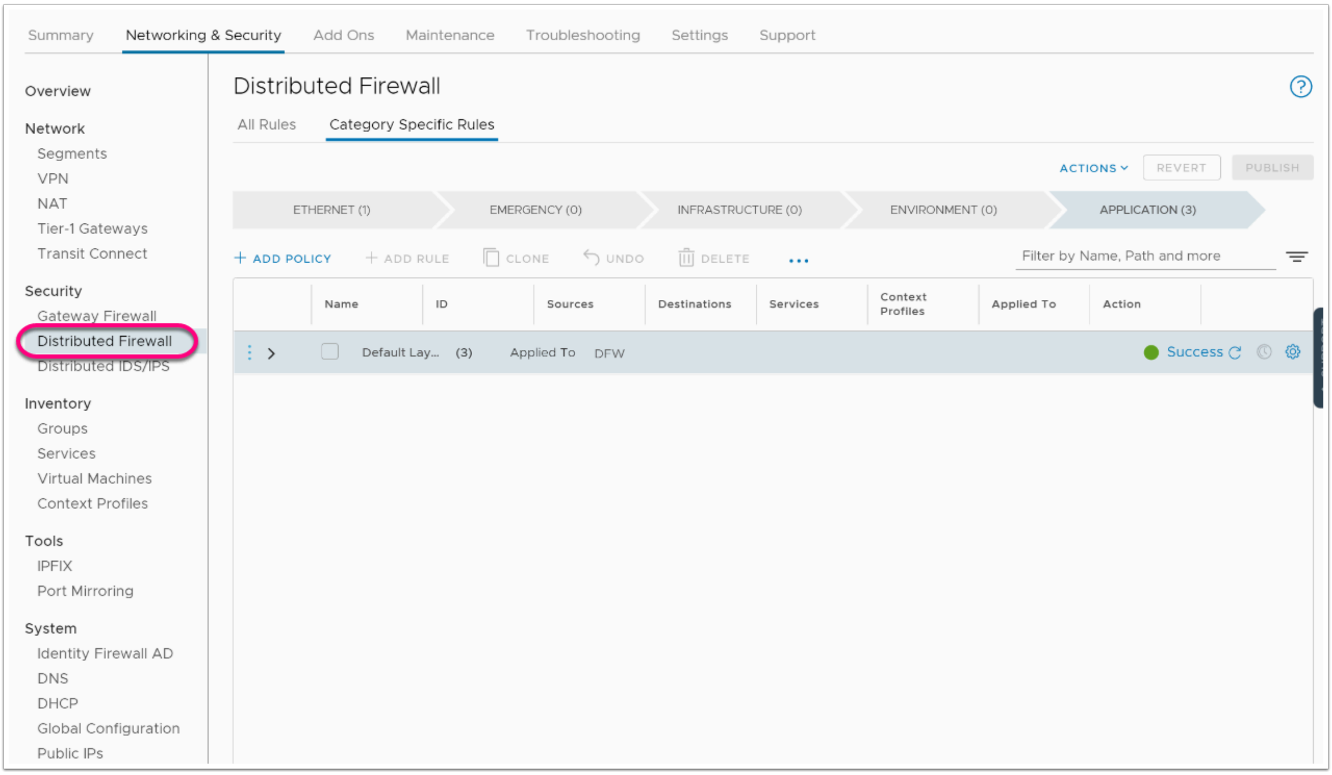
VMware Cloud on AWS Advanced Network Services is now available for new SDDC deployments.

Using VMware Cloud on AWS Advanced Network Services, users have the capability to 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 rules are hit from the top-down.



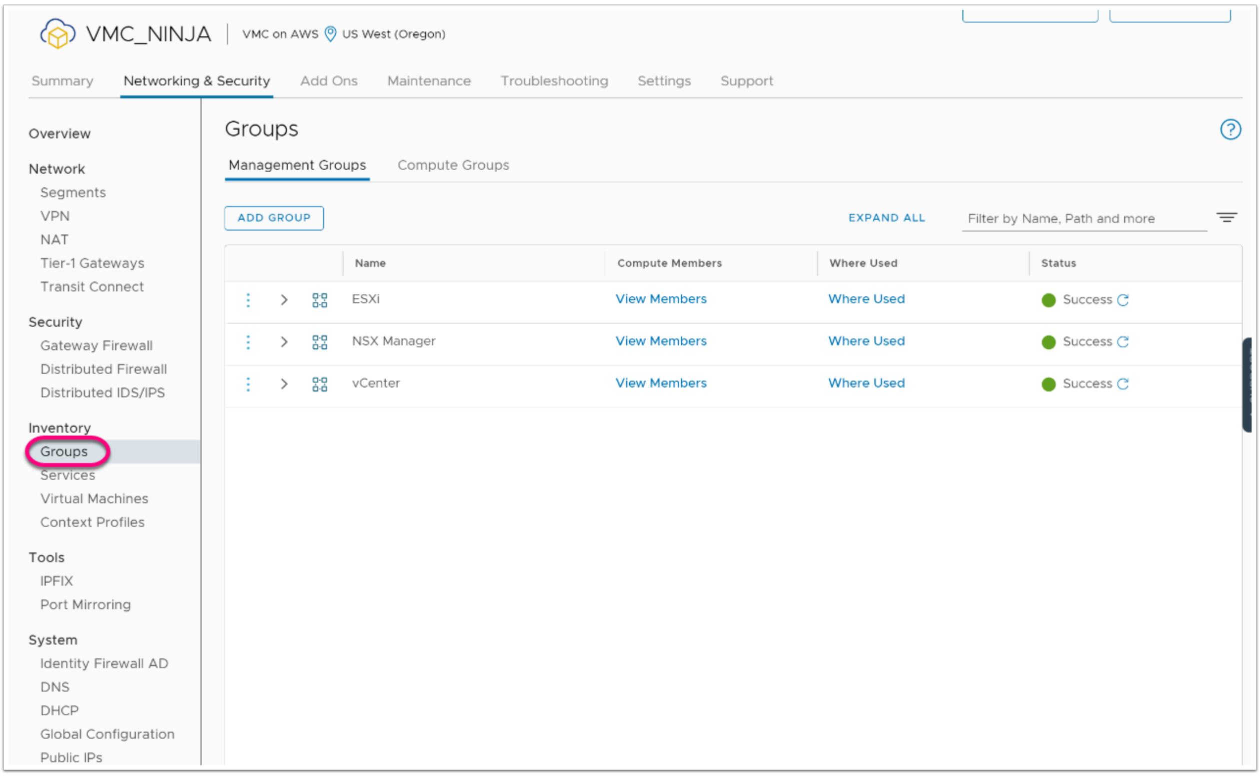
Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
Default Lay... (3)		Applied To DFW					Success

In addition to the new 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.

