vmware®

Getting Started with Oracle Cloud VMware Solution

GET STARTED

Table of Contents

vmware® | **ORACLE** Cloud

Introduction

Oracle Cloud VMware Solution was made generally available on August 6th, 2020, in all oracle regions and *Oracle's dedicated region cloud@customer* service offering. The Oracle Cloud VMware Solution is a customer-managed, VMware Cloud Verified environment consisting of vCenter Server, ESXi hosts, vSAN, and NSX. Also included is VMware HCX to provide services such as seamless migrations and network extension from on-premises to Oracle Cloud VMware Solution and between Oracle VMware Solution Software-Defined Data Centers (SDDC).

Please see Figure 1 for a high-level architecture view the interconnectivity of the VMware SDDC, Oracle Cloud VMware Solution, and Oracle Cloud Infrastructure.
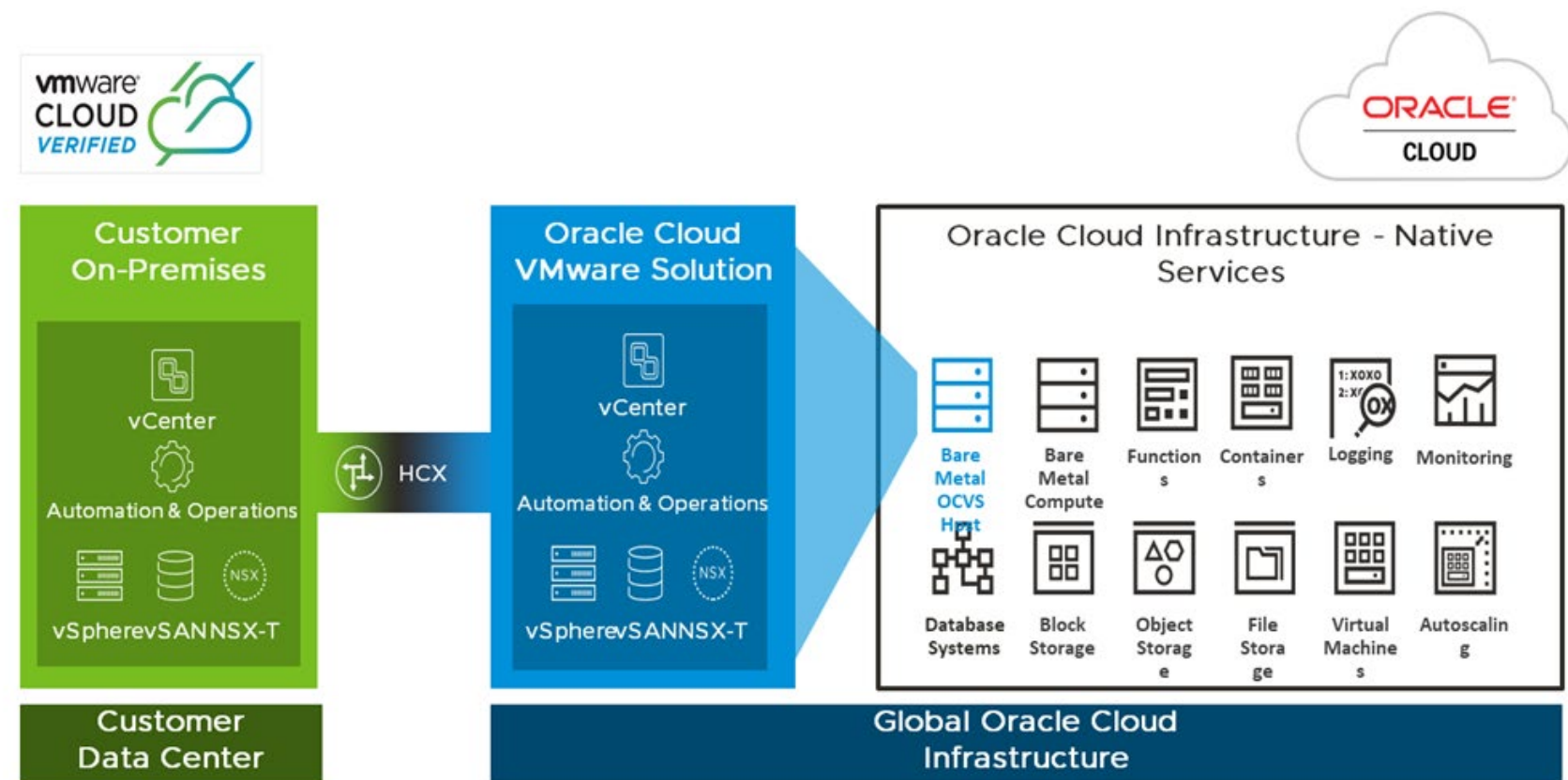
FIGURE 1: Oracle Cloud VMware Solution Architecture Diagram

This eBook will provide an overview of the Oracle Cloud VMware Solution running vSphere 7.0 Update 2 and guide through deploying a VMware Cloud SDDC on Oracle Cloud Infrastructure (OCI), network connectivity, workload migration, and leveraging native Oracle Cloud services. Throughout this eBook, there are additional resources, examples, and implementation details as reference.

Key terms

Before getting started, we will level set with the following concepts and terminology mentioned throughout this eBook and when using Oracle Cloud Infrastructure and Oracle Cloud VMware Solution. Here is a complete list of *Oracle Cloud Infrastructure key concepts and terminology*. The descriptions of the terms below are written in a way to describe how they are used in relationship to Oracle Cloud VMware Solution.

Bare-metal host – The Oracle Cloud VMware Solution's ESXi hosts are provisioned on bare-metal servers. Since the hosts are bare-metal, they can consume all CPU, memory, and networking resources available.

Compartment –A tenancy, which can also be known as the "root compartment," can be sub-divided into additional compartments. Resources that are provisioned must be assigned to a compartment. Administrators can limit access to the resources by compartments.

Console – GUI (Graphical User Interface) is accessed through a web browser. Oracle Cloud VMware Cloud Solution is deployed through the console.

Image – An image is a copy or template that new instances are deployed from. Customized configurations can be saved as an image for reuse. A Bastion Host's image type is selected during installation.

Instance – There are Oracle physical and virtual instances. A physical instance describes a physical compute Server. Virtual machines running in the Oracle Cloud VMware Solution are virtual instances.

Key pair – Using a key pair is a classic way of establishing a secure shell (SSH) connection to a server or device that allows SSH. A key pair includes a public and private key, making up a pair of keys. The public key is stored on the device and the private key locally on the connecting computer. Keys pairs are required to access Oracle Infrastructure via SSH.

Regions and availability domains – When deploying an Oracle Cloud VMware Solution instance, the bare-metal host belong to a single availability domain. The hosts are spread across fault domains in the availability domain. Regions are a geographical grouping of one or more availability domains.

Realms – Realms are a grouping of regions that are isolated from each other. Oracle Cloud Infrastructure currently offers a commercial realm and two realms for government cloud regions: FedRAMP and IL5 authorized.

Shape – A shape describes how much CPU and memory is assigned to an instance.

Tenancy – A tenancy is a logical divider in the Oracle cloud that separates users and resources from each other. Resources allocated for Oracle Cloud VMware Solution will have to be assigned to a tenancy.

Virtual Cloud Network (VCN) – A Virtual Cloud Network defines a network in the Oracle Cloud from an IP and routing perspective. The Virtual Cloud network can span availability domains in a region, but not across multiple regions.

Getting started

User account and permissions

A user account must be obtained with the appropriate permissions to log in to the Oracle Cloud to deploy Oracle Cloud Infrastructure. In a brand-new organization, the tenancy owner is the first administrator assigned to the tenancy. An Oracle Cloud administrator must create and grant users the proper permissions to access and deploy tenancy resources. The permissions to deploy Oracle Cloud Infrastructure is not the same as managing the VMware suite of software that makes up the Oracle Cloud VMware Solution. The VMware SDDC roles and responsibilities are handled the same as an on-premises VMware SDDC.

A user's account must be able to do the following to deploy an Oracle Cloud VMware Solution SDDC:

Service	Required Permission
Oracle Cloud Infrastructure Identity and Access Management	Manage dynamic groups and policies.
Oracle Cloud Infrastructure Networking	Manage VCNs, subnets, internet gateways, NAT gateways, service gateways, route tables, and security lists.

TABLE 1: User account and permissions

Visit *adding users* to learn more about account administration.

Logging into the Oracle Cloud

To get started, log into the *Oracle Cloud Sign-in page*. Once you have logged in with the proper permissions, you can deploy Oracle Cloud Infrastructure (OCI), including Oracle Cloud VMware Solution (OCVS).

A Cloud Account Name is required. This account name is not an email address or username but your tenancy name. If the Cloud Account Name is unknown, it can be found by using the **"Forgot your cloud account name?" Get Help** link.

Suppose the account has been configured to use **Single Sign-On**. In that case, the user will be prompted for their **Identify Provider,** then select **continue**, where they will then be prompted for a username/email address and password. If Single Sign-On is not configured, use the **Oracle Cloud Infrastructure Direct Sign-In**, requiring a username/email address and password.

If all fails, reach out to the Oracle Cloud administrator of the account for assistance.

FIGURE 2: Oracle Cloud Sign-in

Limits, quotas, and usage

Along with using proper permissions, appropriate *Limits, Quotas, and Usage* settings for the Compartment where the Oracle VMware Solution will reside must be configured. The settings cannot be so restrictive that the ESXi host required for vSphere provisioning becomes unavailable as one example.

There are "Service Limits and Usage" settings controlled by Oracle and "Compartment Quotas" set by the Oracle Administrator; both must be configured appropriately to provision resources. Please contact *Oracle Support* for more specific usage limits in accordance with your Oracle agreement.

In the environment shown in Figure 3, a limit on how many SDDCs and ESXi host that can be provisioned has been set.

FIGURE 3. Limits, quotas and usage

SSH keys

Oracle recommends using SSH keys for SSH access instead of passwords. When deploying a Linux Bastion Host instance, the wizard will ask for a public SSH key rather than a root password. For more information, visit *How to Generate SSH Keys*.

Deploying Oracle Cloud Infrastructure

IP address space is a prerequisite to deploying Oracle Cloud Infrastructure. Oracle refers to the overarching IP space, which will be broken up into smaller subnets, as a *Virtual Cloud Network*. Defining a **Virtual Cloud Network** in the Oracle Cloud is equivalent to determining an on-premises data center's IP space. Be mindful not to select an IP address space that will conflict with existing networks in the on-premises or cloud environments. The various subnets provisioned in the Oracle Cloud for the Oracle Cloud Infrastructure will draw from this IP space.

When a Virtual Cloud Network is created, a **Default Security List** and a **Default Route Table** are also produced.

- A Security List is a virtual firewall that accepts or denies traffic. By default, the Default Security List allows the following traffic and blocks everything else:
  - Ingress – TCP Port 22 (used for SSH) and ICMP
  - Egress – All traffic
- The Default Route Table is created without any rules.

There are two types of subnets: **public subnets** and **private subnets**. A public subnet is the entry point from the Internet or outside the Oracle Cloud Infrastructure utilizing a **Bastion Host** (more details will be discussed later).

Public subnets can use an **internet gateway** as an optional virtual router to enable both ingress (incoming) and egress (outgoing) connectivity to the Internet. During the provisioning of the public subnet, the default routing table will point to an internet gateway.

Using the **Start VCN Wizard i**s the easiest way to deploy the Virtual Cloud Network and other components to support the Oracle Cloud VMware Solution.

Creating a Virtual Cloud Network

1. Log in to the **Oracle Cloud Dashboard**
2. Select the correct region to deploy the **Oracle Cloud VMware Solution**
3. Click on the **burger** icon at the top left of the screen to display the Menu
4. Select **Network > Virtual Cloud Networks**
   a. Click **Start VCN Wizard.** This selection will open the Create a Virtual Cloud Network wizard
   b. Select **VCN with Internet Connectivity**
   c. Click Start VCN Wizard
   d. Enter a **Name** (e.g., McoE-OCVS-USW01-VCN)
   e. Select the **Compartment**
   f. Enter the **VCN CIDR block** (e.g., 10.200.0.0/16 providing 65534 available IP addresses)
   g. Enter the CIDR block that will be used for the **public subnet** (e.g., 10.200.0.0/24)
   h. Enter the CIDR block that will be used for the **private subnet** (e.g., 10.200.1.0/24)
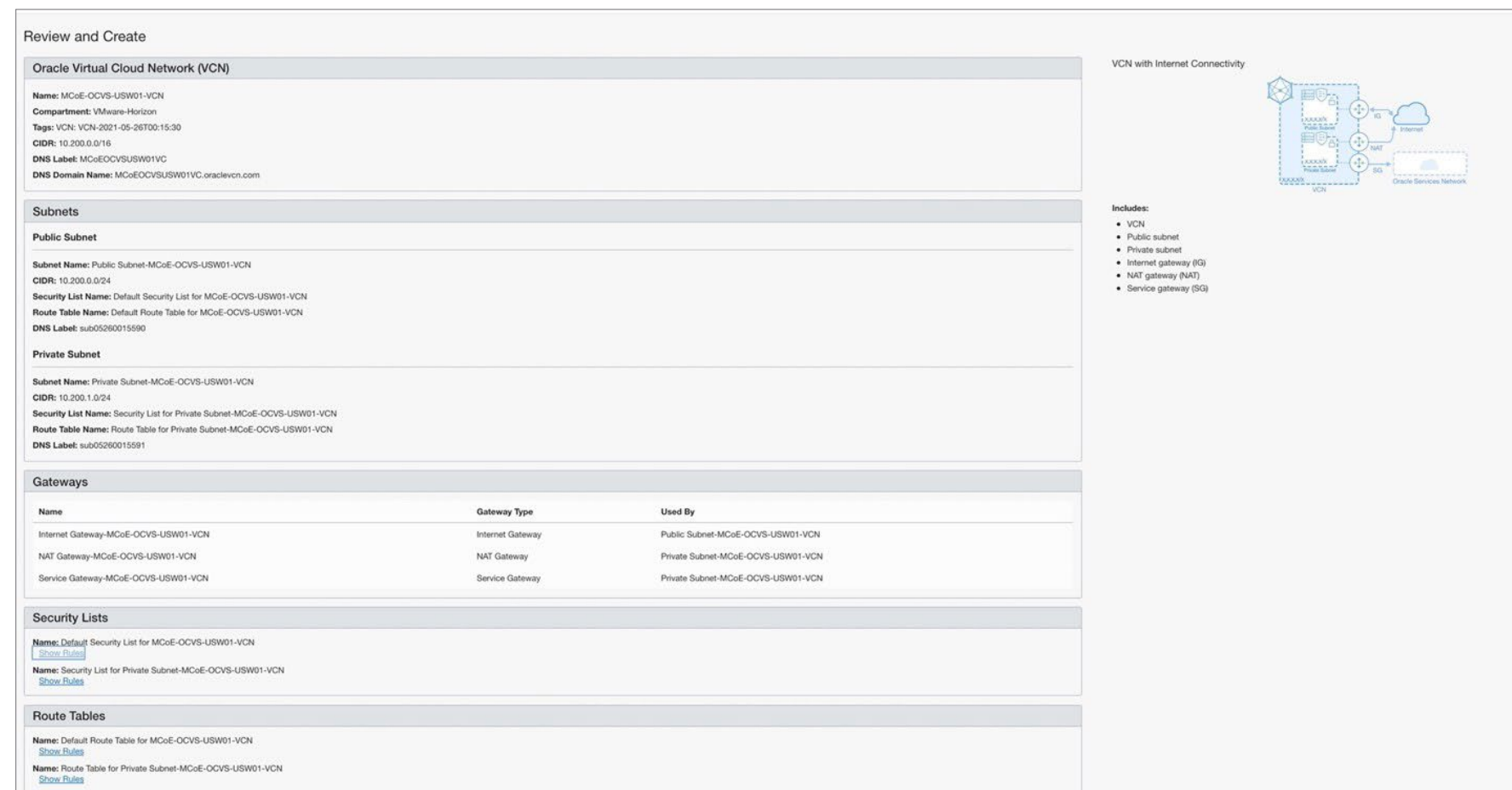   i. Click **Next**

FIGURE 4. Creating a Virtual Cloud Network

Deploying a Bastion Host

When deploying in the Oracle Cloud, there needs to be a way to access instances and environments that do not have access to the Internet. What is needed is a **Bastion Host**, sometimes referred to as a Jumpbox. A Bastion Host is used to bridge connectivity between environment(s) where an end-user does not have direct network access. A Bastion Host has one virtual interface (vnic) deployed in a subnet classified as a public subnet. The vnic is assigned a private IP address. Still, because the subnet is classified as public, the same vnic can also be given a public IP address through the Oracle GUI, creating a bridge between the Internet and the private subnets in the Oracle Cloud.

Windows or Linux Bastion Host are available. A Windows server with Remote Desktop Protocol (RDP) works well too, but the steps below provide the deployment process of a Linux virtual machine (preferred method), which can then be used to provide an **SSH Tunnel** or install **Apache Guacamole**.

Required – Deployment of a Windows Bastion Host requires adding the Remote Desktop Protocol to the security list of the public subnet where the Bastion Host resides.

Deploy a Linux Bastion Host

1. Log in to the **Oracle Cloud Dashboard**
2. Select the correct **region** to deploy the **Oracle Cloud VMware Solution**
3. Click on the **burger** icon at the top left of the screen to display the Menu
4. Select **Compute > Instances**
   a. Click **Create Instance**
   b. **Name** the instance (e.g., MCoE-BST-LNX-01)
   c. Make sure the correct **Compartment** is selected
   d. Select the **Availability Domain** where the instance will be deployed
   e. Select **Change Image** and select the image to deploy
   f. Select **Change Shape** and select the shape to deploy
   g. Select the **Virtual Cloud Network** from the dropdown
   h. Select the **Public Subnet** from the dropdown
   i. Select **Paste Public Key** and paste in the Public Key
   j. Click **Create** to complete the instance configuration

Once the instance has been provisioned, the instance configuration information will be available. Make a note of the **Username and Public IP address** to connect to the Bastion Host (Figure 5).

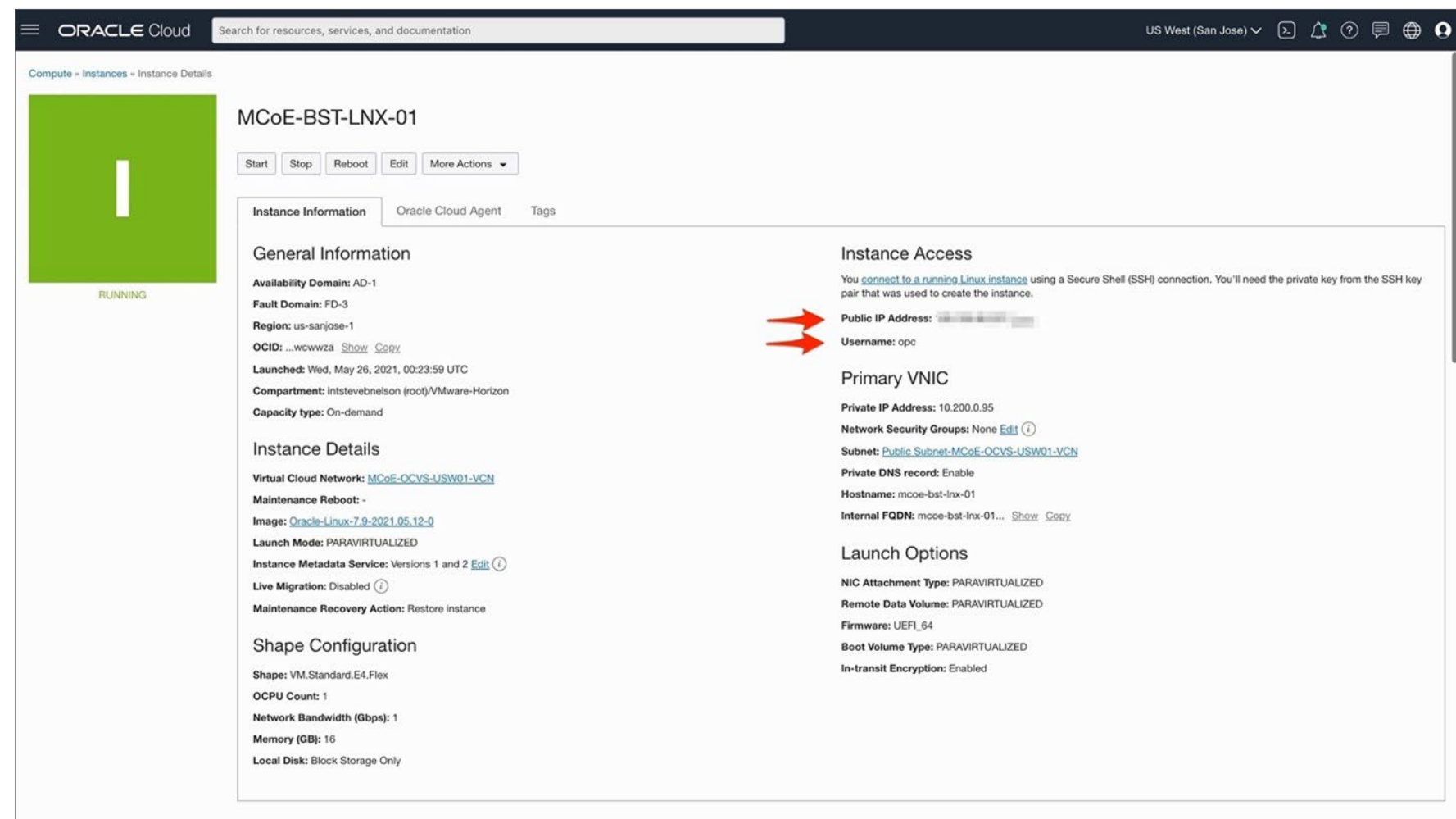FIGURE 5. Deploying a Linux Bastion Host

5. Open an **SSH client** of choice. For illustration purposes, please use:
   o ssh -i <path to privatekey.ppk> <username>@<public IP address>
   Example: ssh -i "C:\Users\Simon\My Documents\tshirts-jump-01-private-key.ppk opc@150.136.x.x

Deploying VMware Software-Defined Datacenter with HCX

With the **Oracle Cloud Infrastructure** prerequisites completed, deploying a VMware Software-Defined Data Center (SDDC) in the Oracle Cloud is next. The Oracle Cloud VMware Solution deployment process is straightforward, but there is one prerequisite that needs to be addressed.

- **SSH Keys:** During the deployment of the Bastion Host, a set of keys (public and private) to access the Bastion Host via SSH was required. The same approach is used to access the ESXi hosts in the SDDC. Instead of providing a root password, a public key will need to be provided.

Deploy an Oracle Cloud VMware Solution instance

1. Log in to the **Oracle Cloud Dashboard**

2. Select the correct **region** to deploy the Oracle Cloud VMware Solution (This should be the same region where the **Bastion Host** resides)

3. Click on the **burger icon** at the top left of the screen to display the Menu

4. Select **Hybrid > VMware Solution**

5. Click **Create SDDC**

   a. **Name** the SDDC (e.g., MCoE-OCVS-USW01)

   b. Select the correct **Compartment**

   c. Uncheck the box next to **VMware HCX i**f it is not to be deployed as part of the Oracle Cloud VMware Solution

   d. Select the **VMware software version** to be deployed. The current options are vSphere v6.5 U3, v6.7 U3, or 7.0 update 2

   e. Select the **Pricing Interval Commitment** of Hourly, Monthly, One year or Three year

   f. Select the **Number of ESXi Hosts** to deploy in the software-defined datacenter (Additional ESXi Hosts can be added after the deployment)

   g. Enter a **Prefix** for the ESXi hosts. (ESXi hosts get named beginning with the <prefix> and incremented by -1,-2, -3,etc.)

   h. Upload or Paste in the **public key**

   i. Select the **Availability Domain** from the dropdown (Make sure to deploy the software-defined datacenter on the same Availability Domain as the Bastion Host)

   j. Click **Next**

   k. Select the **Virtual Cloud Network** to be used from the dropdown

   l. If VMware HCX is to be deployed, name the **NAT Gateway** (The NAT Gateway is required by HCX for license activation, updates, and VMware enhanced support)

   m. Select the correct **Compartment** from the dropdown

   n. Ensure **Create New Subnets** and **VLANs** is selected (All of the Networking required to support the SDDC will be automatically created and configured)

   o. Enter a **software-defined datacenter CIDR** (e.g., 10.230.8.0/21, this CIDR block will be carved up into smaller subnets, each used for different parts of the deployment)

   p. Click **Check Availability** to make sure the CIDR entered can be used

   q. Enter a **software-defined datacenter Workload CIDR** (e.g.192.168.1.0/24, which will be used for workload virtual machines)

   r. Click **Next**

   s. **Review** and amend if needed
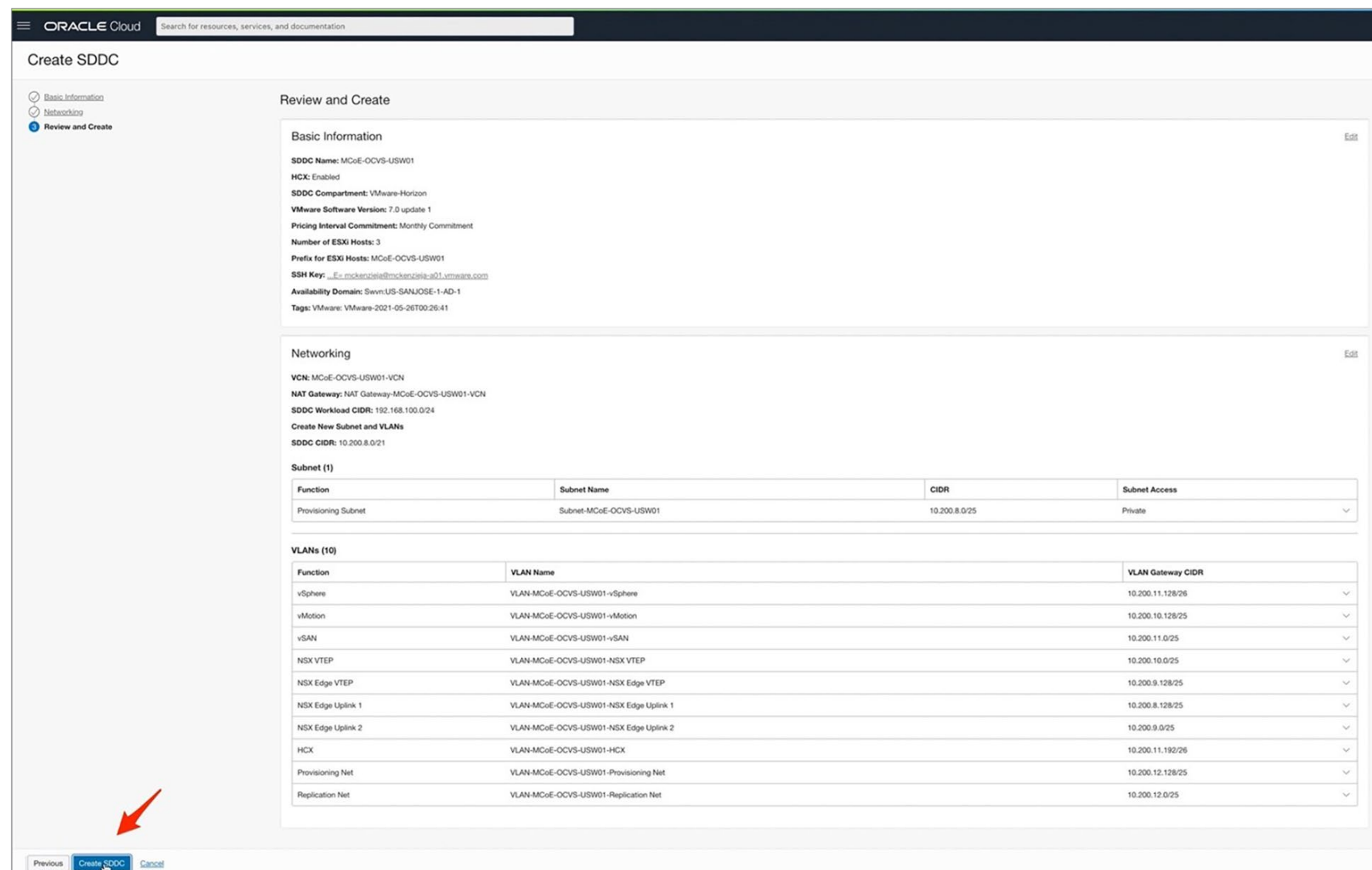
   t. Click **Create SDDC**

FIGURE 6. Deploying an Oracle Cloud VMware Solution Instance

The Oracle Cloud VMware Solution build process will now begin. During this time, the provisioning process can be observed via the Oracle Cloud console.

Once the Oracle Cloud VMware Solution deployment is complete, it's time to take inventory of what was deployed.

Deployment overview

After deploying an Oracle Cloud VMware Solution instance, validating that everything is deployed correctly and accessible should be prioritized. This section will review the software-defined datacenter's deployed components and make sure vCenter, HCX Manager, and NSX-T Manager are healthy and accessible.

The following steps describe how to:

• Locate login information for the deployed Oracle Cloud VMware Solution components.

• Validate access to the vCenter Server, HCX Manager, and NSX-T Manager.

• Identify where Oracle Cloud VMware Solutions cloud infrastructure components are deployed.

Find Oracle Cloud VMware Solution information page

1. Log in to the **Oracle Cloud Dashboard**
2. Select the correct **region** where the Oracle Cloud VMware Solution is deployed.
3. Click on the **burger** icon at the top left of the screen to display the Menu
4. Select **Hybrid > VMware Solution**
   a. Select the **name** of the SDDC

FIGURE 7. The SDDC details screen presents you with the Oracle Cloud VMware Solution information, including all the essential URLs, IP Addresses, Usernames, and passwords needed to access and manage an environment.

View ESXi hosts

Scroll down to the ESXi Hosts section of the screen (bottom of the page) to see the ESXi Hosts that have been deployed. This Menu is also where additional ESXi Hosts can be added to the software-defined datacenter if required. Supplementary information about the ESXi Hosts can be found when viewing Compute Instances.

1. Click on the **burger** icon at the top left of the screen to display the Menu

2. Scroll down on the left-hand side menu and select **Compute > Instances**

When viewing Compute Instances, both ESXi Hosts deployed as a part of the software-defined datacenter and any available Bastion Host are listed in one place. Additionally, the Oracle VMware Cloud Solution service is wholly integrated within Oracle Cloud, making management easier due to having a single screen to view everything.

HELPFUL NOTES

- Virtual Machines running in vSphere are not visible in this view.

- The **Fault Domain** column shows that each ESXi host is in a different Fault Domain within an **Availability Domain**. Oracle will spread the ESXi hosts between multiple Fault Domains so that the instances are not on the same physical hardware within a single Availability Domain.

FIGURE 8. Instances in VMware-Horizon compartment

Availability domains

Each Oracle Cloud Region has at least one Availability Domain. An Availability Domain is a physical data center within a geographical region. Availability Domains within the same region are connected by a low latency, high bandwidth network. Each Availability Domain contains three Fault Domains. A Fault Domain is a grouping of hardware and infrastructure. Fault Domains provide anti-affinity, allowing the distribution of instances across Fault domains so that the instances are not on the same physical hardware within a single Availability Domain.

Figure 9 illustrates an Oracle Cloud VMware Solution deployment within the US East (Ashburn) Oracle Cloud Region. Here we are only using AD-1, and the ESXi Hosts are distributed across all three Fault Domains.
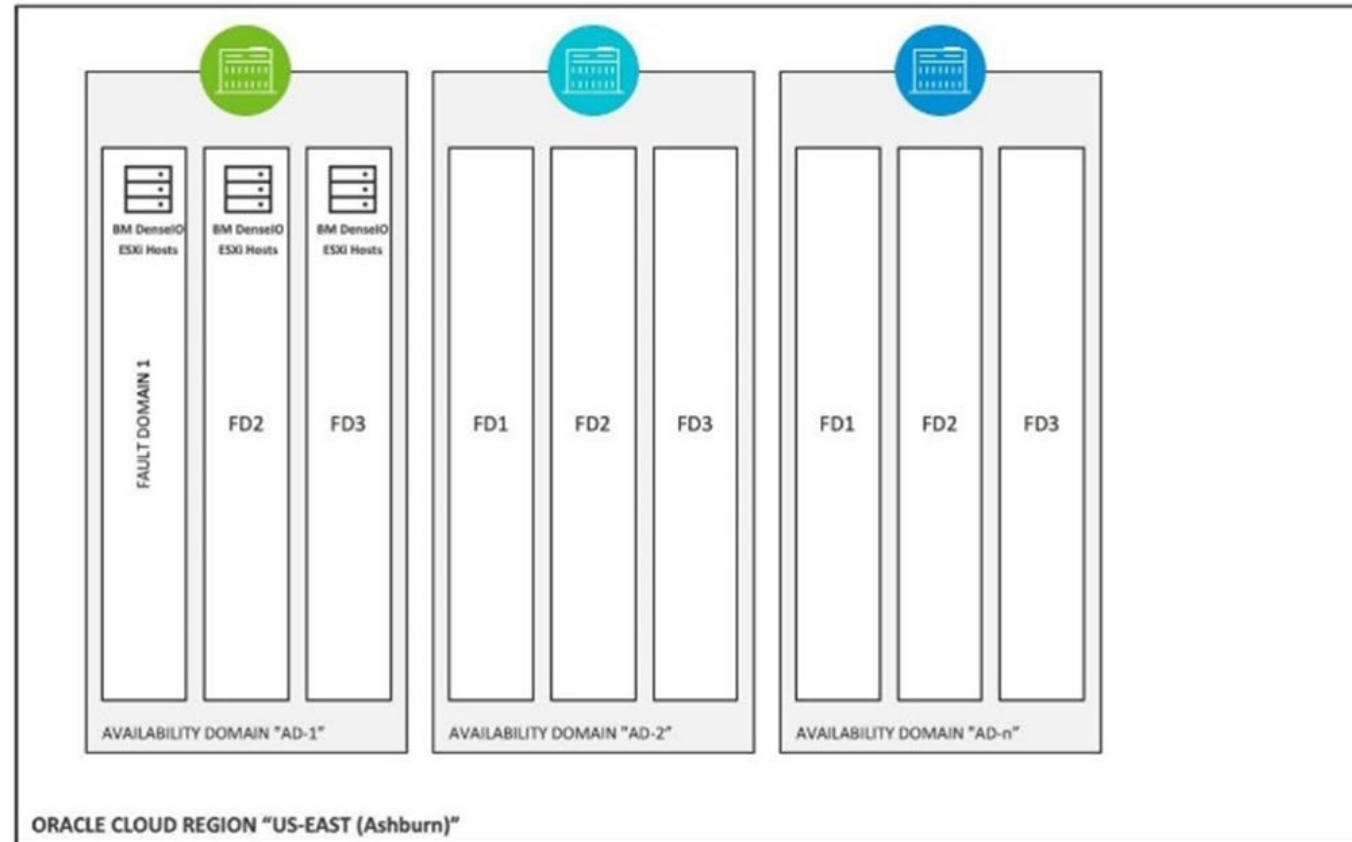
FIGURE 9. Example of Availability Domains on Oracle Cloud VMware Solution deployment

Accessing management components

When a Oracle Cloud VMware Solution instance is fully deployed, ensuring access to the vCenter Server, NSX-T, and HCX should be a priority.

Test vCenter access

Access to the vCenter Server, which provides the management plane for the deployed ESXi host, will be reviewed first.

1. Click on the burger icon at the top left of the screen to display the Menu

2. Select **Hybrid** > **VMware Solution**

   a. Select the **name** of the software-defined datacenter

   b. In the Software-Defined Datacenter Information section, copy the **vSphere Client URL**

   c. Open a **browser window,** either on the **Bastion Host** or on a machine that has access to the Bastion Host via an **SSL Tunnel**

   d. Paste the vSphere Client URL into a new browser tab

   e. Copy/Paste the **vCenter Initial Username** and **vCenter Initial password** to log in to vCenter

HELPFUL NOTES

Log in with the Administrator account. After deploying the environment, Oracle removes its access and gives the customer **FULL ACCESS** to the whole vSphere environment. This access is entirely private, as Oracle has **ZERO ACCESS** to software-defined datacenter after the initial deployment.
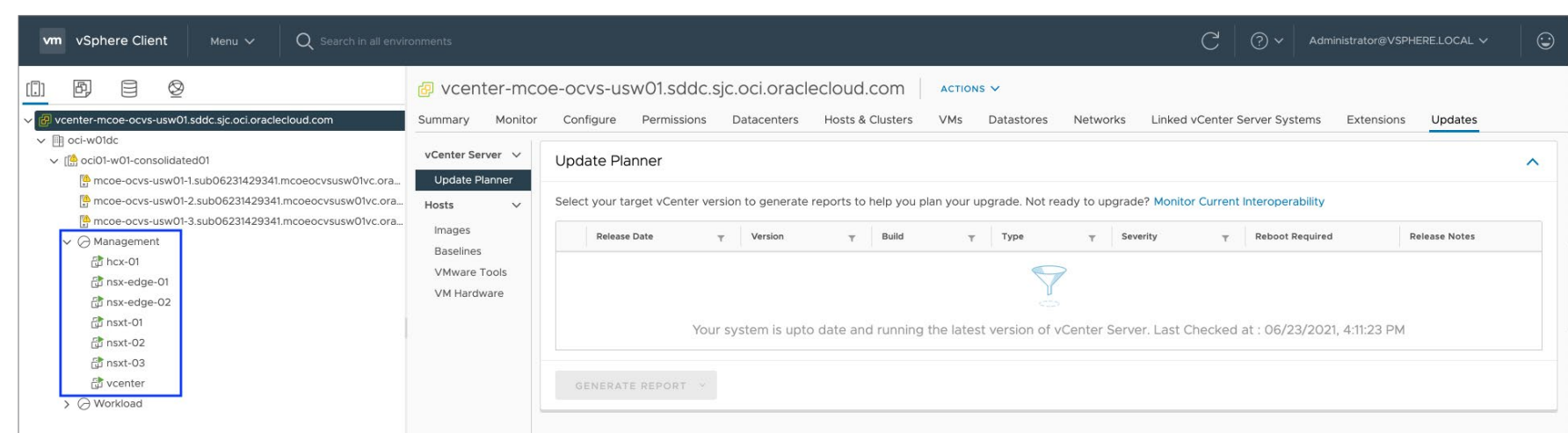
FIGURE 10. VMware HCX, NSX-Edge Nodes, VMware-NSX-T nodes, and vCenter Server

In the vCenter, the ESXi Hosts and virtual machines are available. The virtual machines that are deployed include the following:

- vcenter = vCenter Appliance
- hcx-01 = HCX Management Appliance
- NSX-T-01,02,03 = NSX-T Manager Appliances (Three are deployed for high availability)
- nsx-edge-01,02 = NSX-T Edge Appliances (Two are deployed for high availability)

View vSAN datastore

The Oracle Cloud VMware Solution host utilizes vSAN storage. The vSAN Database will show how much storage is available for workloads.