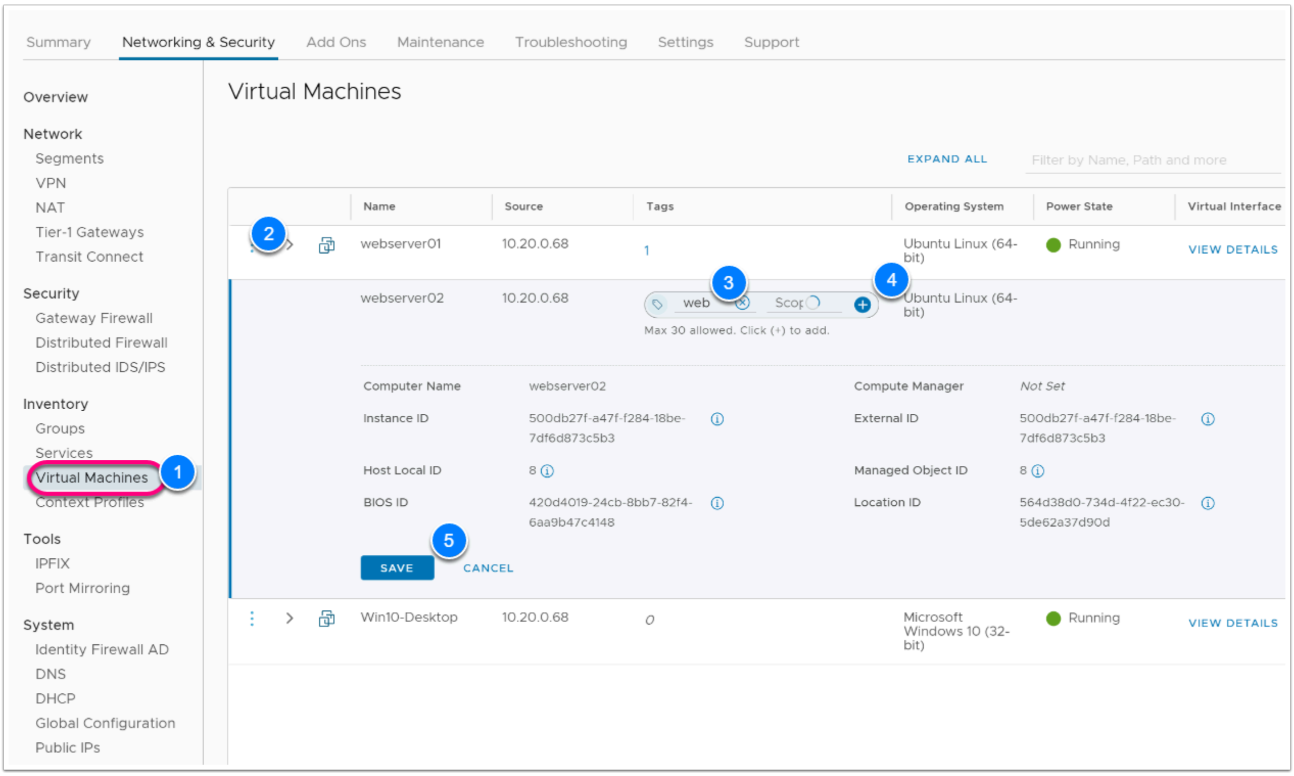
Task 3.5.1 - Apply Security Tag to Virtual Machines



Name	Compute Members	Where Used	Status
ESXi	View Members	Where Used	● Success
NSX Manager	View Members	Where Used	● Success
vCenter	View Members	Where Used	● Success

We will now create a network firewall policy in the distributed firewall to prevent communications between webserver01 and webserver02. To facilitate this, we will first create a tag, which will be applied to the VMs, followed by a dynamic group based on the tag.

1. Navigate back to the VMC on AWS console tab in your browser. You may need to sign back in. Click on the **Networking & Security** tab to access the networking configuration.
2. Under Inventory, click on **Virtual Machines** to access the virtual machines that are part of the SDDC.
3. Locate **webserver01** and click the three vertical dots and click **Edit**.
4. Under Tags, Type **Web**
5. Click **Add Item(s): Web**
6. Leave the **Scope** field blank Select the **blue +** sign to add the tag (a popup should appear and **web** should have a bubble around it)
7. Click **Save** to commit the changes
8. Repeat steps 3 - 7 for **webserver02**



Name	Source	Tags	Operating System	Power State	Virtual Interface
webserver01	10.20.0.68	1	Ubuntu Linux (64-bit)	● Running	VIEW DETAILS
webserver02	10.20.0.68	web Scope Max 30 allowed. Click (+) to add.	Ubuntu Linux (64-bit)		
Win10-Desktop	10.20.0.68	0	Microsoft Windows 10 (32-bit)	● Running	VIEW DETAILS

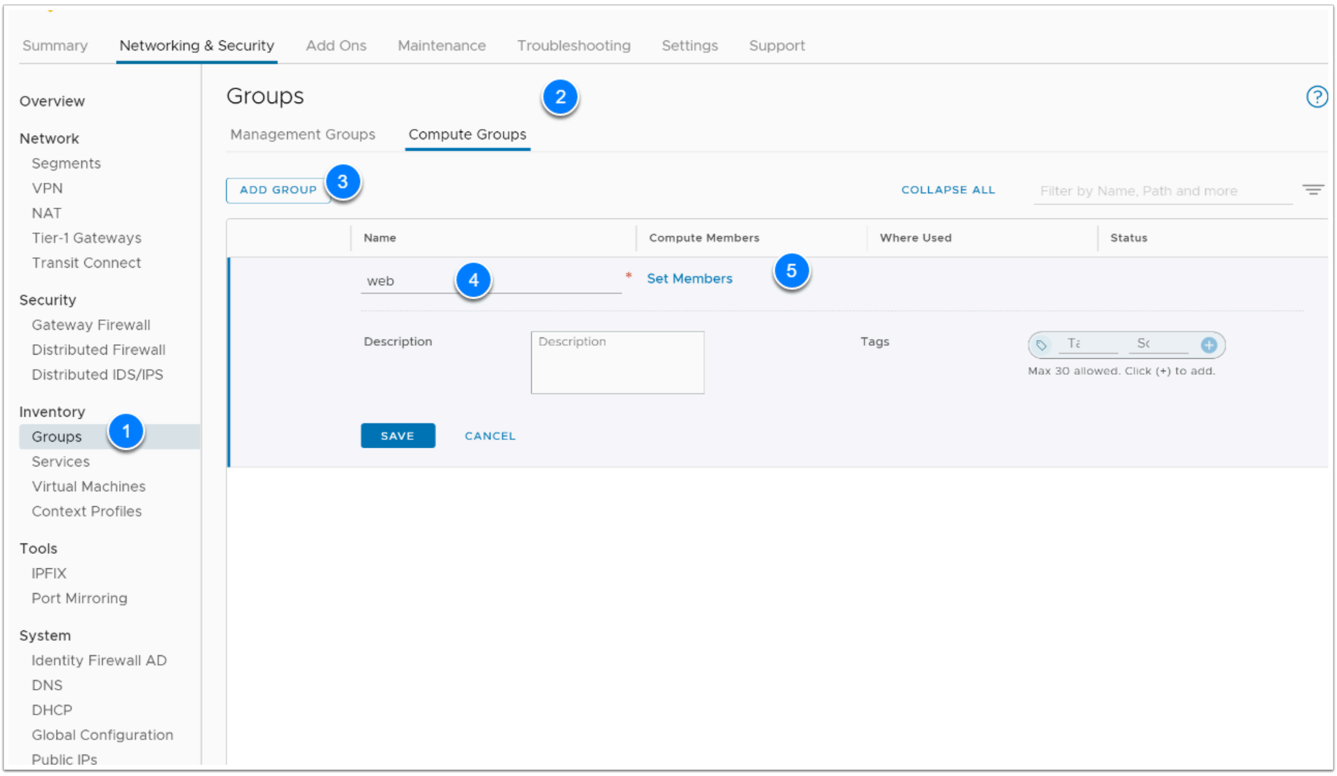
Computer Name	webserver02	Compute Manager	*Not Set*
Instance ID	500db27f-a47f-f284-18be-7df6d873c5b3	External ID	500db27f-a47f-f284-18be-7df6d873c5b3
Host Local ID	8	Managed Object ID	8
BIOS ID	420d4019-24cb-8bb7-82f4-6aa9b47c4148	Location ID	564d38d0-734d-4f22-ec30-5de62a37d90d