1. Click **Menu** in the vSphere client and select **storage** from the dropdown menu
   a. Click **Monitor**
   b. Expand the vCenter> datacenter exposing the **vsanDatastore**
   c. Click **VSAN > Capacity**
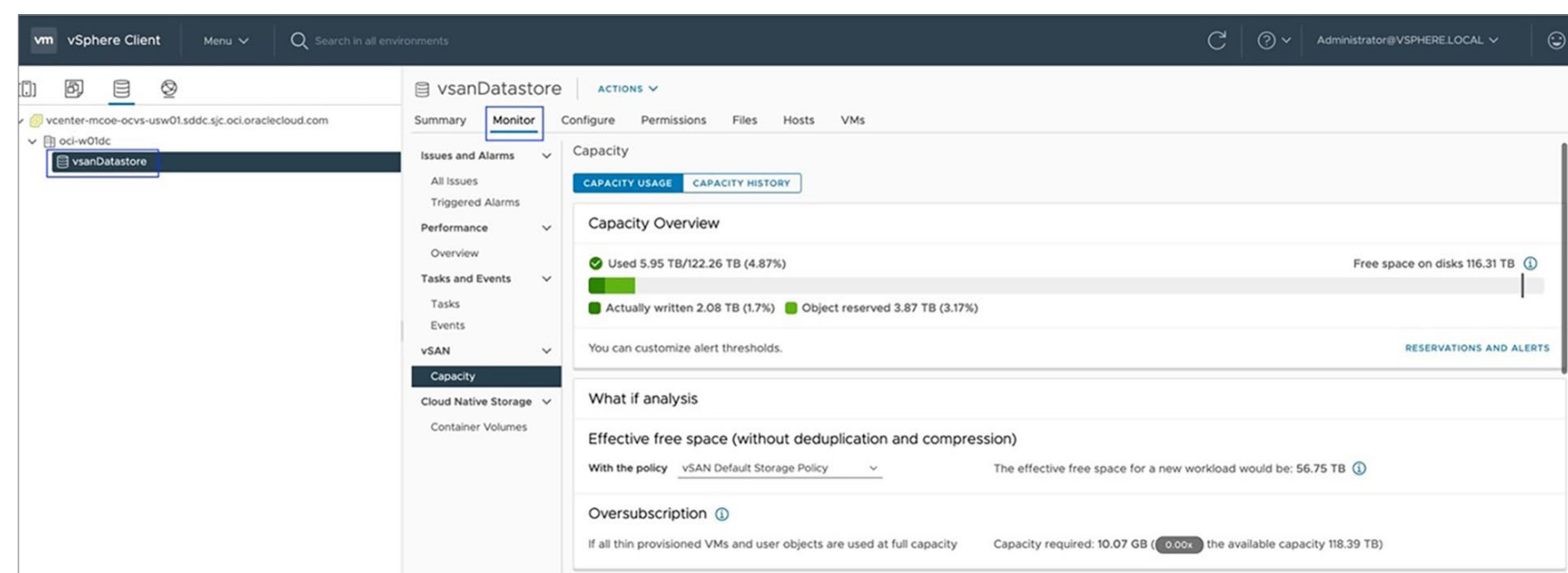
FIGURE 11. The screenshot displays the vSAN Datastore information that is deployed as part of the SDDC environment. The size of the vSAN Datastore may vary in the future as Oracle introduces additional physical server shapes.

Test VMware HCX access

The Oracle Cloud VMware Solution deployment includes VMware HCX unless it was decided not to be deployed during the deployment process. VMware HCX can be used to migrate workloads from or to Oracle Cloud VMware Solution.

1. Click Menu in the vSphere client and select **HCX** from the dropdown menu (Figure 12). VMware HCX is deployed, integrated into vCenter, and ready for Site Pairing.
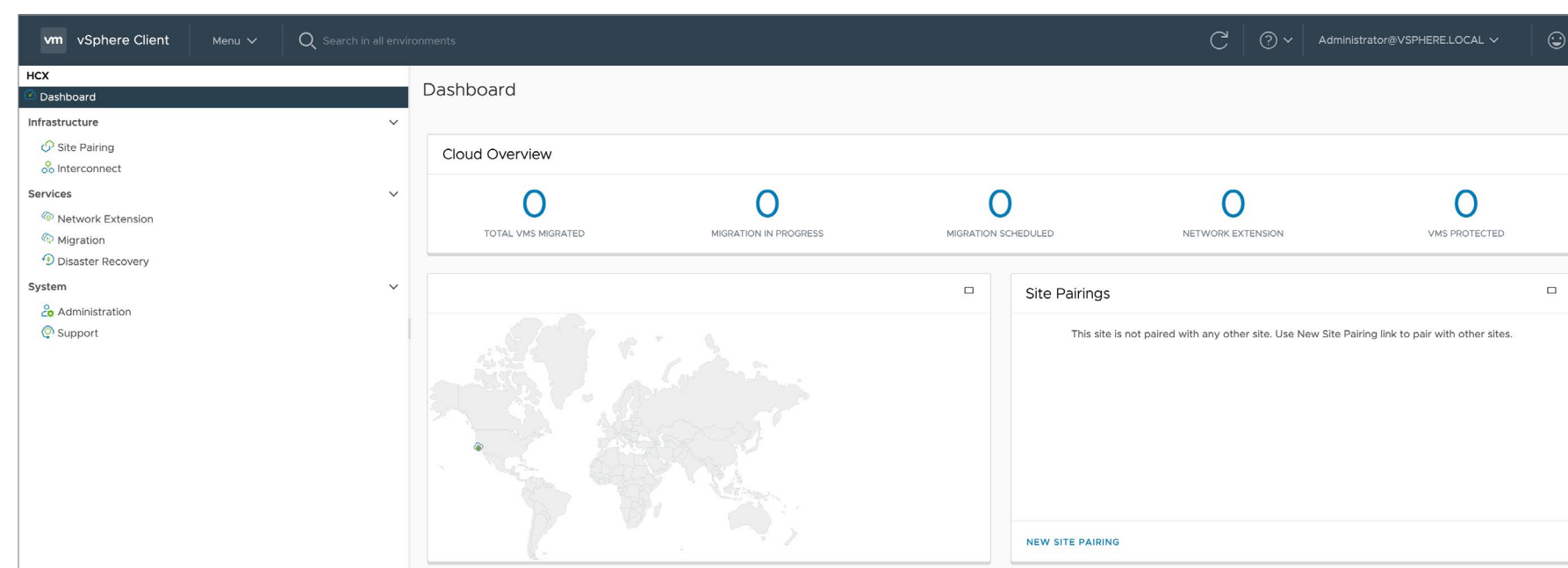
FIGURE 12. VMware HCX access

Test VMware NSX-T access

NSX-T is the core of the software-defined datacenter for software-defined networking. To log in, complete the following:

1. In the **Oracle Cloud Console,** click on the burger icon at the top left of the screen to display the menu

2. Select **Hybrid > VMware Solution**

    a. Select the name of the deployed software-defined datacenter

    b. In the Software-Defined Datacenter Information section, copy the **NSX Manager URL**

    c. Open a browser window either on the Bastion Host or on a machine that has access to the Bastion Host via an SSL Tunnel

    d. Paste the **NSX Manager URL** into a new browser tab

    e. Copy/Paste the **NSX Manager Initial Username** and **NSX Manager password** to log in to NSX-T Manager
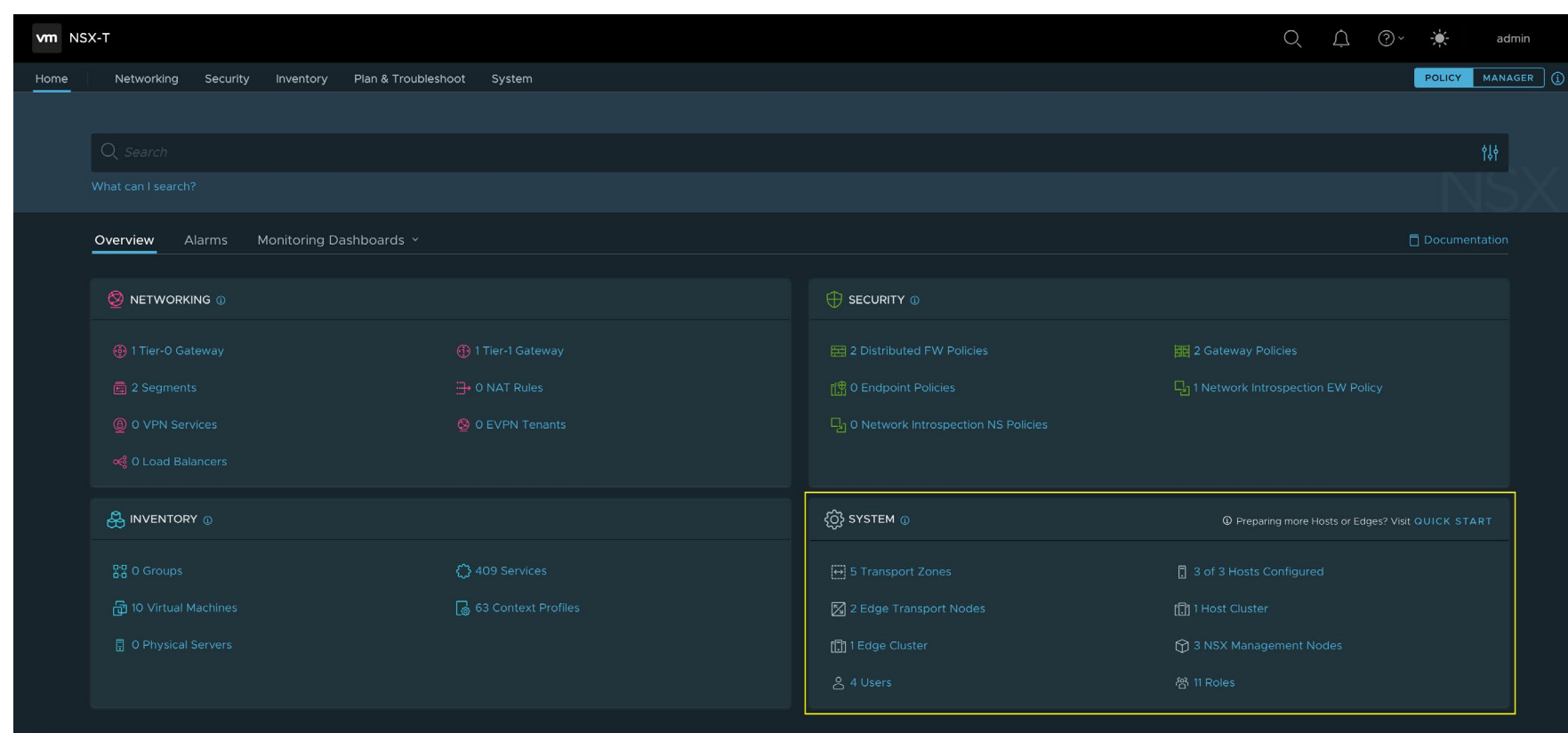
FIGURE 13. VMware NSX-T access

At the bottom right of the Overview page, there is a section titled System. Listed here are the NSX-T components that are automatically deployed:

• 3 x NSX-T Manager Nodes (VMs nsxt-01,02,03)

• 2 x NSX-T Edge Transport Nodes (VMs nsx-edge-01,02)

• 3 x VMware ESXi Hosts have been enabled as Transport Nodes

For additional information on NSX-T, visit the *VMware NSX-T Data Center Documentation*.

Oracle Cloud Infrastructure (OCI) and Oracle Cloud VMware Solution Networking

This chapter will review the overall networking configuration that supports deploying a VMware software-defined datacenter, including NSX-T. The deployment of infrastructure in the Oracle Cloud is simple. However, understanding how the logical and physical devices communicate with each other can be challenging without a deep knowledge of the Network.

The following steps describe how to:

• Understand where to find the VLANs and subnet that are provisioned as part of an Oracle Cloud VMware Solution

• Get a brief overview of network security

Configuration review

Address space

The address space allocated for a VMware software-defined datacenter consist of a contiguous range of IPv4 addresses that do not overlap with other address space in the Virtual Cloud Network. A different CIDR block would have to be specified if a second software-defined datacenter using the same Virtual Cloud Network is deployed. If another software-defined datacenter uses the same CIDR block, an error will occur.

FIGURE 14. Overlap address space

ESXi host VMware Software Defined-Networking connectivity

The following steps show how to view how ESXi Hosts are connected to the Oracle Cloud infrastructure.

1. Log in to the **Oracle Cloud Dashboard**

2. Select the correct region that the **Oracle Cloud VMware Solution** is deployed.

3. Click on the burger icon at the top left of the screen to display the Menu

4. Select **Compute>Instance**

   a. Select one of the **ESXi Hosts**

   b. Scroll down to Select **Attached VNICs** on the Resources menu (Located on the left-hand side of the page)

Figure 15 illustrates ESXi Host connectivity to the various VLANs deployed as part of a software-defined datacenter configuration. All VLANs are trunked to both physical NICs available on the bare-metal host.

FIGURE 15. Virtual network interfaces and VLANs attached to the ESXi Host

VLANs

A VLAN is an object within a Virtual Cloud Network. VLANs are used to partition the Virtual Cloud Networks into Layer 2 broadcast domains. Each VLAN has a Route-Table associated with it. The Route-Table is responsible for the traffic forwarding to a specific destination. In addition to the Route-Table, each VLAN has a Network Security Group or Security Rules (firewall rules) associated with it. These Network Security Groups function in the same way as a firewall, allowing and denying traffic in and out of the VLAN.

HELPFUL NOTES

When manually creating a new VLAN or subnet, all traffic is denied by default. Rules will need to be added to allow traffic.

Each VLAN within the Virtual Cloud Network is automatically assigned a VLAN ID. These VLAN IDs are local to the Virtual Cloud Network, so there might be cases where the same VLAN ID is used in an SDDC in another Availability Domain or Region. Even though they might share the same VLAN ID, it's essential to understand that they are not the same VLAN.

VLAN-<SDDC NAME>-NSX Edge Uplink 1	This VLAN is used for communication between the VMware software-defined datacenter and Oracle Cloud Infrastructure.
VLAN-<SDDC NAME>-NSX Edge Uplink 2	This VLAN is used for communication between the VMware software-defined datacenter and Oracle Cloud Infrastructure.
VLAN-<SDDC NAME>-NSX Edge VTEP	This VLAN is used for data-plane traffic between the ESXi host and NSX Edge.
VLAN-<SDDC NAME>-NSX VTEP	This VLAN is used for data-plane traffic between ESXi hosts.
VLAN-<SDDC NAME>-vMotion	This VLAN is used for vMotion (VMware migration tool) management and workload.
VLAN-<SDDC NAME>-vSAN	This VLAN is used for vSAN (VMware storage) data traffic.
VLAN-<SDDC NAME>-vSphere	This VLAN is used to manage the software-defined datacenter components (ESXi, vCenter, NSX-T, and NSX Edge).
VLAN-<SDDC NAME>-HCX	This VLAN is used for HCX traffic.
VLAN-<SDDC NAME>-Replication Net	This VLAN is used for the management of the vSphere Replication component.
VLAN-<SDDC NAME>-Provisioning Net	This VLAN is used for Provisioning activities

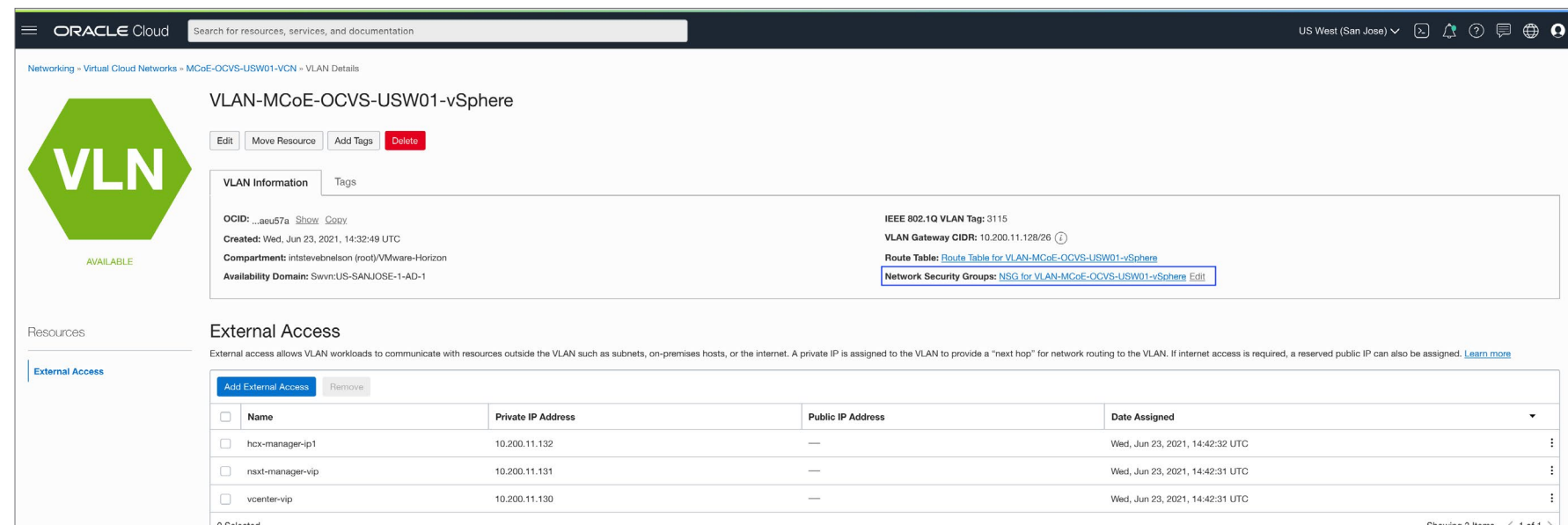TABLE 2. VLANs connected to each ESXi Host

FIGURE 16. VLAN details

To take a closer look at the vSphere VLAN:

1. Click **VLAN-<SDDC NAME>-vSphere** in the attached VNICs section under Subnet or VLAN (Figure 16).

Here we can see some additional information about the VLAN (Figure 17). By default, the vSphere VLAN has **External Access** configured for:

- The vCenter (vcenter-vip)

- The NSX-T Management Cluster Virtual IP (nsxt-manager-vip)
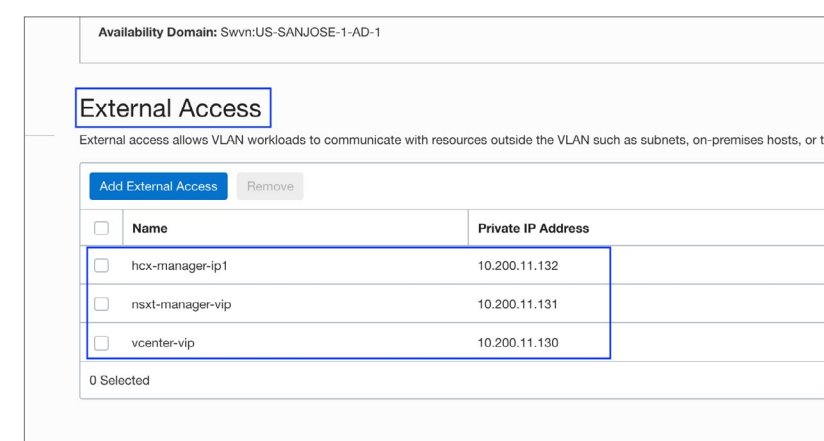
- The HCX Manager (hcx-manager-ip1)

FIGURE 17. VLAN External Access configuration

The external access type for all these components is **Route Target Only**. This setting assigns an IP address that can be used as a route target on the VLAN so that other Oracle Cloud Infrastructure VLANs can access these IP addresses. In addition to the External Access information, the **Route Table** and **Network Security Group (Firewall)** associated with the VLAN can be found here.

2. Click **Route Table tor <SDDC NAME>-vSphere** (Figure 18).

The Route table for the vSphere VLAN specifies the NAT Gateway as the default gateway for all traffic on this VLAN. This setting allows the virtual machines on this VLAN to access the Internet if permitted in the Security Rules.

The Route table for the vSphere VLAN specifies the NAT Gateway as the default gateway for all traffic on this VLAN (Figure 19). This setting allows the virtual machines on this VLAN to access the Internet if permitted in the Security Rules.

FIGURE 18. VLAN Route Table
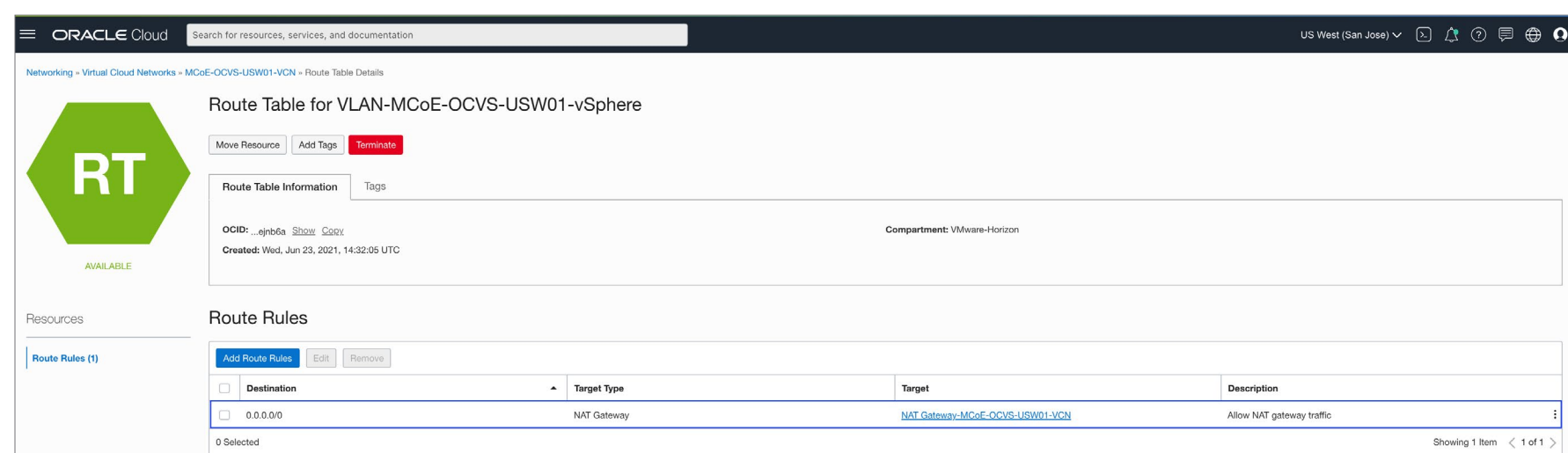
FIGURE 19. VLAN Route Table configuration

3. Return to the previous window and click **NSG For
<SDDC NAME>-vSphere** (Figure 20).

Security Rules are added to the **Network Security
Group (Firewall)**, as shown in Figure 21. Security rules
are automatically configured to allow components of
the software-defined datacenter and VMware HCX to
communicate with each other and access the Internet.
The screenshot only shows a few of the many rules that
are added to the Network Security Group. Also, each
individual rule can be clicked and explored to gain a
deeper understanding of what traffic flows are
occurring.
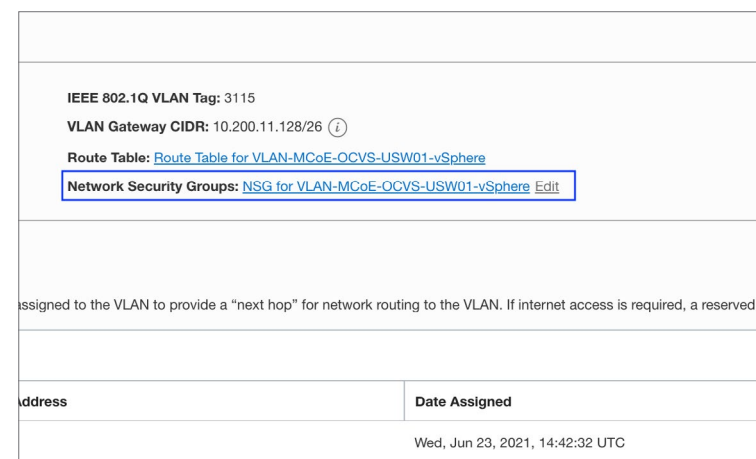
FIGURE 20. VLAN Network Security Groups
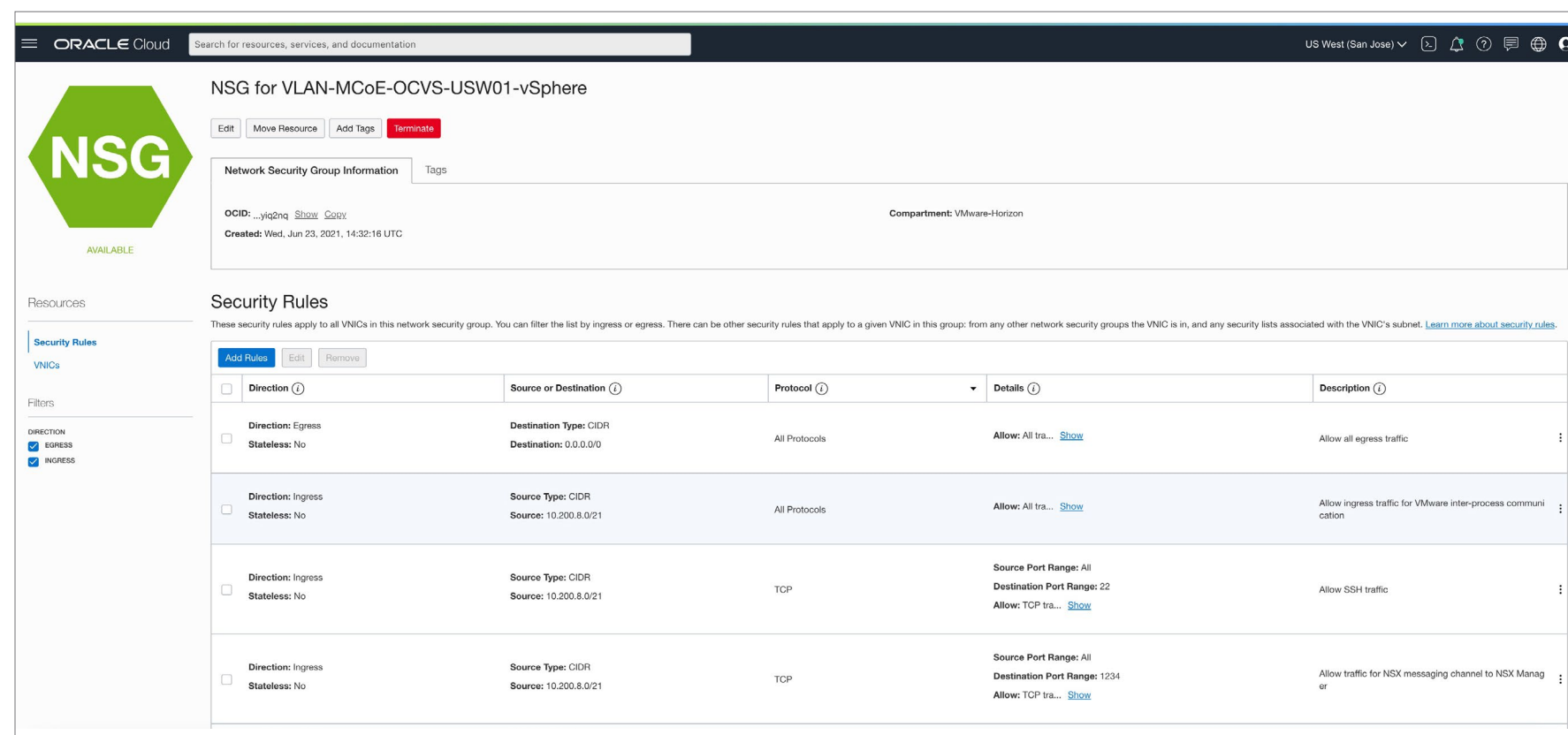
FIGURE 21. VLAN Network Security Group Information

Virtual port groups

Another way of viewing the ESXi Host connectivity is from a vSphere Client. So far, ESXi Host
connectivity has been explored within the Oracle Cloud interface. It might help clarify things by
looking at it from the vSphere Client

To view the virtual networking configuration inside the vSphere client:

1. In the Oracle Cloud Interface, click on the burger icon at the top left of the screen to display the
Menu

  a. Select **Hybrid > VMware Solution**

  b. Select the name of your newly deployed **software-defined datacenter**

  c. Copy the **vSphere Client URL**

  d. Open a **browser window** either on the Bastion Host or on a machine that has access to the
Bastion Host via an SSL Tunnel

  e. Paste the **vSphere Client URL** into a new browser tab

  f. Copy/Paste the **vCenter Initial Username** and **vCenter Initial password** to log in to vCenter

Once you are logged into vCenter:

1. Click **Menu** in the vSphere client

2. Select **Networking** on the dropdown menu

  a. Expand the tree on in the left pane until the "DSwitch" is visible (Figure 22)
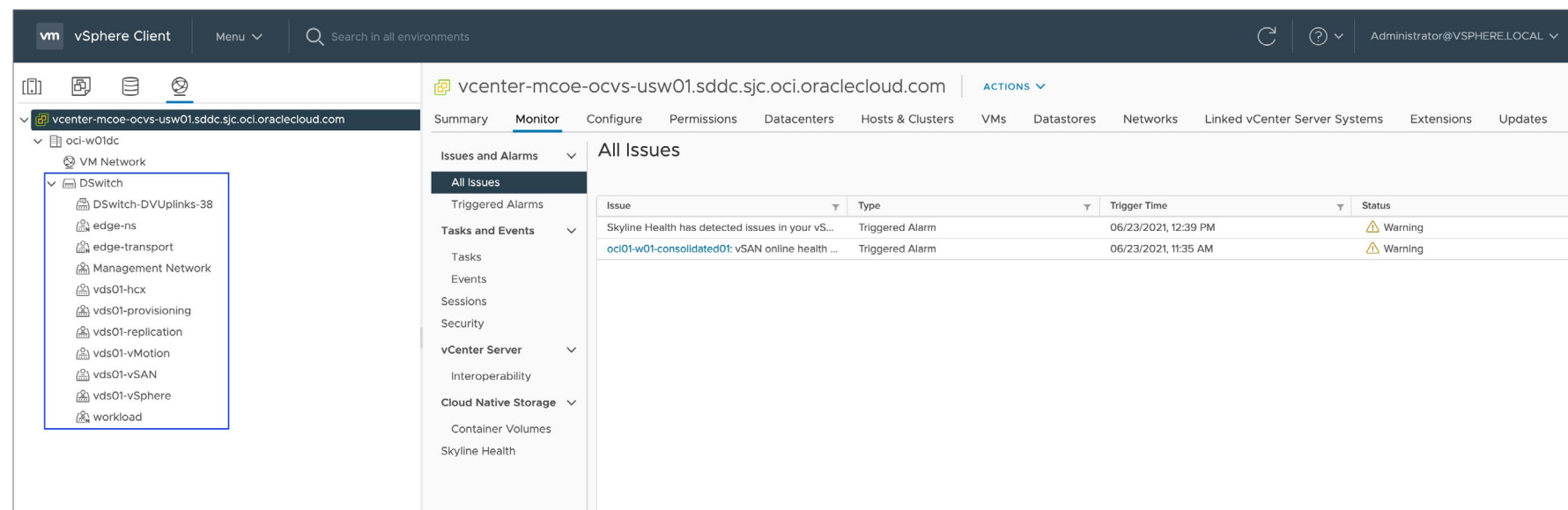
FIGURE 22. Distributed Virtual Switch (vDS) port-groups

Visible in the Figure 22 is the virtual distributed switch (vDS) port-groups. You should notice that these port groups names are similar to our software-defined datacenter VLANs reviewed earlier.

edge-ns	NSX Edge Uplink 1 VLAN
edge-transport	NSX Transport
Management network	ESXi Management VLAN(ESXi Host vmk0 lives here)
vds01-HCX	HCX VLAN
vds01-provisioning	(ESXi Host vmk4 lives here)
vds01-replication	(ESXi Host vmk3 lives here)
vds01-vMotion	vMotion VLAN (ESXi Host vmk1 lives here)
vds01-vSAN	vSAN VLAN (ESXi Host vmk2 lives here)
vds01-vSphere	ESXi management (ESXi vmk0 lives here)
workload	The NSX-T segment for our virtual machines that we specified during the configuration of the software-defined datacenter

TABLE 3. Virtual Distributed Switch (vDS) port groups

ESXi Host connectivity

1. Click Menu in the vSphere client and select **Hosts and Clusters** on the dropdown menu
2. Select a hostname **<hostprefix>-1**
   a. Select the **Configure** tab
   b. Select **Physical adapters**
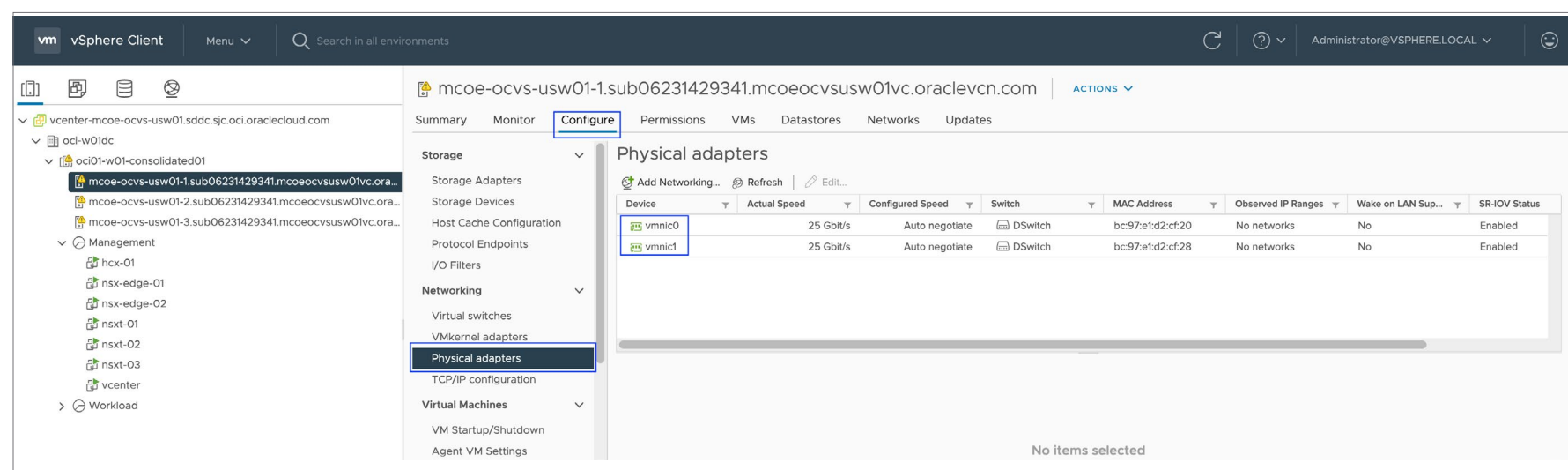
FIGURE 23. Physical adapters

The current hardware configuration of the physical ESXi hosts (BM.DenseIO2.52) used for the Oracle Cloud VMware Solution software-defined datacenter has 2 x 25Gbit/s physical network cards.

vmnic0	Assigned to the Distributed Virtual Switch (DSwitch)
vmnic1	Assigned to the Distributed Virtual Switch (DSwitch)

TABLE 4. Physical adapters configuration

View VMkernel adapters

1. Select **VMkernel adapters**
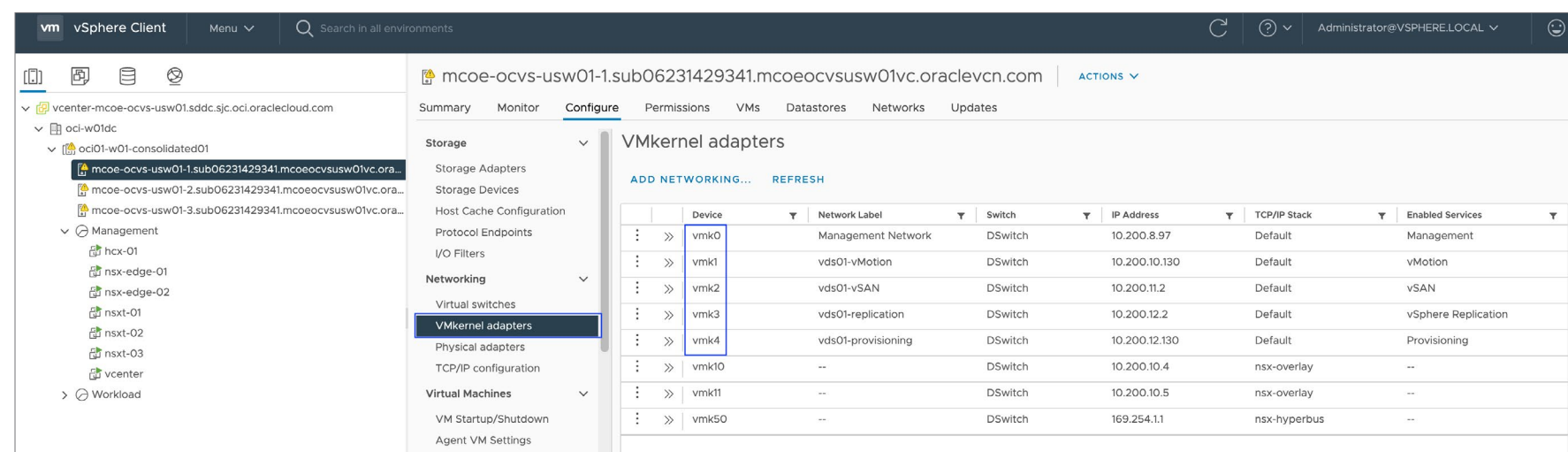
FIGURE 24. VMkernel adapters

There are five VMkernel adapters configured by default when deploying a VMware software-defined datacenter with HCX.