Task 3.5.2 - Create a Dynamic Security Group

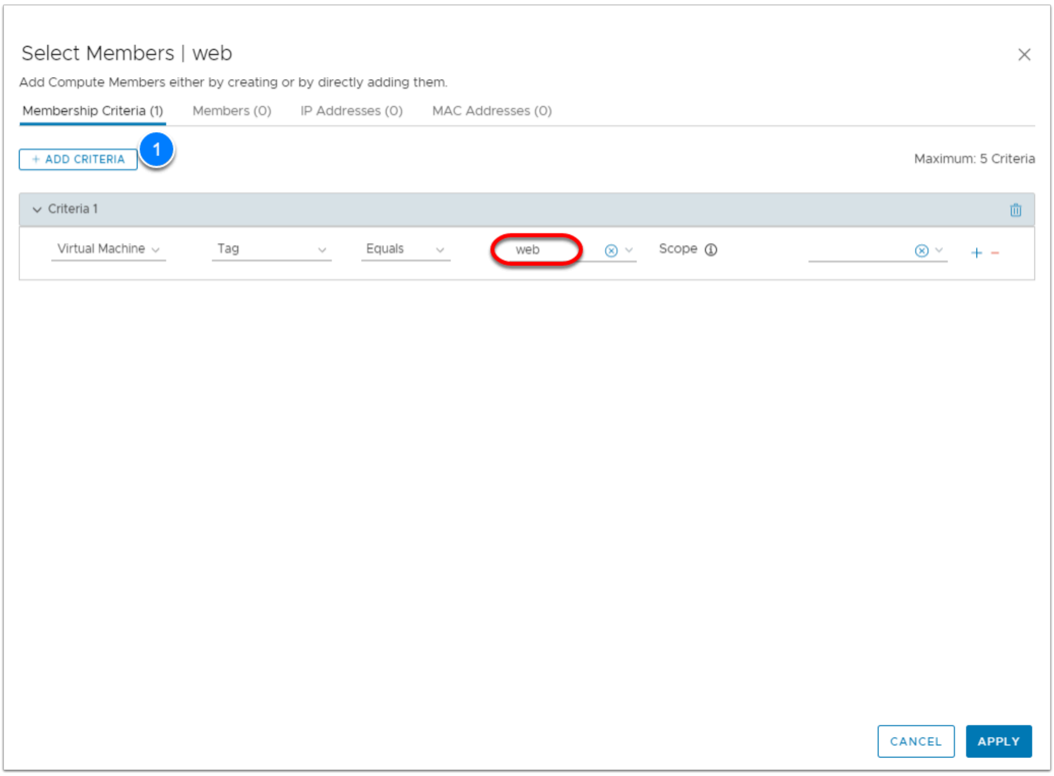
Groups can be used in VMware Cloud on AWS Advanced Network Services to group virtual machines and simplify rule based configuration. In this exercise we will group the two webservers into a group and then create a firewall rule to block communication between them. In a properly architected traditional 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. In the **Networking & Security** menu, click on **Groups** under Inventory.
2. Click on **Compute Groups**, then **Add Group**
3. Under Name enter **Web** for the name of the group.
4. Click **Set Members**



5. Select**+ADD CRITERIA**.
6. Leave the Virtual machine, Tag, Equals fields as is and in the 4th column type and select "**Web**". You should now see **VM Tag Equals Web** as your criteria. You can leave scope as blank.
7. Click **APPLY**
8. Click **SAVE**