vmk0	Added to the Management Network vDS and configured to be used for ESXi management traffic
vmk1	Added to the vds01-vMotion vDS and configured to be used for ESXi vMotion traffic
vmk2	Added to the vds01-vSAN vDS and configured to be used for ESXi vSAN traffic
vmk3	Added to the vds01-replication and configured to be used for HCX
vmk4	Added to the vds01-provisioning and configured to be used VM provisioning

TABLE 5. VMkernel adapters

View virtual switches

2. Select **Virtual switches**

3. Click the down arrow next to **Distributed Switch: DSwitch** to display all Virtual Switches. There are two virtual switches configured on the ESXi Host identified earlier.

    a. Distributed Switch: DSwitch

    b. Standard Switch: vSwitch0 (unused)
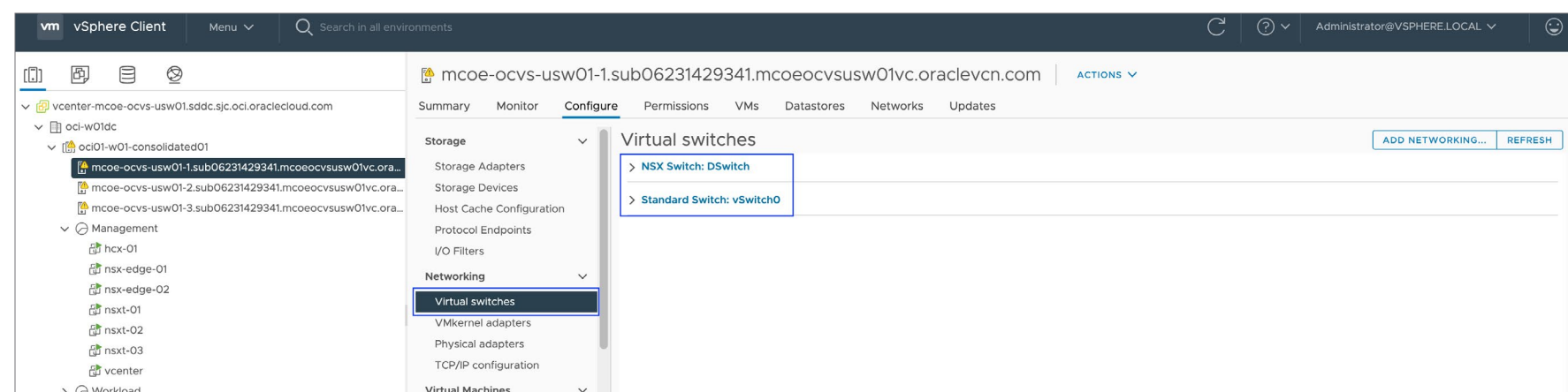
FIGURE 25. Virtual switches

3. Click the **chevron icon (>)** next to Distributed Switch: DSwitch to expand the switch. The port-groups are configured within the vDS and the uplinks used for the vDS. In this case, dual uplink ports are configured for redundancy (Figure 26).
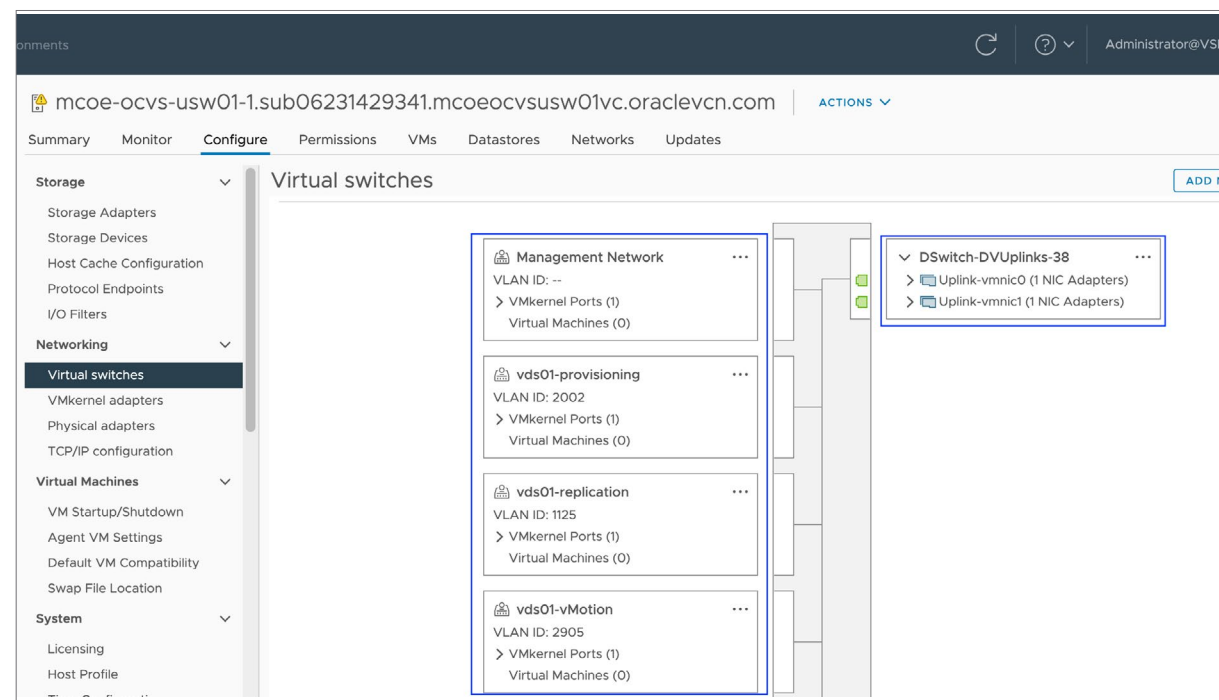
FIGURE 26. Distributed switch details

vmware® | ORACLE Cloud

NSX configuration

NSX-T is automatically deployed and configured as a part of the Oracle Cloud VMware Solution. However, ongoing management and configuration of NSX-T will be required if additional workload segments in the future are required.

View NSX configuration

1. In the **Oracle Cloud Interface,** click on the burger icon at the top left of the screen to display the Menu

    a. Select **Hybrid > VMware Solution**

    b. Select the name for the **software-defined datacenter**

    c. In the Software-Defined Datacenter Information section, Copy the **NSX Manager URL**

    d. Paste the **vSphere Client URL** into a new browser tab

    e. Copy/Paste the **NSX Manager Initial Username** and **NSX Manager Initial password** to log in to NSX Manager

NSX-T segments

6. Click on **Segments**
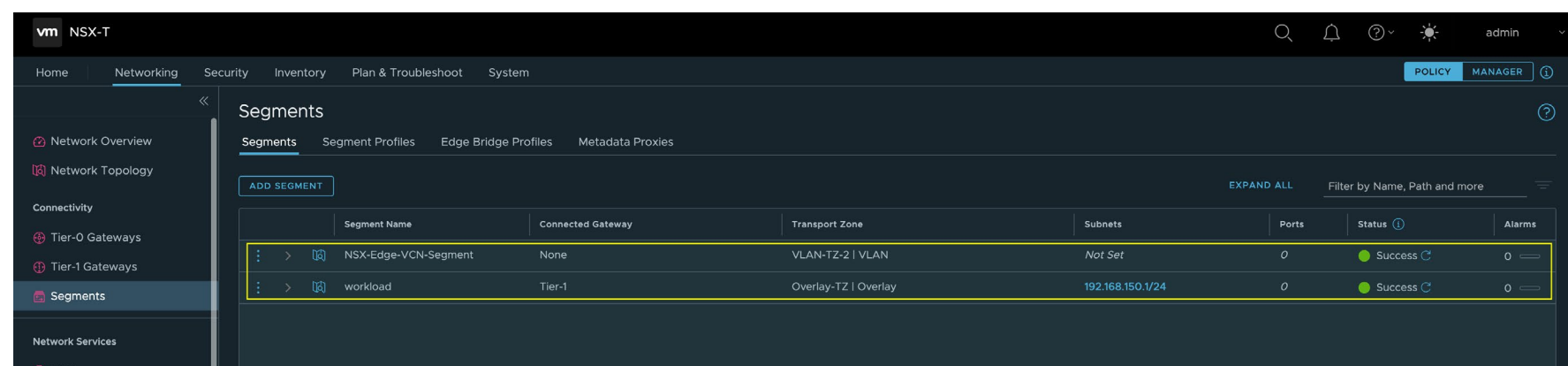
FIGURE 27. NSX-T segments

There are two segments created by default. When creating additional segments, use the workload segment as a template.

NSX-Edge-VCN-Segment	This segment is used for connectivity between the two Edge nodes
workload	This segment is used for the workload network (192.168.150.1/24) that was specified during the deployment of the software-defined datacenter (If you did not choose to deploy a workload network, you might not have this segment)

TABLE 6. Default NSX-T segments

NSX-T logical routers

There are two logical routers, Tier-0 and Tier-1.

Tier-0	Connected to the NSX Edge VTEP VLAN, it allows Geneve-encapsulated traffic to flow between the Edge nodes and ESXi Host. The NSX Edge Uplink VLANs allow traffic in and out of the environment
Tier-1	Connected to the workload segment where the virtual machines will live. As you add additional segments, these will be connected to the Tier-1

TABLE 7. NSX-T logical routers
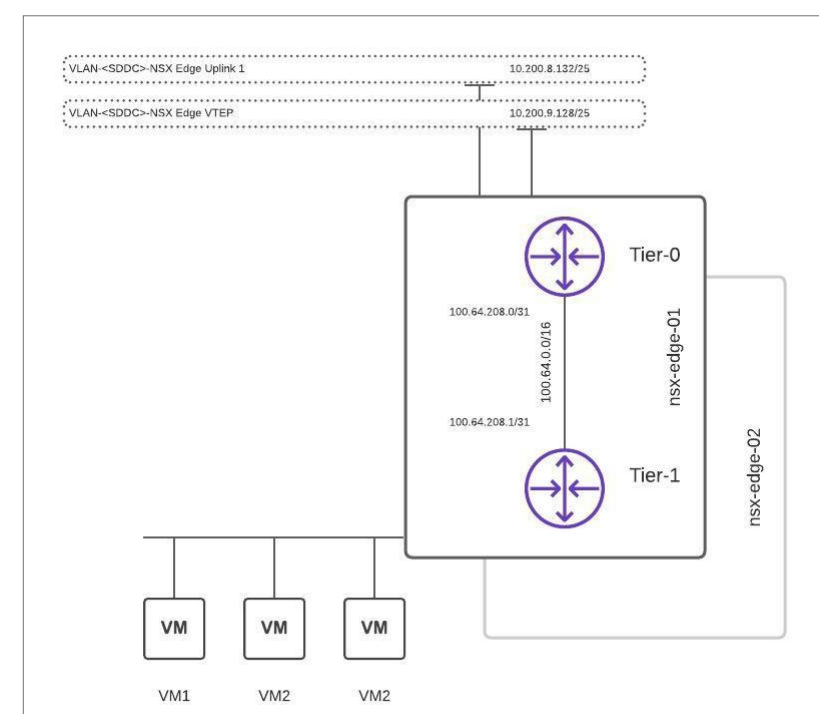
FIGURE 28. NSX-T logical routers

vmware® | ORACLE Cloud

NSX-T Transport Zones

There are three Transport Zones configured by default.

Overlay-TZ	An Overlay Transport Zone includes all ESXi Hosts and both NSX-T Edges and is used by the workload segments. This Transport Zone should be used when deploying additional segments.
VLAN-TZ	A VLAN Transport Zone which includes all ESXi Hosts and both NSX-T Edges and is used by the edge-ns and edge-transport logical switches
VLAN-TZ-2	A VLAN Transport Zone which only includes both NSX-T Edges and is used for Edge-to-Edge Geneve encapsulated traffic over the NSX-Edge-VCN-Segment segment

TABLE 8. NSX-T Transport Zones
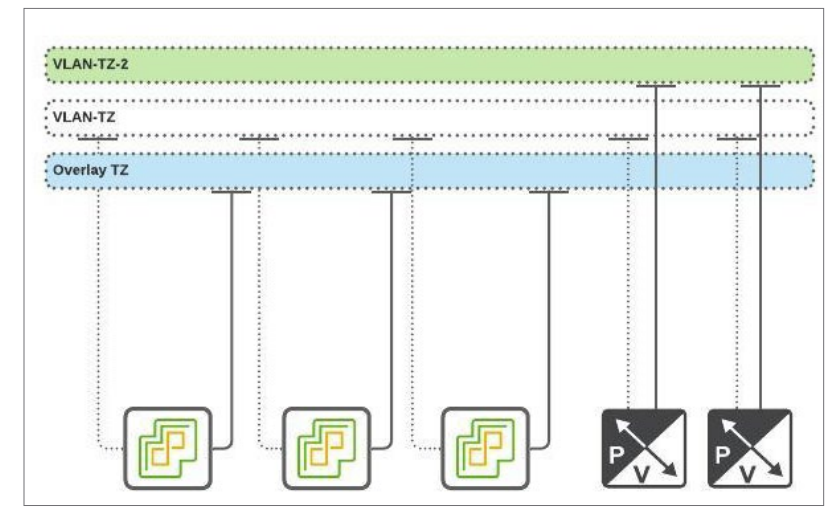
FIGURE 29. NSX-T Transport Zones

Networking summary

Figure 30 illustrates how all the components that make up the Oracle Cloud VMware Solution software-defined datacenter environment are connected.
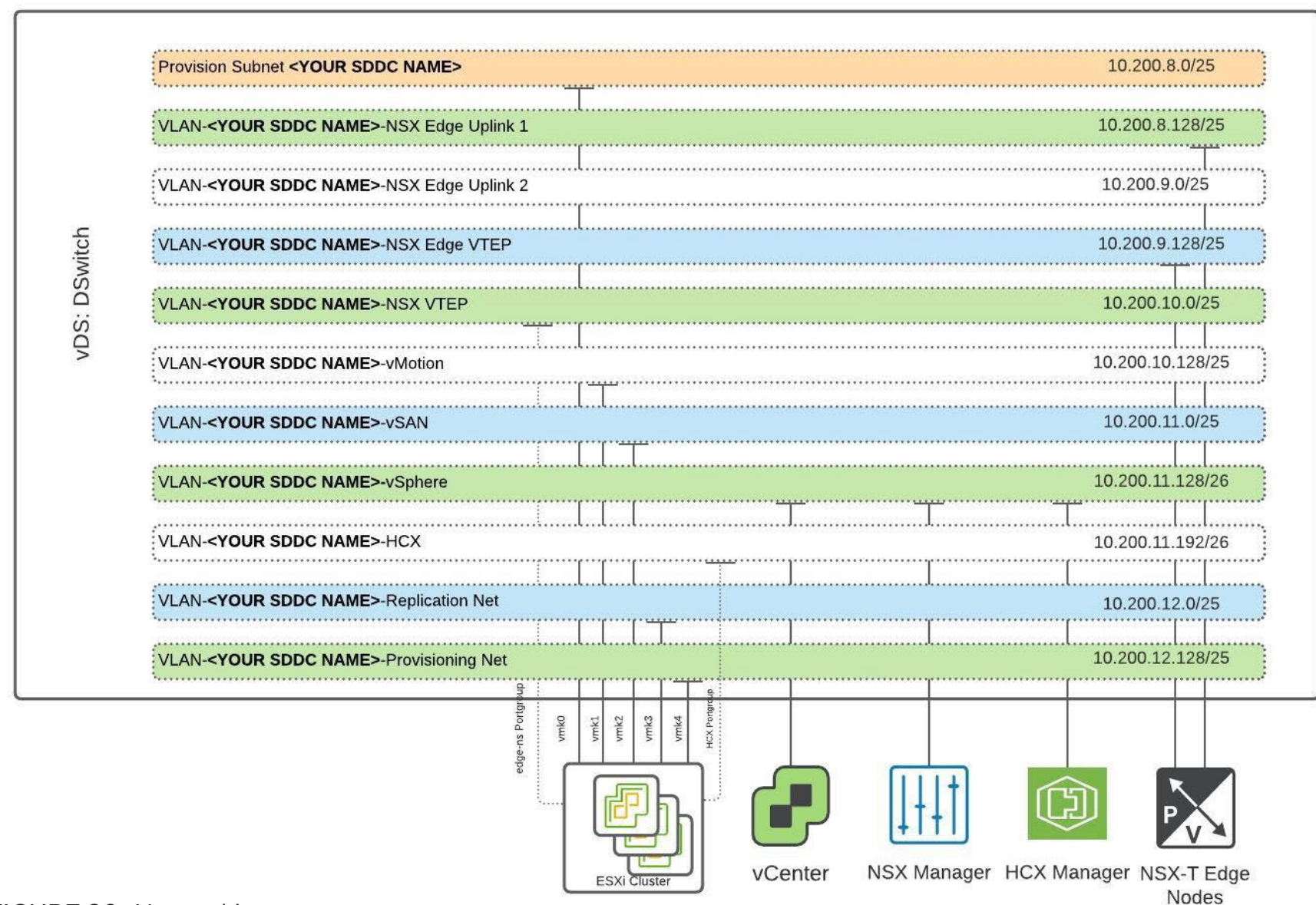
FIGURE 30. Networking summary

Connecting to Oracle Cloud Infrastructure Services

This chapter will discuss deploying a Windows Server into an Oracle Cloud VMware Solution software-defined datacenter and connecting it to an Oracle Cloud Infrastructure Network File System (NFS) used to store files and folders for users. This example will show how easy it is to connect Oracle VMware Cloud Solution workloads to Oracle Cloud Infrastructure services. Figure 31 diagrams this configuration at a high level.
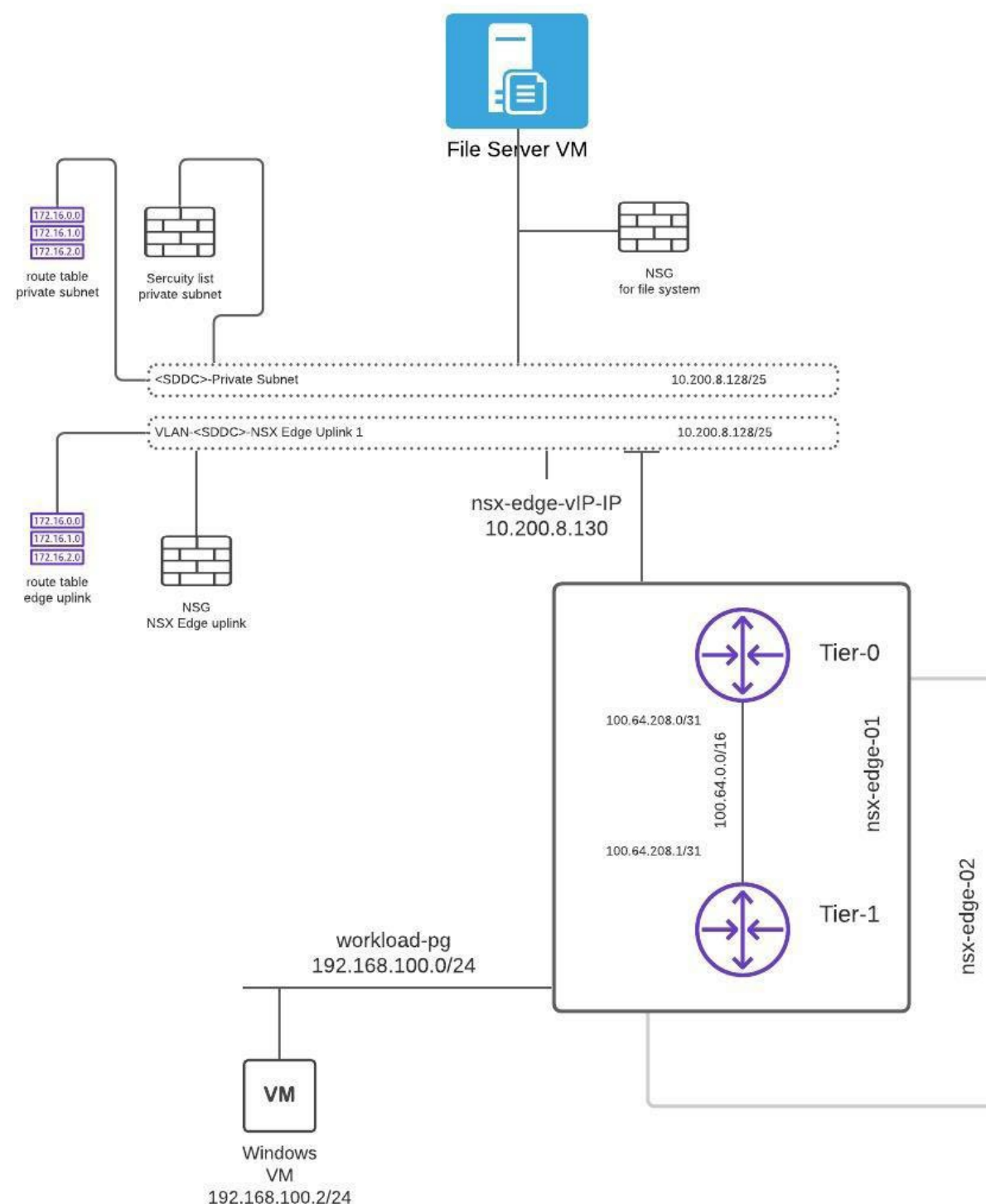
FIGURE 31. Connecting to a file system

Deploying a virtual machine in an Oracle Cloud VMware Solution SDDC

The process of creating virtual machines within the Oracle Cloud VMware Solution is the same as it is in an on-premises environment. Once a virtual machine is created in vCenter, a Windows ISO can be uploaded onto the vSAN datastore and the virtual machine booted from the ISO to install Windows Server. Next, the Windows Server virtual machine is connected to the Network. The workload network is an NSX overlay network that was created during the deployment of the software-defined datacenter.

Add a route to a route table

During the Virtual Cloud Network provisioning process, a private subnet was provisioned. That private subnet in this example will also be used for the File System.

The Windows Server is on a network that is not part of the Virtual Cloud Network. In that case, a route needs to be created so that traffic that needs to go from the private subnet to the Windows Server knows that to get to the Server. It needs to send the traffic to the NSX Edge uplink virtual IP

(VIP). Once the traffic reaches the NSX Tier-0 router via the Edge VIP, it is routed to the Windows server through the Tier-1 router.

For the creation of the Route Table Rules, the following information is needed.

- The workload (overlay) network CIDR block (e.g., 192.168.150.0/24)
- The NSX Edge virtual IP Address (e.g., 10.200.8.130)

The fastest way to find the Edge VIP is the following:

1. Click on the burger icon at the top left of the screen to display the Menu
2. Select **Networking > Virtual Cloud Networks**
   a. Click on the **Virtual Cloud Network** (e.g., MCoE-OCVS-USW01-VCN)
   b. Select **VLANs** in the **Resources** section on the bottom left of the screen
   c. Select **VLAN-<SDDC name>-NSX Edge Uplink 1**
   d. Make a note of the **Private IP Address** of the **nsx-edge-up1-vip** (e.g., 10.200.8.130)
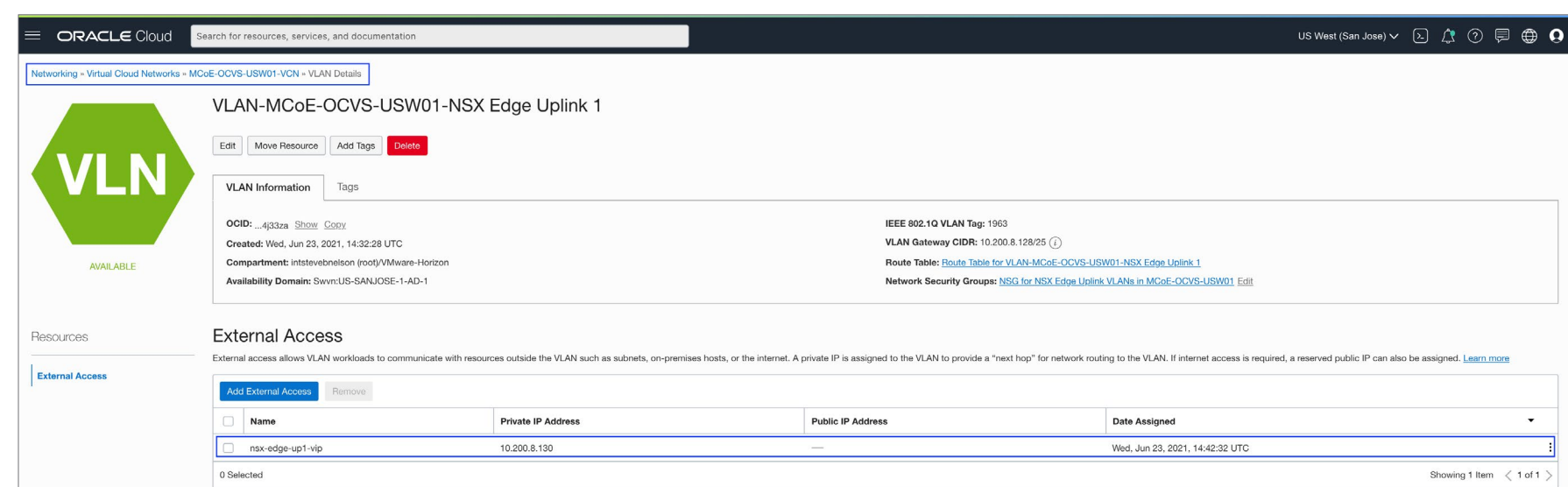
FIGURE 32. Edge vIP

With the information gathered, it is time to update the route table of the private subnet:

3. Click on the burger icon at the top left of the screen to display the Menu
4. Select **Networking > Virtual Cloud Networks**
5. Click on **Virtual Cloud Networks** (e.g., MCoE-OCVS-USW01-VCN)
   a. Click **Route Tables**
   b. Select **Route Table for <Private Subnet-<SDDC>-VCN**
   c. Click Add **Route Rules**
      - Select **Private IP** as the Target Type
      - Enter the **CIDR Block** for the workload (overlay) network (e.g., 192.168.150.0/24)
      - Enter the **NSX Edge vIP Address** in Target Selection (e.g 10.200.8.130)
      - Click **Add Route Rules**
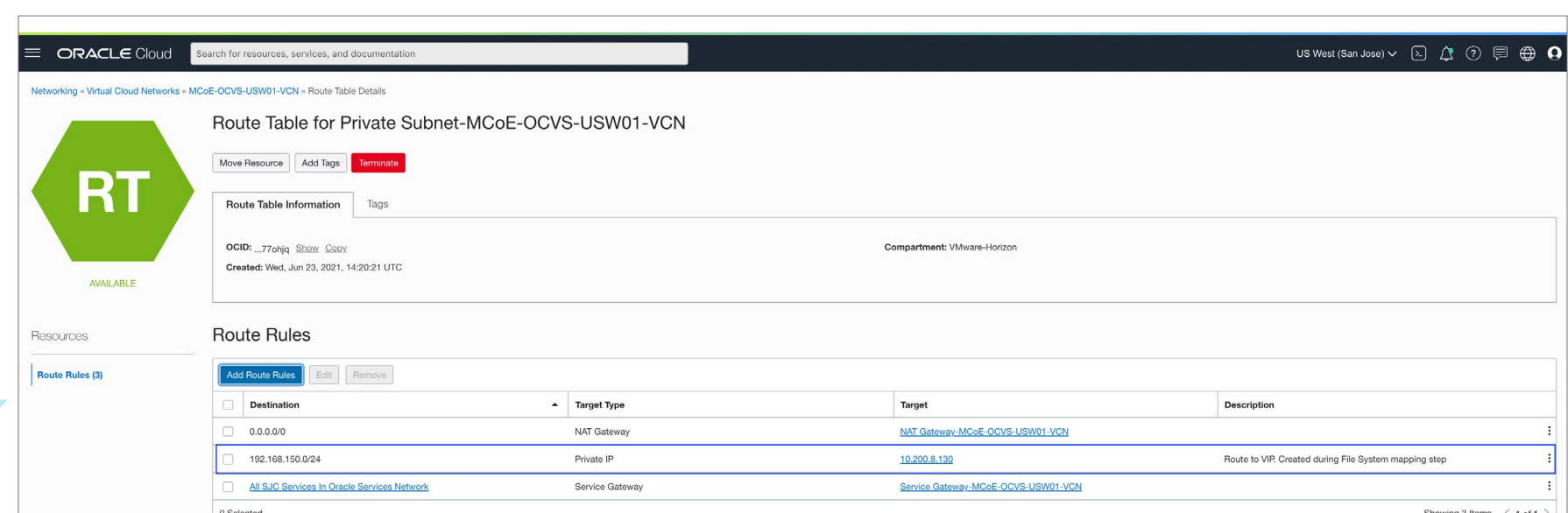
FIGURE 33. Route Rule

The Route Rule should look like Figure 33. This rule directs any traffic that to go to the workload network to the NSX Edge vIP address.

Network security groups

Network Security Groups (NSG) will allow traffic to flow from the NSX Edge Uplink 1 VLAN to the File System. In addition, Security Lists can also be used to allow traffic to flow.

Create a network security group

1. Click on the burger icon at the top left of the screen to display the Menu

2. Select **Networking > Virtual Cloud Networks**

   a. Click the **Virtual Cloud Network** (e.g., MCoE-OCVS-USW01-VCN)

   b. Select **Network Security Groups**

   c. Click **Create Network Security Groups**

   • **Name** the NSG (e.g. 'NSG for File System (NFS)' is used)

   • Click **Next**

   • Click **Create**

> **WHY USE NETWORK SECURITY GROUPS INSTEAD OF SECURITY LISTS?**
>
> Security lists are associated with subnets. If a security list is used to set up your security rules, those rules will apply to all vNICs in the subnet. Unlike security list rules, NSGs apply only to resource vNICs you add to the NSG and allow more granularity.
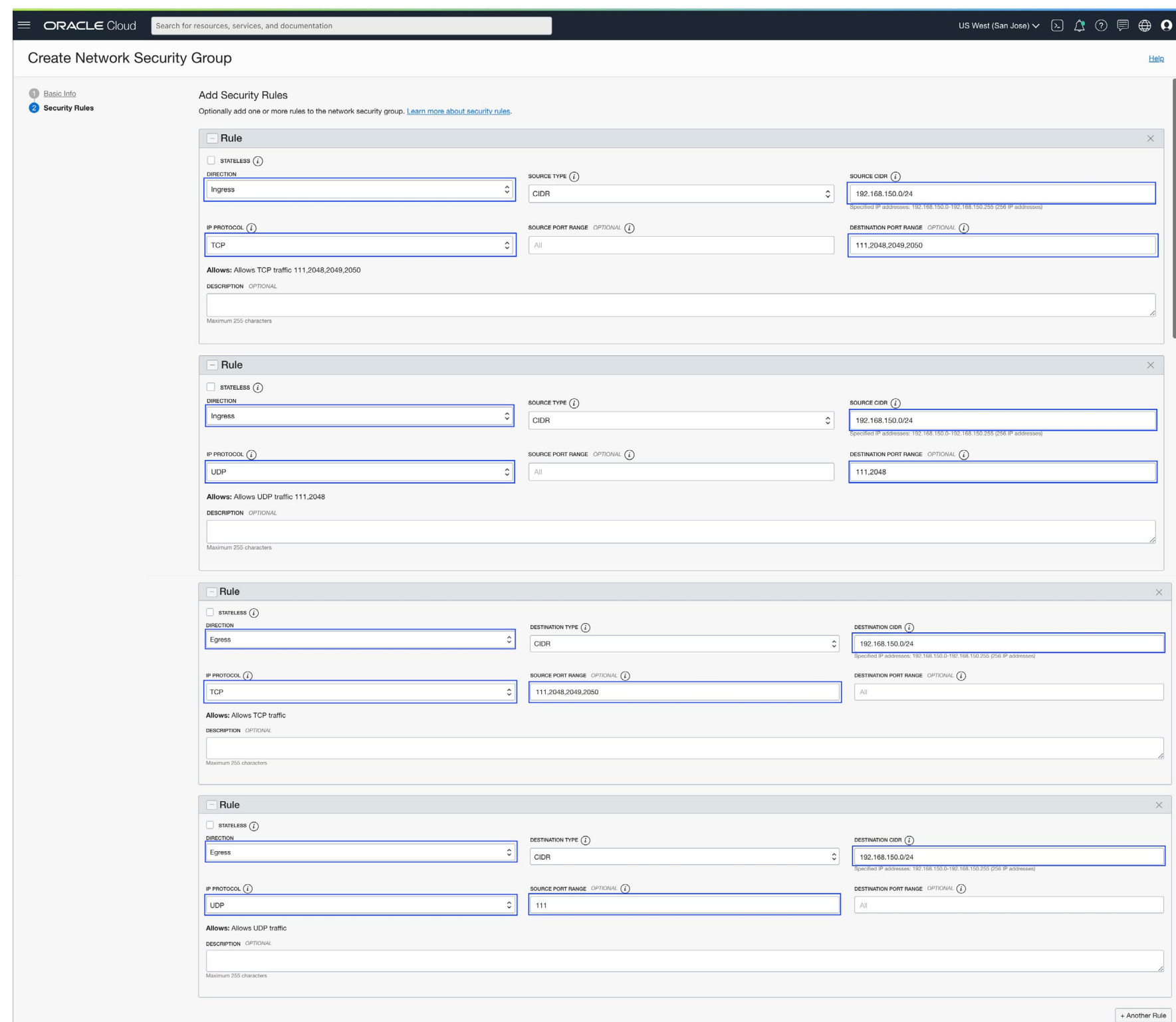
FIGURE 34. Creating a Network Security Group

Use the following *Security Rules for File Storage* to enable NFS communication. Different OCI service(s) may require different ports.

NOTE: The Source CIDR specified in the screenshots is the CIDR for the workload (overlay) network here in this environment.

See Table 9 for a summary of Security Rules for File Storage.

vmware® | ORACLE Cloud

Direction	Source or Destination	Protocol	Ports
Ingress	Source Type: CIDR Source: 192.168.150.0/24	TCP	Source Port Range: ALL Destination Port Range: 111,2048-2050
Ingress	Source Type: CIDR Source: 192.168.150.0/24	UDP	Source Port Range: ALL Destination Port Range: 111,2048
Egress	Destination Type: CIDR Source: 192.168.150.0/24	TCP	Source Port Range: 111,2048-2050 Destination Port Range: All
Egress	Destination Type: CIDR Source: 192.168.150.0/24	UDP	Source Port Range:111 Destination Port Range: All

TABLE 9. Security Rules for File Storage

File systems

Up next is creating a **File System** that will be mounted to the Windows Server virtual machine and used to store users' files and folders.

Create a file system

1. Click on the burger icon at the top left of the screen to display the Menu

2. Select File **Storage > File Systems**

3. Click **Create File System**

   a. Click **Edit Details** in the File System Information section (Figure 35)

   b. **Name** the File System (e.g. MCoE-OCVS-USW01-userdata)

3. Click **Edit Details** in the Mount Target Information section (Figure 36)

   a. Select **Create New Moun**t

   b. Name the **New Mount Target** (e.g userdata)

   c. Select a **private subnet** in the Subnet dropdown

   d. Check **Use network security groups** to control traffic

   e. Select the **Network Security Group** created earlier

   f. Click **Create**

FIGURE 35. File System Information

FIGURE 36. Mount Target Information

Mounting the file system

With the new File System created and the Network Security Group applied to the Target Mount, the File System is ready to be mounted on a Windows Server virtual machine.