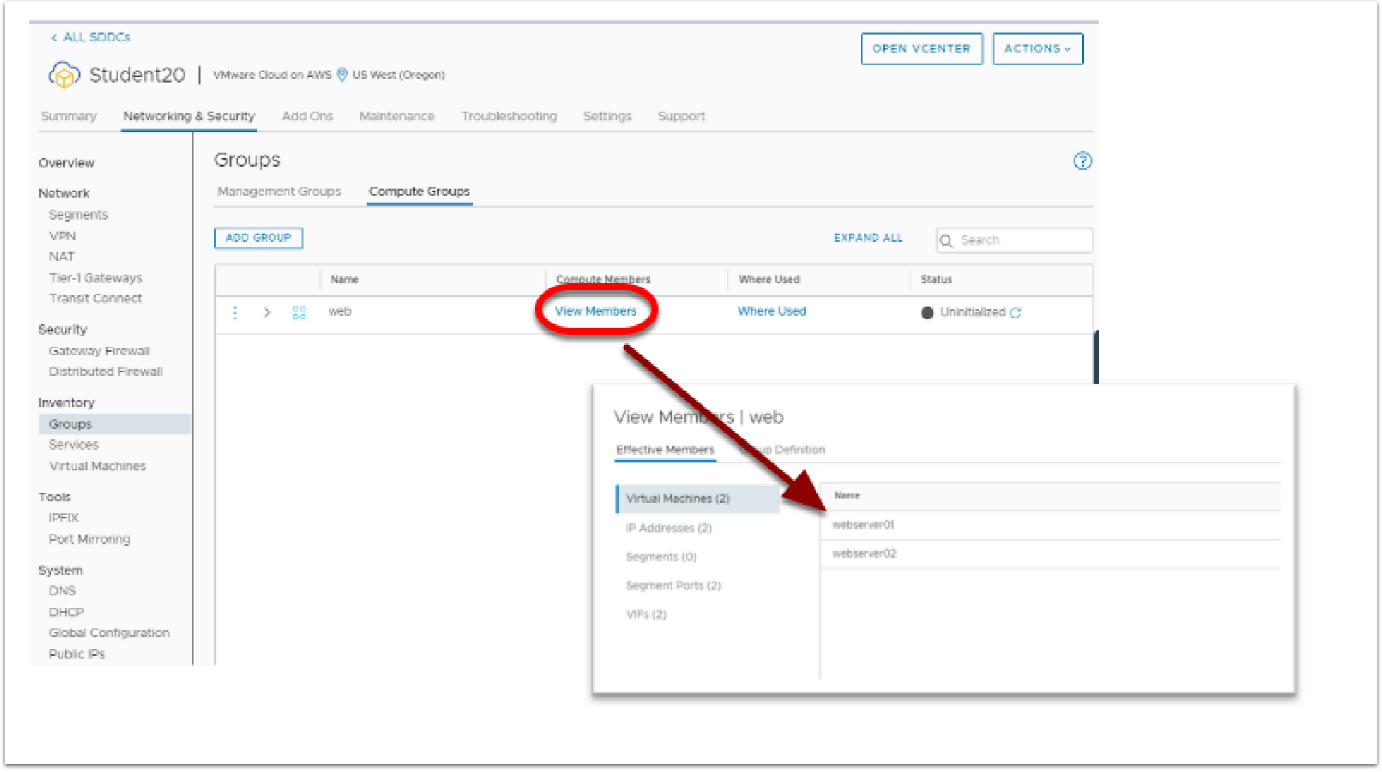


Select Members | web

Add Compute Members either by creating or by directly adding them.

Virtual Machine	Tag	Equals	web

Validate that both **webserver01** and **webserver02** appear in the group membership, by clicking **View Members.** Close the popup once complete



Name	Compute Members	Where Used	Status
web	View Members	Where Used	Uninitialized

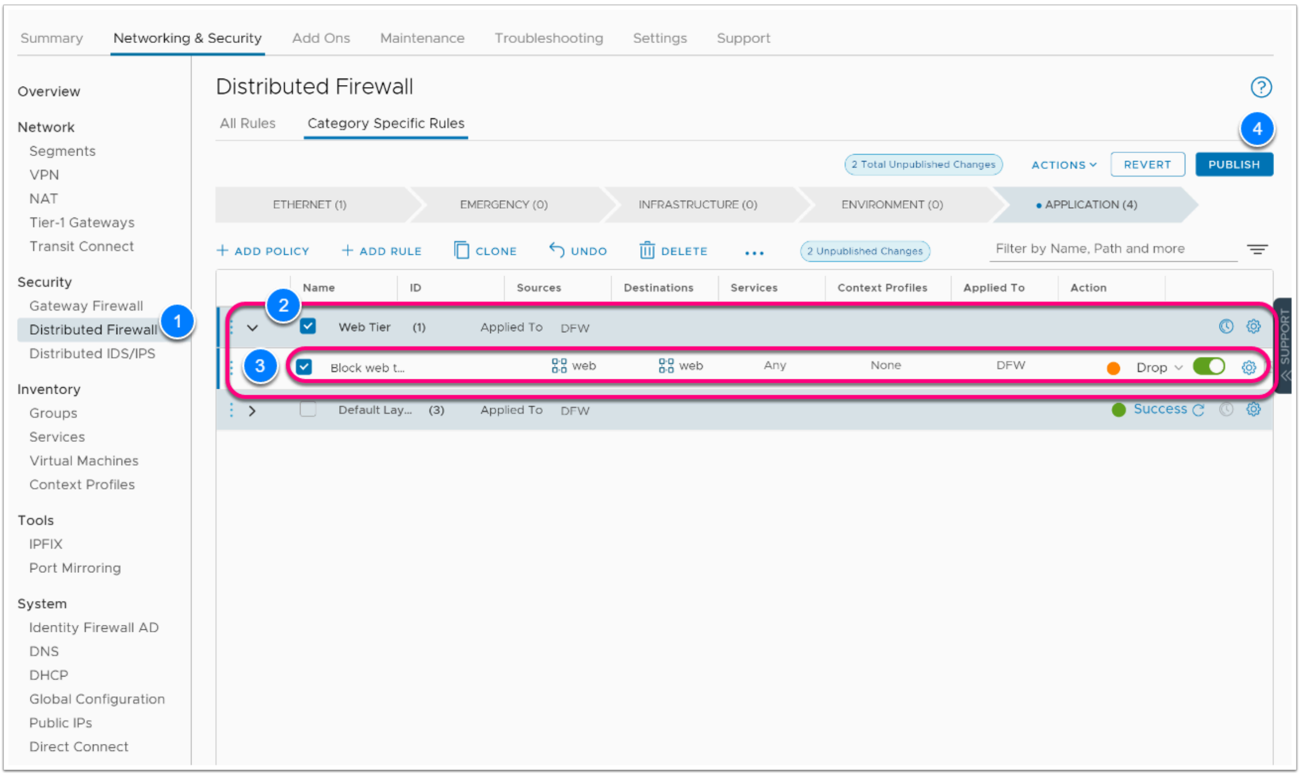
View Members | web

Name
webserver01
webserver02

If they do not, go back and verify there are no typos. Common errors encountered include typo on the tags, or not clicking the blue plus sign when adding the tag in the previous step.

Task 3.5.3 - 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.

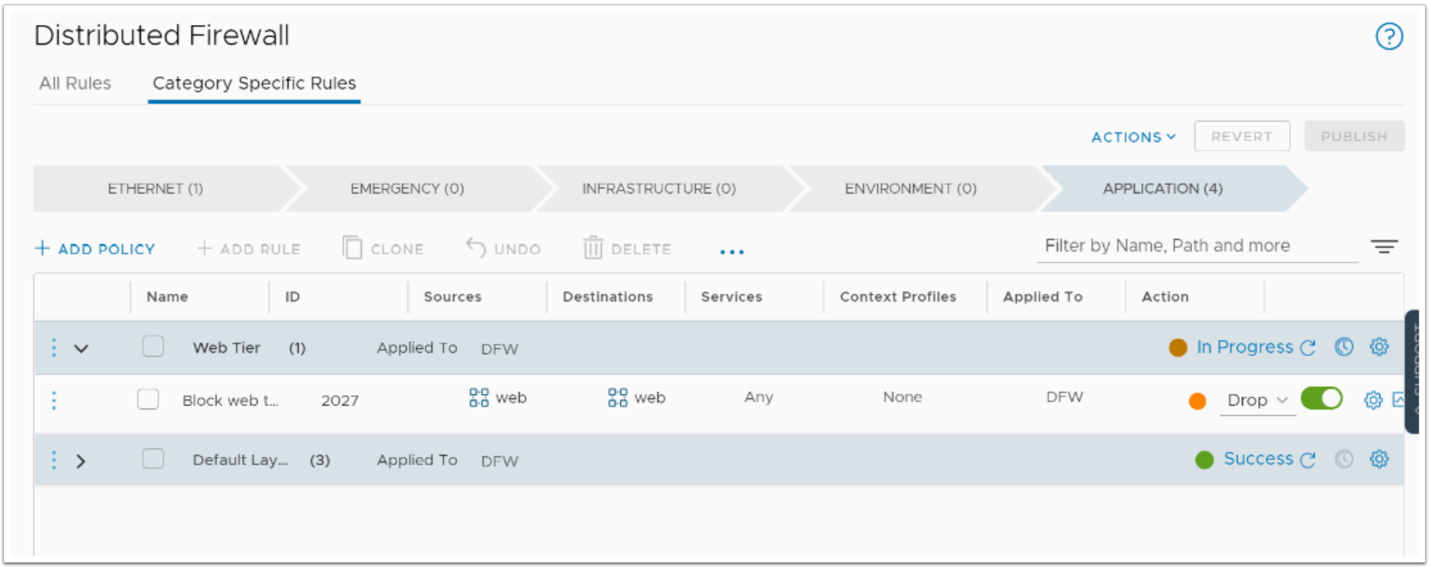


Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
☑ Web Tier	(1)	Applied To DFW					
☑ Block web t...		web	web	Any	None	DFW	Drop
□ Default Lay...	(3)	Applied To DFW					Success

1. In the **Networking and Security** Section, click **Distributed Firewall** on the left-hand side of the screen.
2. On the Arrow Shaped menu, click the **Application** bar.
3. 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.
4. Click the "**new policy**" text in the name column, Type **Web Tier**.
5. Click the **Checkbox** next to the **Web Tier** section.
6. Click **Add Rule** in the menu above the rules.
7. Under Name, Type **Block Web To Web**.
8. Under Action, click the **drop-down** and select **Drop**.
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** to commit the changes to the rule.
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** to commit the changes to the rule.
15. Click the **Gear** at the far right of the rule
16. Move the **Slider** to the right to enable logging

17. Click **APPLY**
18. Click **Publish** to commit the rule and begin blocking traffic between the web servers.
    NOTE: Action should be set to **Drop**

It might take a few 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.

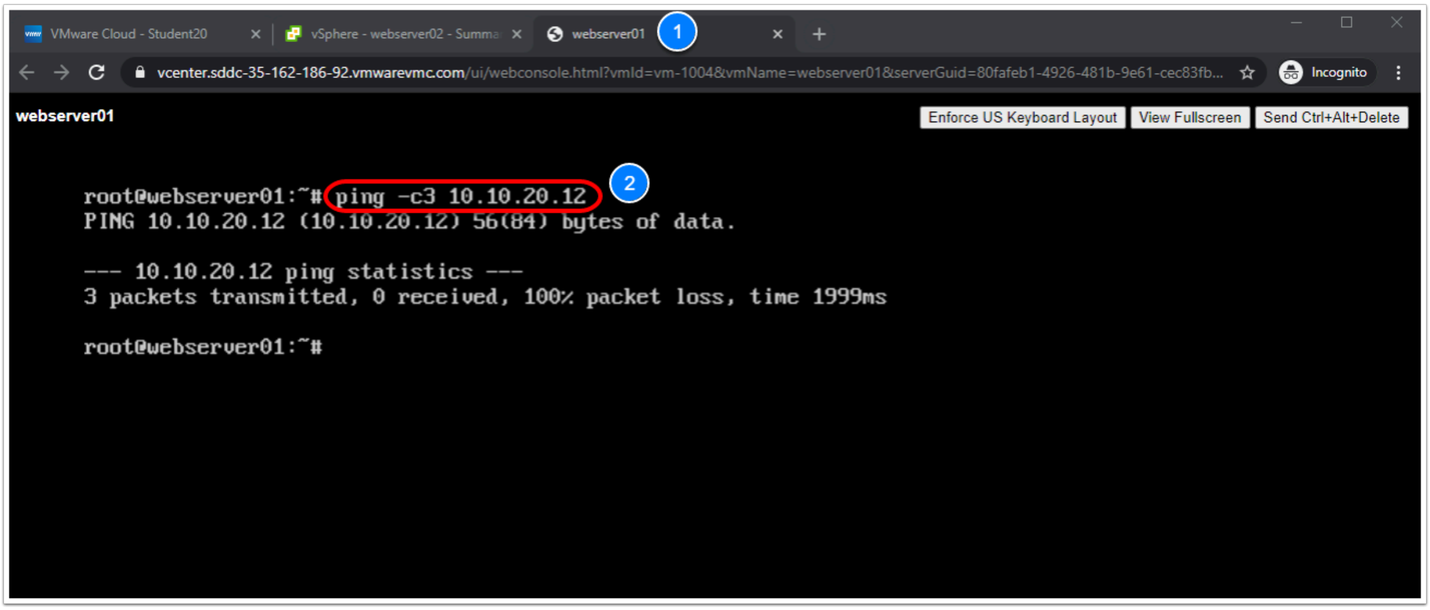


Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
Web Tier	(1)	Applied To	DFW				● In Progress
Block web t...	2027	web	web	Any	None	DFW	● Drop
Default Lay...	(3)	Applied To	DFW				● Success

Task 3.5.4 - Confirm Success of the DFW Policy

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

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 xx.xxx.xxx.xx)



VMware Cloud - Student20
vSphere - webserver02 - Summa
webserver01
1
vcenter.sddc-35-162-186-92.vmwarevmc.com/ui/webconsole.html?vmId=vm-1004&vmName=webserver01&serverGuid=80fafeb1-4926-481b-9e61-cec83fb...
Incognito
webserver01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
2