There are two pieces of information required to mount the File System: the **Mount Target IP Address** and **Export Path.**

7. Click on the burger icon at the top left of the screen to display the Menu

8. Select **File Storage > File Systems**

    a. Click the **File System Name**

    b. Click the **Mount Target**

    • Note the **IP Address** (e.g.10.200.1.196)

    • Note the **Export Path** (e.g. /MCoE-OCVS-USW01-userdata)
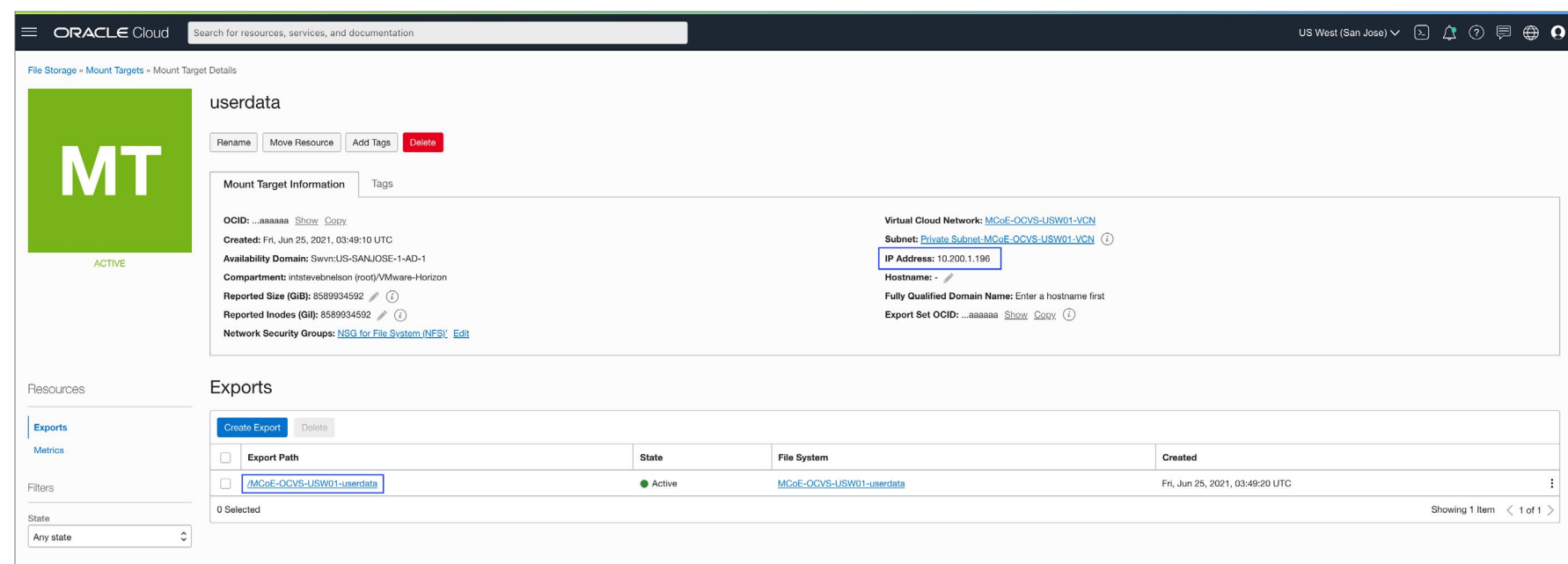
FIGURE 37. Mounting the file system

With this information, *mounting the File System* to a Windows Server can be completed.
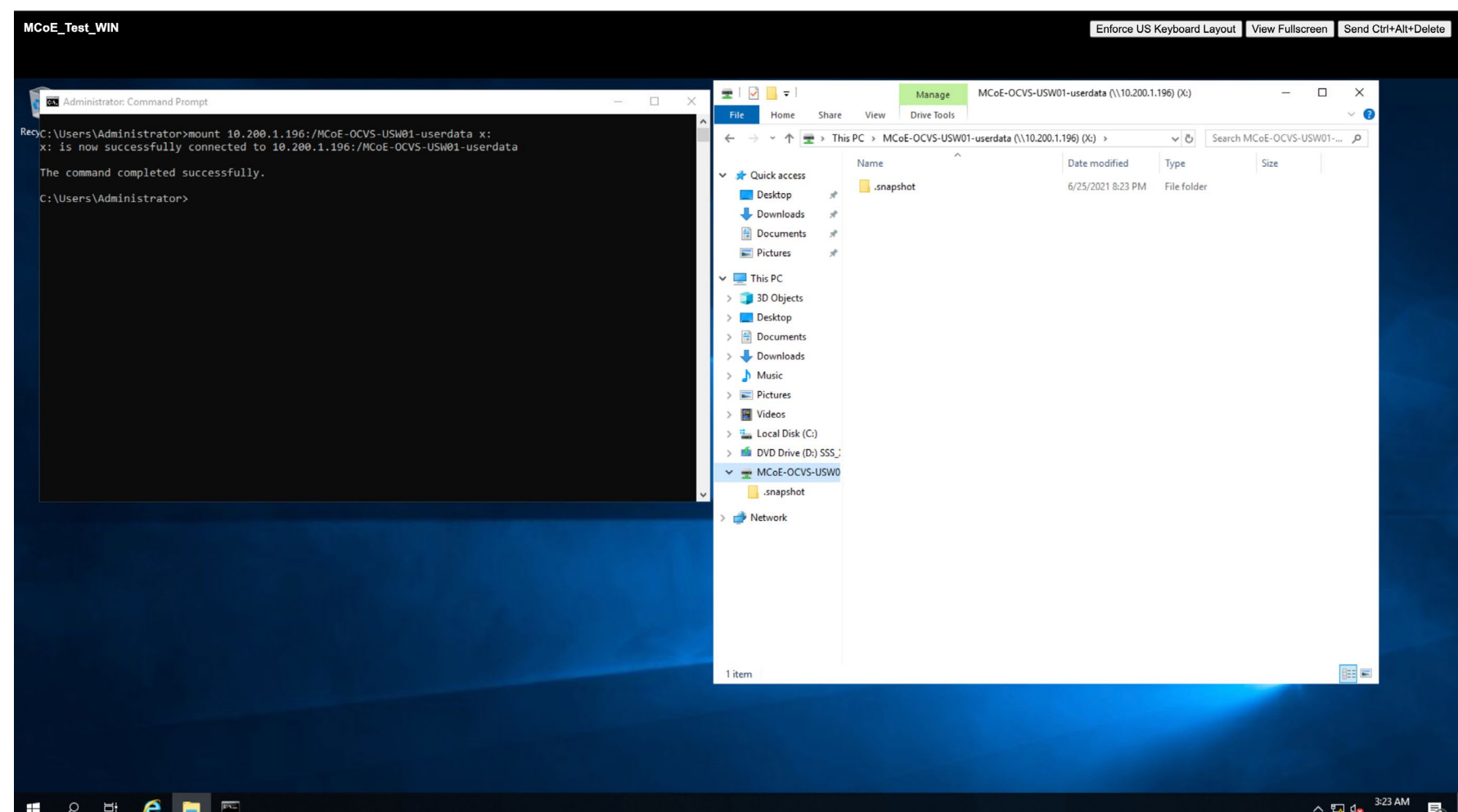
FIGURE 38. Mounting the file system

Figure 39 illustrates the simplicity of how Oracle Cloud VMware Solution workloads can interact with native Oracle Cloud services.

In the high-level diagram, all the components deployed for the Windows server within the SDDC communicate with the File System within OCI. This visual of the traffic flow between the servers will make things a little clearer.
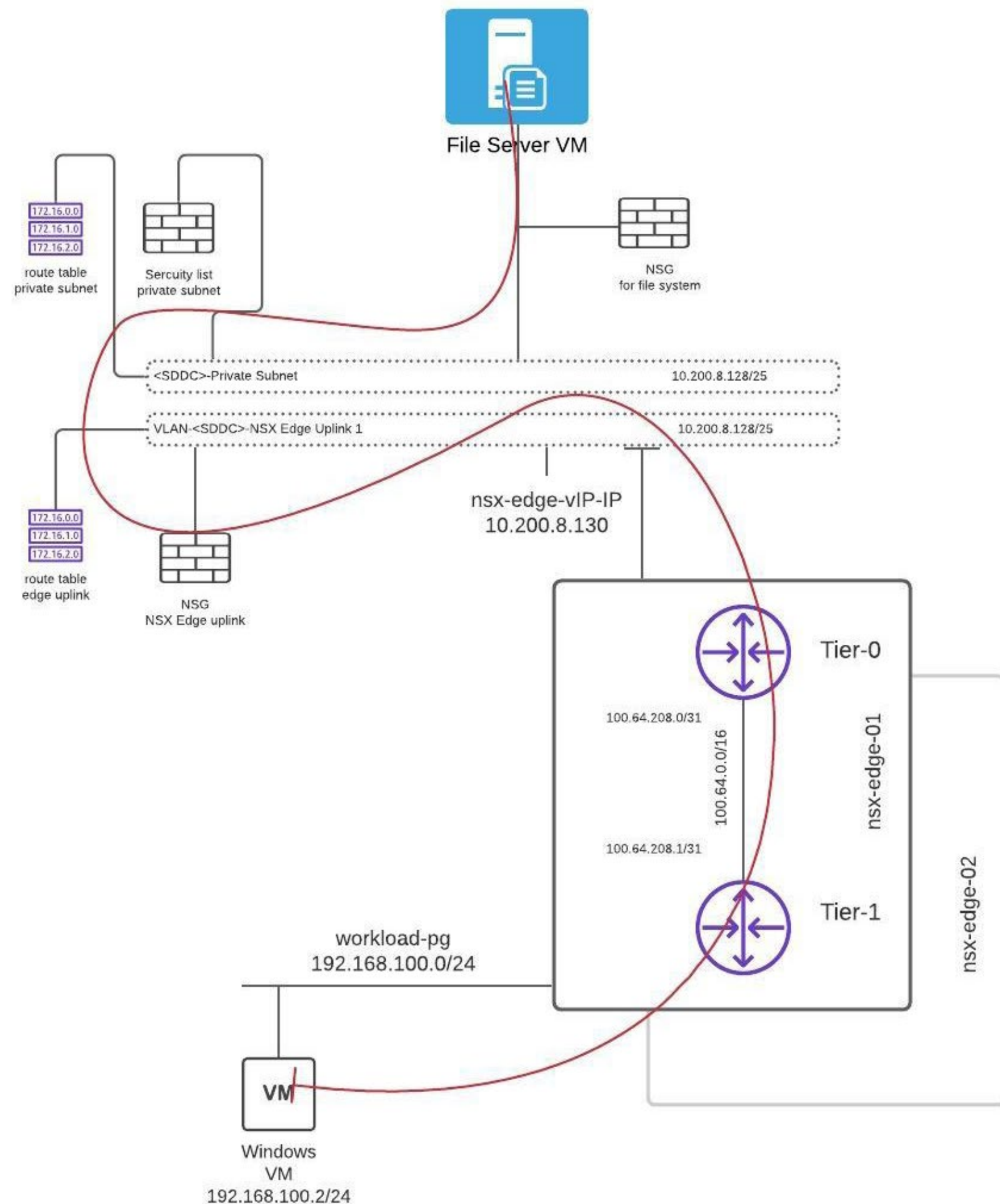
FIGURE 39. File system flow diagram

Starting at the bottom of the graphic and moving to the top, the traffic from the Windows server flows through the Tier-1 router and out through the Tier-0 router. The traffic flow is due to the File System resides outside of the software-defined datacenter. The traffic exits the NSX-T Edge using the Uplink 1 VLAN and out through the VLAN default gateway. The traffic arrives on the private subnet and is then checked against the Security List for the Private VLAN and the Network Security Group for the File system before reaching the Mount Target.

Connecting to an on-premises environment

This chapter addresses external connectivity and how to connect an on-premises vSphere environment to Oracle Cloud VMware Solution, achieving hybrid connectivity between an on-premises environment and the Cloud. This configuration will allow on-premises workloads to communicate with workloads in the Oracle Cloud.

There are two main ways to connect Oracle Cloud VMware Solution to an on-premises environment: *Oracle FastConnect* or *Oracle VPN Connect*. In this chapter, we will use an Oracle FastConnect connection provided by *Megaport*, as demonstrated in Figure 40.

HELPFUL NOTE

There are other ways to set up Oracle FastConnect via third-party service providers. This guide references the direct use of Oracle FastConnect or Oracle VPN Connect solutions.
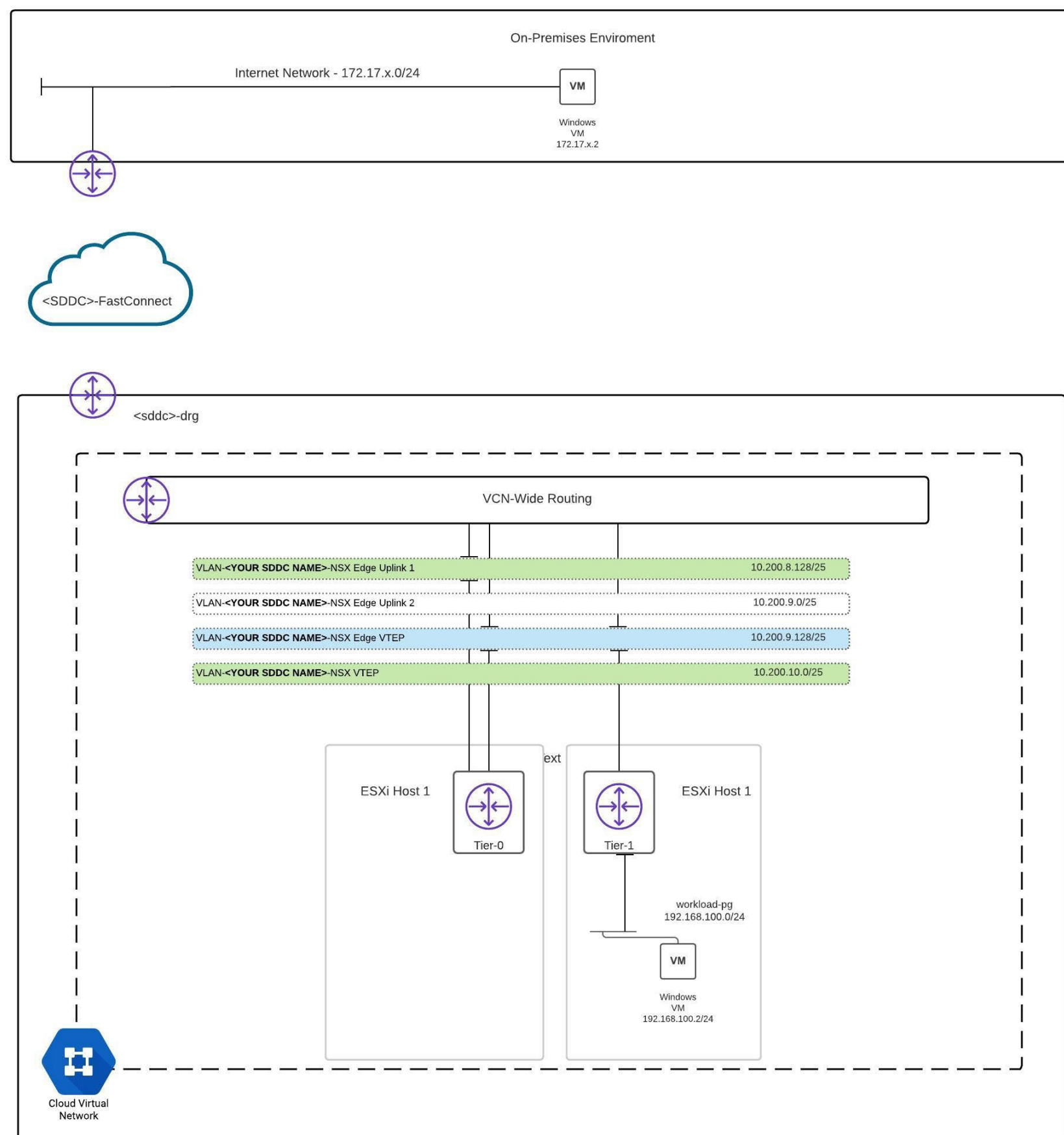
FIGURE 40. Connecting to an On-Premises Environment

The following steps describe how to:

• Create a Dynamic Routing Gateway

• Create a FastConnect instance

• Configure BGP in the Cloud and on-premises

• Verify connectivity

Create a Dynamic Routing Gateway

The first step to enabling hybrid connectivity is to deploy a *Dynamic Routing Gateway (DRG)* within the Oracle Cloud Infrastructure (OCI). Think of a Dynamic Routing Gateway as a virtual router that provides a path for private traffic (that is, traffic that uses private IP v4 addresses) between a Virtual Cloud Network and networks outside the Virtual Cloud Network's region.

1. Log in to the **Oracle Cloud VMware Solution console**
2. Select the correct **Region** (This should be the same region that the software-defined datacenter and the Bastion Host are deployed)
3. Click on the burger icon at the top left of the screen to display the Menu
4. Select Networking > Dynamic Routing Gateways

   a. Click **Create Dynamic Routing Gateway**

   b. Select the correct **Compartment**

   c. Name the **DRG**

   d. Click **Create Dynamic Routing Gateway**

Once the DRG has been created, attach it to the Virtual Cloud Network.

5. Click **Virtual Cloud Networks** on the Resources section (left-hand side)

   a. Click **Attach to Virtual Cloud Network Attachments**

   b. Name the **Attachment**

   c. Select your **Virtual Cloud Network** in the dropdown

   d. Click **Create Cloud Network Attachment**

Create A FastConnect instance

Before a FastConnect connection can be created, you need to collect the information required for this process.

- **BGP IP Addresses**: You will need two IP addresses to use for the BGP connection between the FastConnect and your on-premises or cloud router. Typically, *Link-Local Addresses* are used for this.

- **Customer BGP ASN**: You will need the *Autonomous System Number (ASN)*. When using a service like Megaport, the ASN can be found in the portal. If you use an on-premises router, you can usually choose an ASN from the private range: 64512 – 65534. If you aren't sure, speak to your networking team.

1. Log in to the **Oracle Cloud VMware Solution console**
2. Select the correct **Region** (This should be the same region that the software-defined datacenter and the Bastion Host are deployed)
3. Click on the burger icon at the top left of the screen to display the **Menu**
4. Select **Networking > FastConnect**

   a. Click **Create FastConnect**

   b. Select your **Connection Type** (Here Partner is selected because Megaport is being used)

   c. If you selected FastConnect Partner, select your **Partner** from the dropdown

   d. Click **Next**

      - **Name** the FastConnect Connection

      - Select **Private Virtual Circuit**

      - Select your **Dynamic Routing Gateway** from the dropdown

      - Select the **Bandwidth** for the connection

      - Enter the **Customer BGP IPv4 Address** (e.g 169.254.238.49/30)

      - Enter the **Oracle BGP IPv4 Address** (e.g., 169.254.238.50/30)

      - Enter the **Customer BGP ASN** (133937)

      - Click **Create**

vmware® | ORACLE Cloud

Configuring BGP on-premises

In this step, you configure the on-premises router to establish a BGP session. This step depends on the router or service you are using for your on-premises connectivity. I use a Megaport connection for the example/demo; refer to the *Connecting to Oracle Cloud Infrastructure FastConnect documentation* for more details.

The information needed to complete the configuration can be found in the OCI interface.