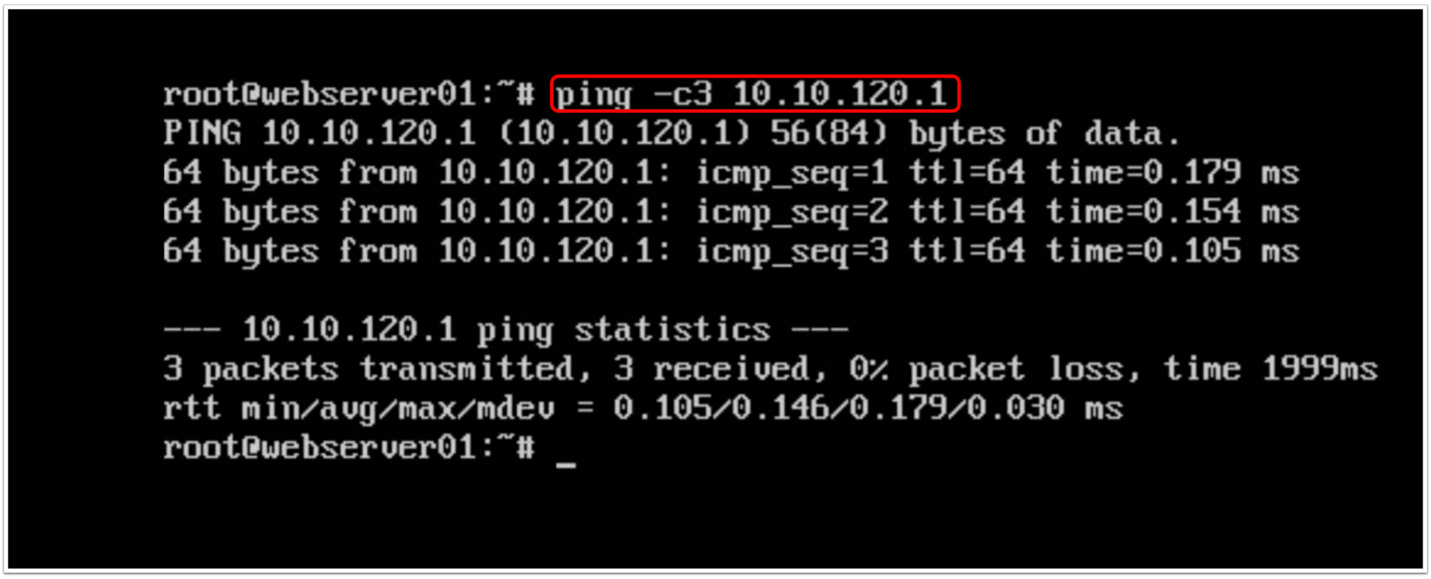
```
root@webserver01:~# ping -c3 10.10.20.12
PING 10.10.20.12 (10.10.20.12) 56(84) bytes of data.

--- 10.10.20.12 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

root@webserver01:~#
```

1. Click the Chrome Tab for **webserver01**.
2. Ping webserver02 IP address 10.10.xx.xxx. (ping -c3 xx.xx.xx.xx)

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

3. Type **Ping -c3 10.10.1xx.1** (i.e ping -c3 10.10.120.1)
4. Your ping test should succeed



```
root@webserver01:~# ping -c3 10.10.120.1
PING 10.10.120.1 (10.10.120.1) 56(84) bytes of data.
64 bytes from 10.10.120.1: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 10.10.120.1: icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from 10.10.120.1: icmp_seq=3 ttl=64 time=0.105 ms

--- 10.10.120.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.105/0.146/0.179/0.030 ms
root@webserver01:~# _
```

NOTE: If this pinging the Desktop-net gateway fails you need to double-check your Distributed firewall rule. Consult the rule definition in TASK 3.5.3, 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.

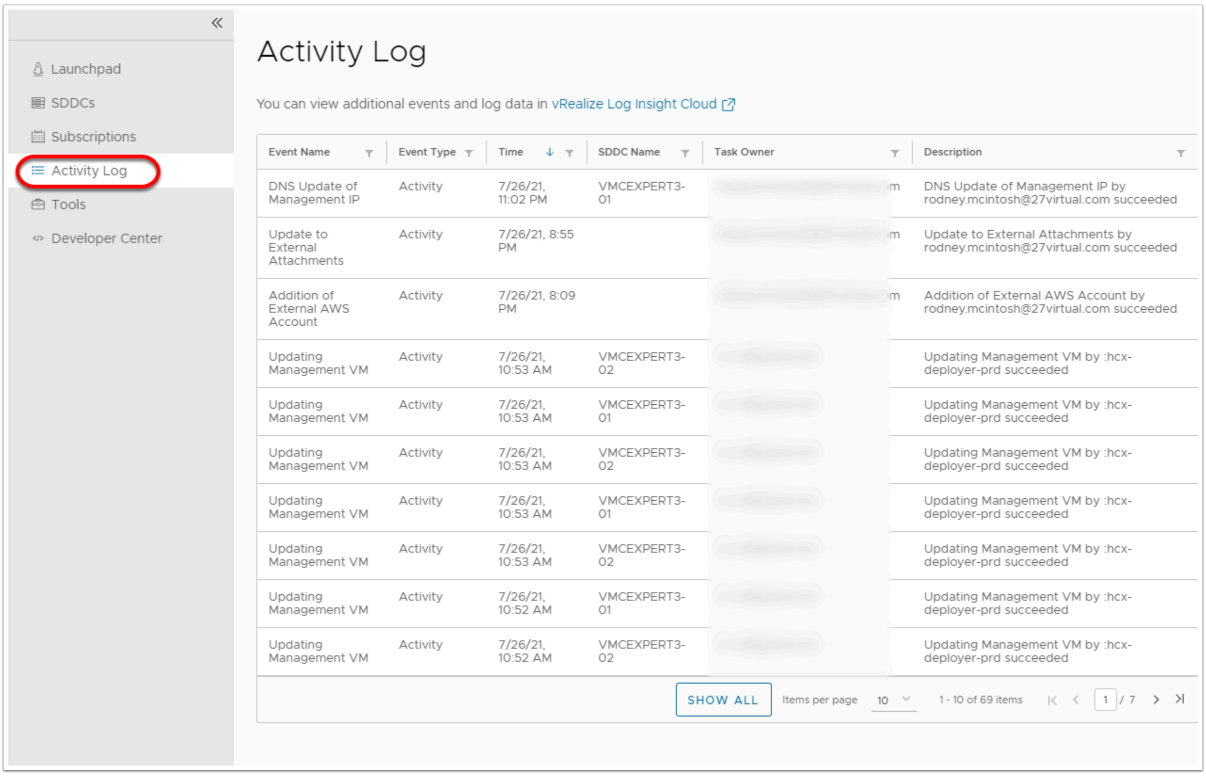
Task 4 - Visibility & Operations

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..



Activity Log

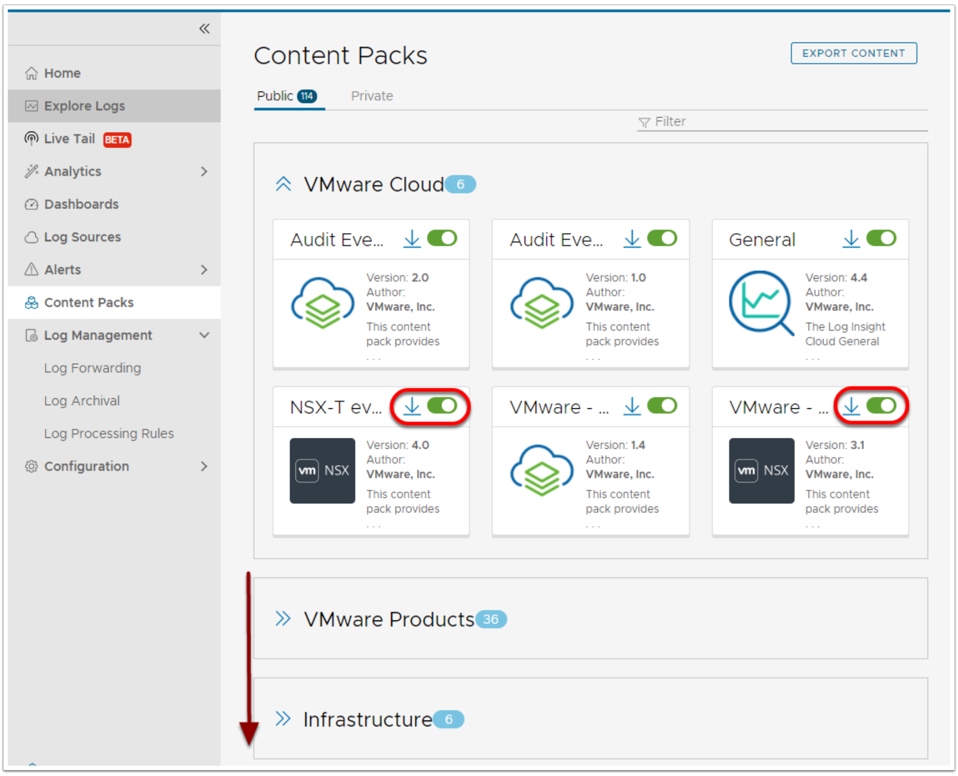
You can view additional events and log data in vRealize Log Insight Cloud

Event Name	Event Type	Time	SDDC Name	Task Owner	Description
DNS Update of Management IP	Activity	7/26/21, 11:02 PM	VMCEXPERT3-01	[redacted]	DNS Update of Management IP by rodney.mcintosh@27virtual.com succeeded
Update to External Attachments	Activity	7/26/21, 8:55 PM		[redacted]	Update to External Attachments by rodney.mcintosh@27virtual.com succeeded
Addition of External AWS Account	Activity	7/26/21, 8:09 PM		[redacted]	Addition of External AWS Account by rodney.mcintosh@27virtual.com succeeded
Updating Management VM	Activity	7/26/21, 10:53 AM	VMCEXPERT3-02	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:53 AM	VMCEXPERT3-01	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:53 AM	VMCEXPERT3-02	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:53 AM	VMCEXPERT3-01	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:53 AM	VMCEXPERT3-02	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:52 AM	VMCEXPERT3-01	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded
Updating Management VM	Activity	7/26/21, 10:52 AM	VMCEXPERT3-02	[redacted]	Updating Management VM by :hcx-deployer-prd succeeded

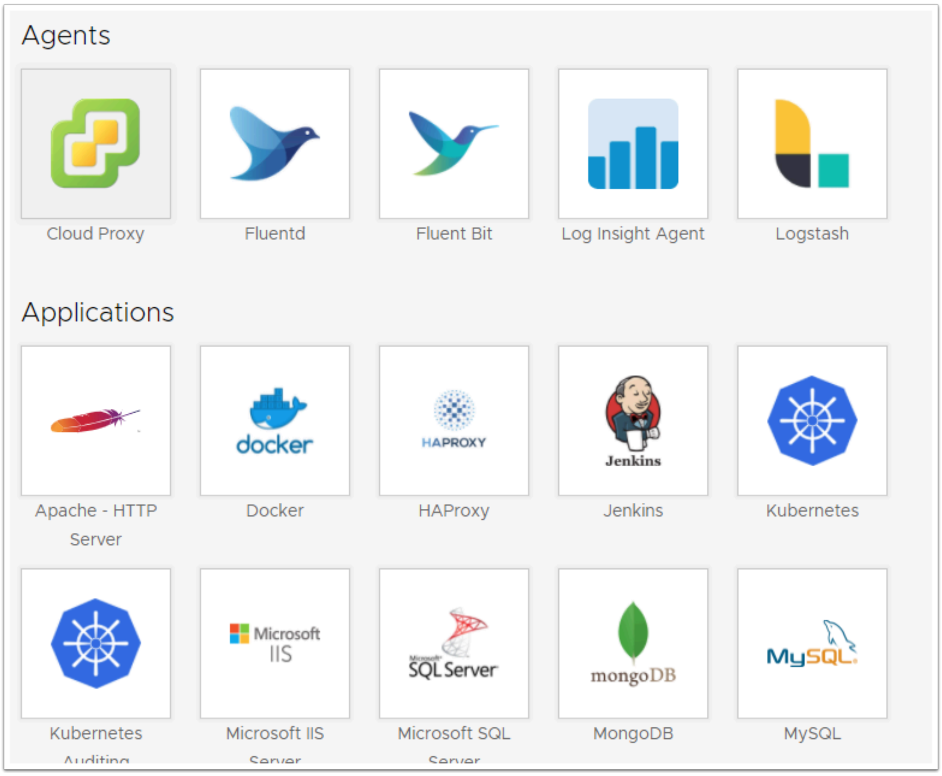
We'll now take a look at Log Insight were we will be able to see log entries providing more details and from multiple sources.

2. Click **vRealize Log Insight Cloud**
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
NOTE: Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs

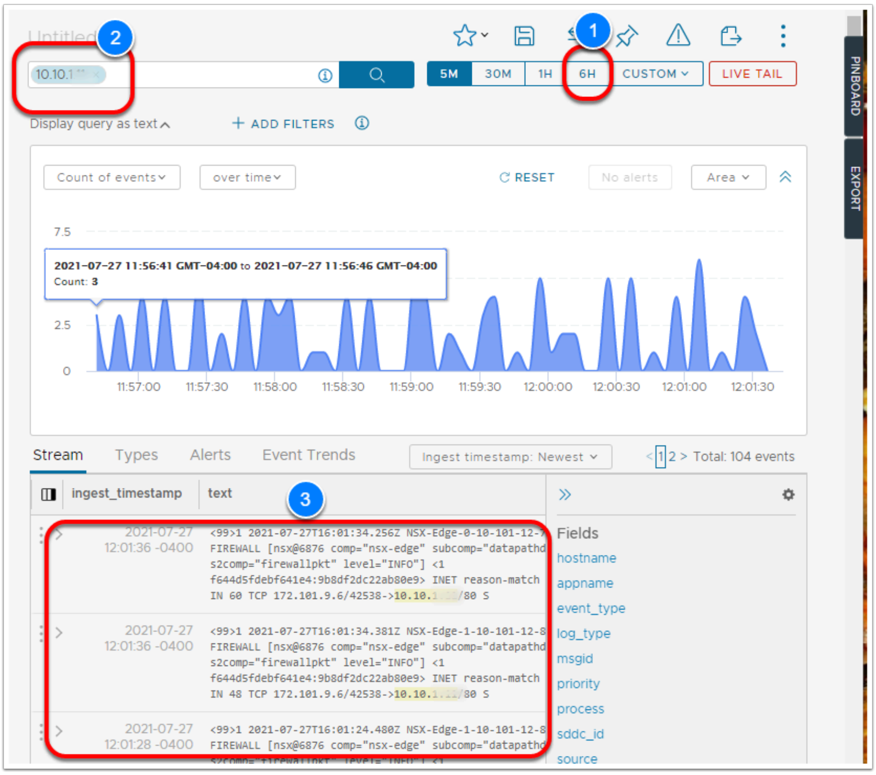


6. In the left Pane, Click Log Sources, to see all of the sources log insight cloud supports



7. In the Left Pane, Click **Dashboards**
8. Scroll down and click **Distributed Firewall - Traffic**
9. **adjust the time scope to 6H. to See log entries over the past 6 hours**
10. Click **Explore Log**, in the left pane

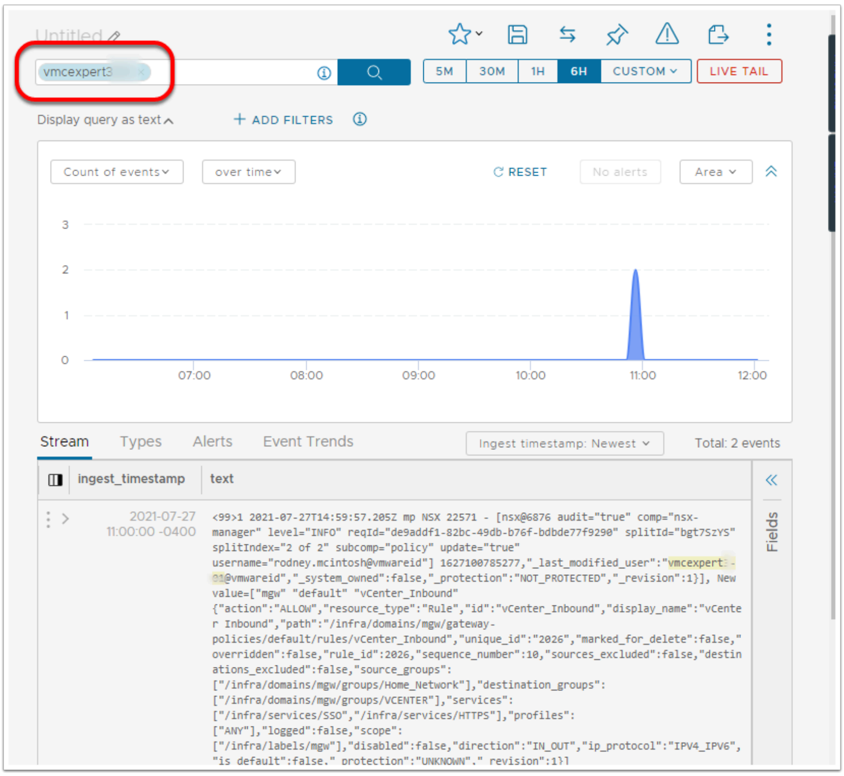
11. In the search bar type in the <**IP address of your webserver01**> (10.10.x.x)
12. Notice the firewall log entries from your earlier pings



2021-07-27 11:56:41 GMT-04:00 to 2021-07-27 11:56:46 GMT-04:00
Count: 3

```
2021-07-27        <99>1 2021-07-27T16:01:34.256Z NSX-Edge-0-10-101-12-7
12:01:36 -0400    FIREWALL [nsx@6876 comp="nsx-edge" subcomp="datapathd
                  s2comp="firewallpkt" level="INFO"] <1
                  f644d5fdebf641e4:9b8df2dc22ab80e9> INET reason-match
                  IN 60 TCP 172.101.9.6/42538->10.10.1[redacted]/80 S

2021-07-27        <99>1 2021-07-27T16:01:34.381Z NSX-Edge-1-10-101-12-8
12:01:36 -0400    FIREWALL [nsx@6876 comp="nsx-edge" subcomp="datapathd
                  s2comp="firewallpkt" level="INFO"] <1
                  f644d5fdebf641e4:9b8df2dc22ab80e9> INET reason-match
                  IN 48 TCP 172.101.9.6/42538->10.10.1[redacted]/80 S

2021-07-27        <99>1 2021-07-27T16:01:24.480Z NSX-Edge-1-10-101-12-8
12:01:28 -0400    FIREWALL [nsx@6876 comp="nsx-edge" subcomp="datapathd
```

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



```
2021-07-27        <99>1 2021-07-27T14:59:57.205Z mp NSX 22571 - [nsx@6876 audit="true" comp="nsx-
11:00:00 -0400    manager" level="INFO" reqId="de9addf1-82bc-49db-b76f-bdbde77f9290" splitId="bgt7SzYS"
                  splitIndex="2 of 2" subcomp="policy" update="true"
                  username="rodney.mcintosh@vmwareid"] 1627100785277,"_last_modified_user":"vmcexpert[redacted]-
                  [redacted]@vmwareid","_system_owned":false,"_protection":"NOT_PROTECTED","_revision":1}], New
                  value=["mgw" "default" "vCenter_Inbound"
                  {"action":"ALLOW","resource_type":"Rule","id":"vCenter_Inbound","display_name":"vCente
                  r Inbound","path":"/infra/domains/mgw/gateway-
                  policies/default/rules/vCenter_Inbound","unique_id":"2026","marked_for_delete":false,"
                  overridden":false,"rule_id":2026,"sequence_number":10,"sources_excluded":false,"destin
                  ations_excluded":false,"source_groups":
                  ["/infra/domains/mgw/groups/Home_Network"],"destination_groups":
                  ["/infra/domains/mgw/groups/VCENTER"],"services":
                  ["/infra/services/SSO","/infra/services/HTTPS"],"profiles":
                  ["ANY"],"logged":false,"scope":
                  ["/infra/labels/mgw"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6",
                  "is_default":false,"_protection":"UNKNOWN","_revision":1}]
```

Conclusion

ℹ 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

2nd Gen Intel® Xeon® Scalable processors are designed to take full advantage of the scalable memory, storage and network bandwidth offered by AWS storage-optimized i3en instances to deliver optimal performance for your applications running in VMware Cloud on AWS.

https://www.vmware.com/company/news/releases/vmw-newsfeed.VMware-Cloud-on-AWS-Delivers-on-Customer-Requirements-for-Agility-Business-Continuity-and-Better-Cloud-Economics.7aa53d77-e377-458d-960f-5bf151e3f90c.html

VMware Cloud on AWS running on i3en.metal instances powered by 2nd Generation Intel® Xeon® Scalable processors, include new capabilities that provide an enhanced solution for disaster recovery and migrating application to the cloud.

- Intel® Mesh architecture optimizes data sharing and memory access between all vCPUs to fully take advantage of the 1.5x more RAM and 4.3x more raw storage capacity (as compared to i3) while delivering consistent, low latencies.
- VMware vSphere® vMotion® allows live migration of VMs from one Intel host to another with zero downtime.
- I3en instances deliver 4x the raw storage capacity at roughly half the cost per GB of storage per host compared to previous offerings, making them ideal for disaster recovery and other storage-demanding use cases.
    - Double orders per minute on scaled up i3.en instances running SQL Server:https://www.vmware.com/techpapers/2020/sqlserver-vmconaws-i3en-perf.html
    - Double the Oracle database operations per minute in a scale out scenario:https://www.vmware.com/techpapers/2020/oracle-vmc-aws-i3en-perf.html