1. Click on the burger icon at the top left of the screen to display the **Menu**

2. Select **Networking > FastConnect**

    a. Click the **name of the FastConnect Connection** you just created

    b. Click the **BGP Information** tab.
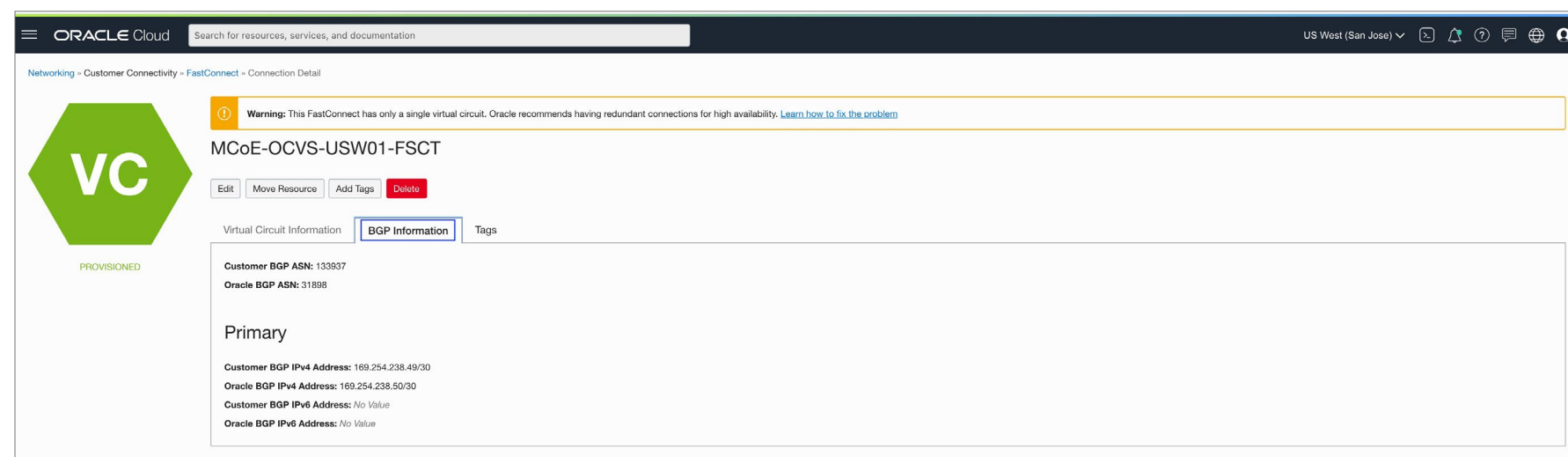
FIGURE 41. BGP Information

    c. The information you are looking for is as follows:

    • **FastConnect OCID** (The OCID is often required by services such as Megaport)

    • **Oracle BGP ASN**

    • **Oracle BGP IPv4 Address**
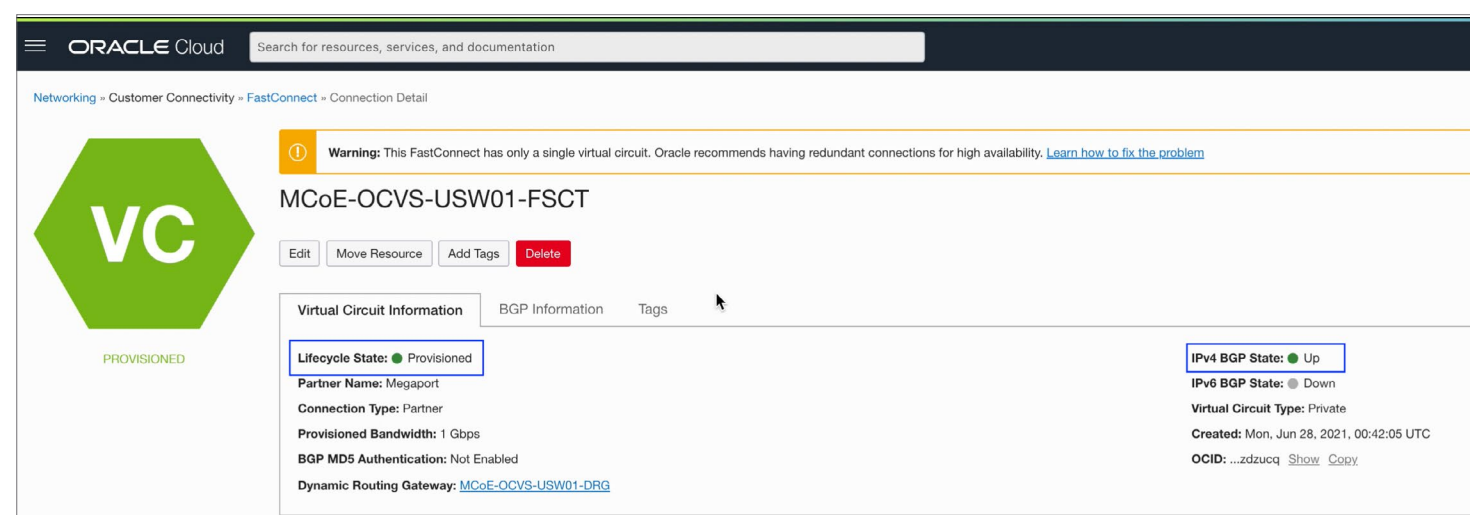
FIGURE 42. FastConnect Provision Status

With this information, configure BGP. Once correctly configured, the OCI console will appear green, Lifecycle State will show as Provisioned, and the IPv4 BGP Status will display as UP.

vmware® | ORACLE Cloud

Configure route tables and network security groups

With the on-premises connectivity established, the next step is configuring the OCI environment to allow traffic to flow between the on-premises environment and the Windows Server virtual machine running within the Oracle Cloud VMware Solution software-defined datacenter.

Oracle Cloud provides a simple wizard that creates the required configuration automatically.

1. Click on the burger icon at the top left of the screen to display the Menu

2. Select **Hybrid > VMware Solution**

    a. Select the **name** of the **software-defined datacenter**

    b. Click **Configure connectivity to your on-premises Network** (Figure 43)
       • Enter the **CIDR Block** of the **workload overlay network** (In this example, we used 192.168.150.0/24)
       • Enter the **CIDR Block** of the **on-premises Network** that you want to connect to (172.17.31.0/24)

    c. Click **Next**

FIGURE 43. Configure connectivity to your on-premises network

    d. **Review** the configuration (Figure 44)

    e. Click **Apply Configuration**

FIGURE 44. Review configuration

The review page displays Route Table and Network Security Group configurations the wizard is going to create. By default, the wizard allows ALL traffic between the on-premises Network and the workload network. If this is not desired, change the rules configured on the following NSG: 'NSG for NSX Edge Uplink VLANs in <your sddc>.'
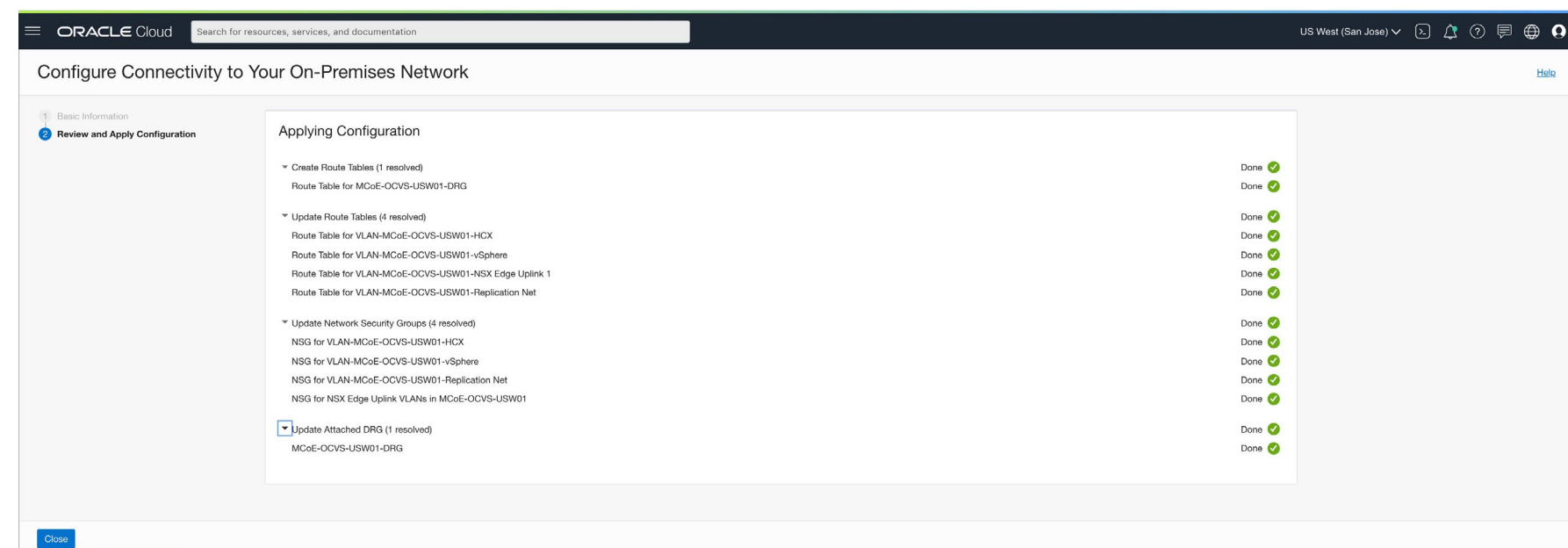

FIGURE 45. Applying configuration

Testing connectivity

The last step is to validate that connectivity works between your on-premises environment and your Windows server running in the Oracle Cloud VMware Solution software-defined datacenter.

1. Perform a simple ping from a server running in the on-premises environment to a server running in Oracle Cloud VMware Solution.

2. If the ping responds, try pinging from the Windows server from a Remote Desktop. Remote Desktop isn't enabled by default in Windows either, so be sure to enable it first.

> **HELPFUL NOTE**
> Windows will block ping by default, so allow ping through the windows firewall if you haven't already.
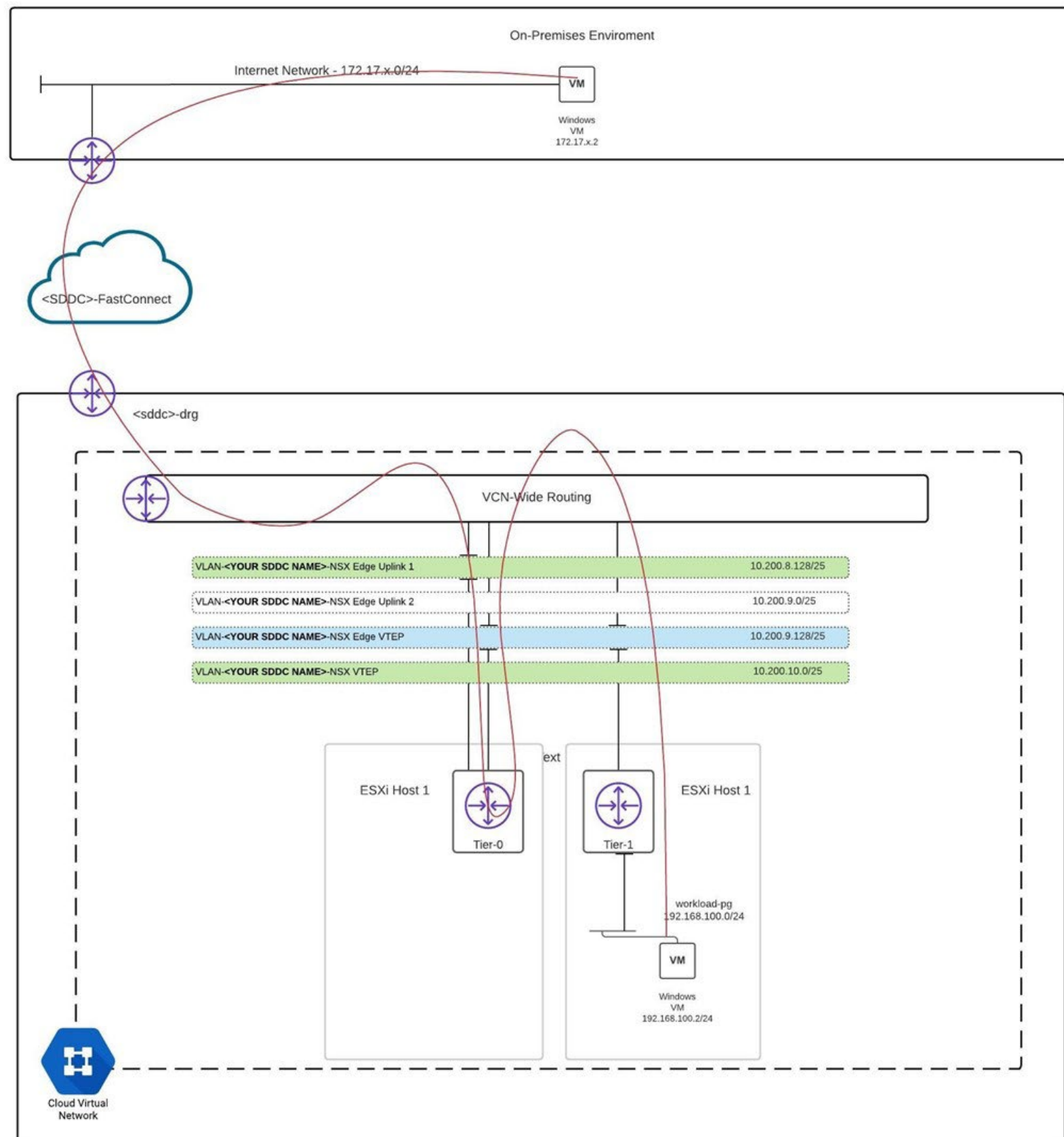
FIGURE 46. Traffic flow from on-premises to cloud

Traffic flowing from your on-premises virtual machine exits the on-premises router via its BGP connection established with the Oracle FastConnect. Traffic then enters the Oracle Cloud infrastructure via the Dynamic Routing Gateway and is sent to the 'VLAN-<sddc>-NSX Edge Uplink 1' VLAN, where it enters the NSX Edge VIP. Finally, the NSX-T Tier-0 router forwards the traffic to the Tier-1 router, which sends the traffic to the Windows server connected to the workload Segment.

Migrating workloads using VMware HCX

This chapter covers the installation of VMware HCX in an on-premises vSphere environment and a site-pairing configuration between the on-premises environment and Oracle Cloud VMware Solution. Once HCX is configured, connectivity will be tested by migrating a workload between sites. The vMotion of virtual machines between sites requires extending networks allowing virtual machines to move between sites without changing the IP addresses. The process to extend a network will also be covered in this chapter.

Figure 48 is a high-level diagram of an HCX deployment utilizing FastConnect to connect an on-premise SDDC to an Oracle Cloud VMware Solution SDDC.

> **HELPFUL NOTE**
>
> This chapter will not review the details of how to configure your HCX service mesh. More information about the configuration of the HCX service mesh can be found in VMware's official documentation: *VMware HCX User Guide*.
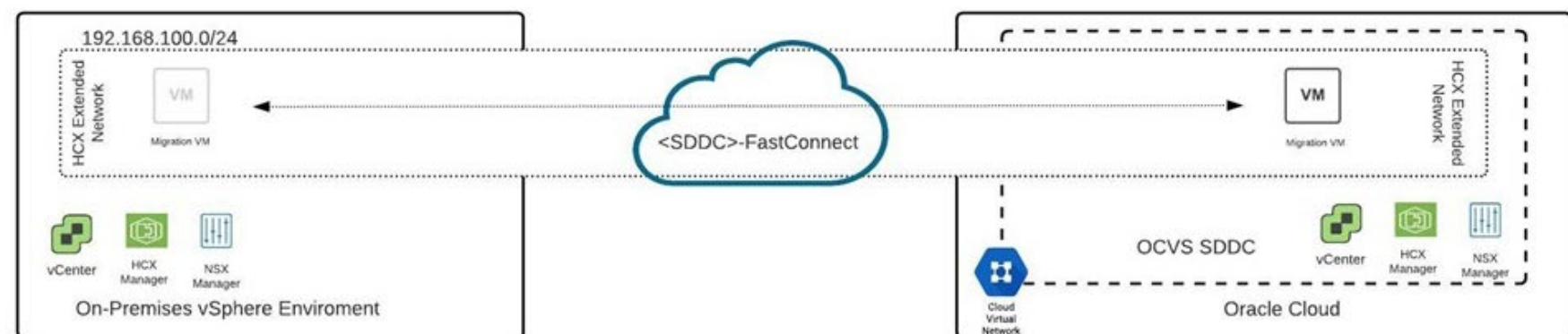

FIGURE 48. HCX deployment

The following steps describe how to:

• Install HCX Connector

• Connect on-premises to Oracle Cloud VMware Solution

• Extend a network from on-premises to Oracle Cloud VMware Solution

• vMotion VMs from on-premises to the Oracle Cloud VMware Solution

• Bulk Migration of a VM from on-premises to Oracle Cloud VMware Solution

Installing the HCX connector

The first step to installing VMware HCX in an on-premises environment is to download the HCX Connector appliance from the HCX instance running in the Oracle Cloud VMware Solution environment. The HCX Connector OVA can also be downloaded from the *HCX Manager*.

1. Log in to the **Oracle Cloud VMware Solution console**

2. Select the correct **region**. This region is where the software-defined datacenter and Bastion Host were deployed.

3. Select **Hybrid > VMware Solution**

   a. Select the name of the **software-defined datacenter**

4. In the **Software-Defined Datacenter Information** section, Copy the **vSphere Client URL**
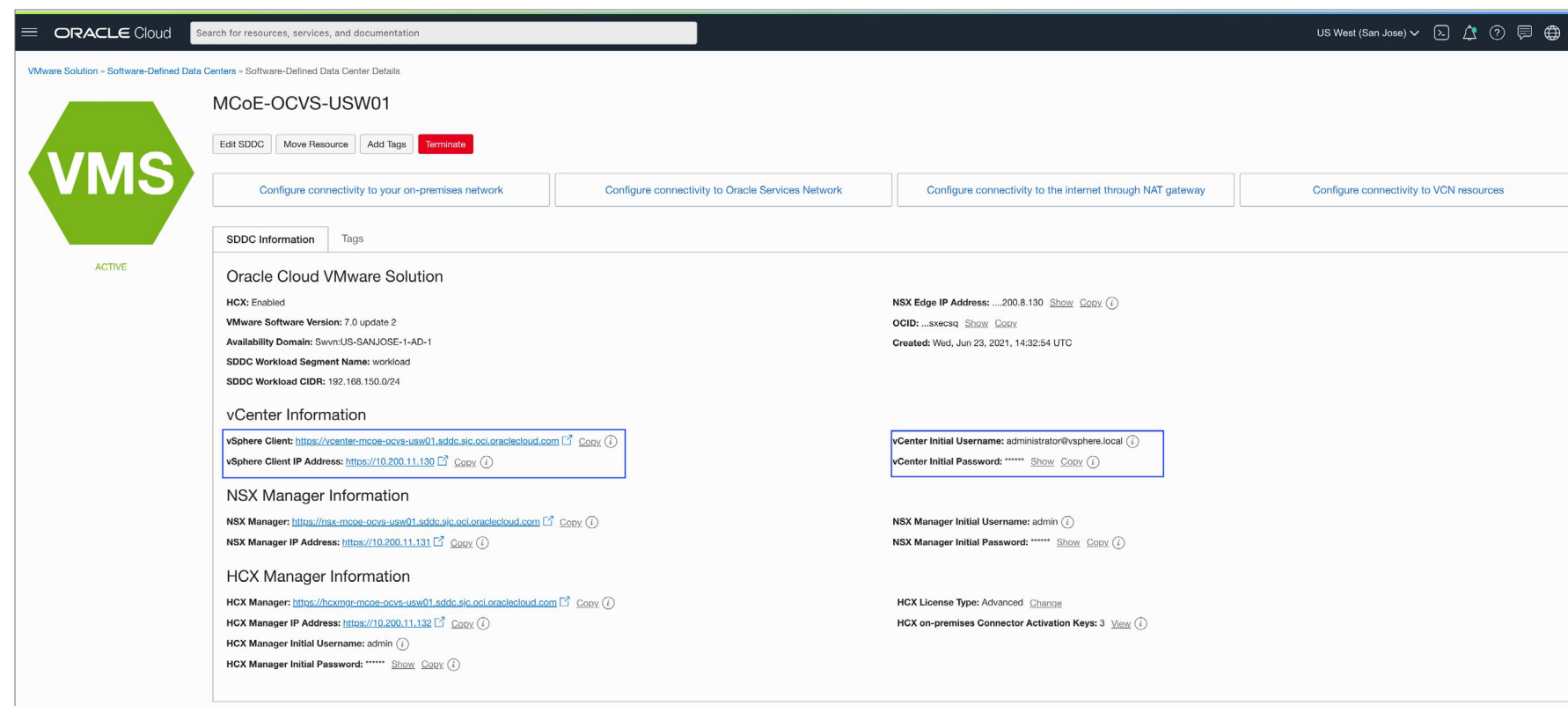
FIGURE 49. Installing the HCX connector

5. Open a browser window either on the **Bastion Host** or on a machine that has access to the Bastion Host via an *SSL Tunnel*

6. Paste the **vSphere Client URL** into a new browser tab

7. Copy/Paste the **vCenter Initial Username** and vCenter Initial password to log in to vCenter

Once logged into vCenter, head into the **HCX interface**.

1. Click **Menu** in the vSphere client and select **HCX** from the dropdown menu (Figure 50)

2. Click **Administration** in the left-hand Menu (Figure 51)
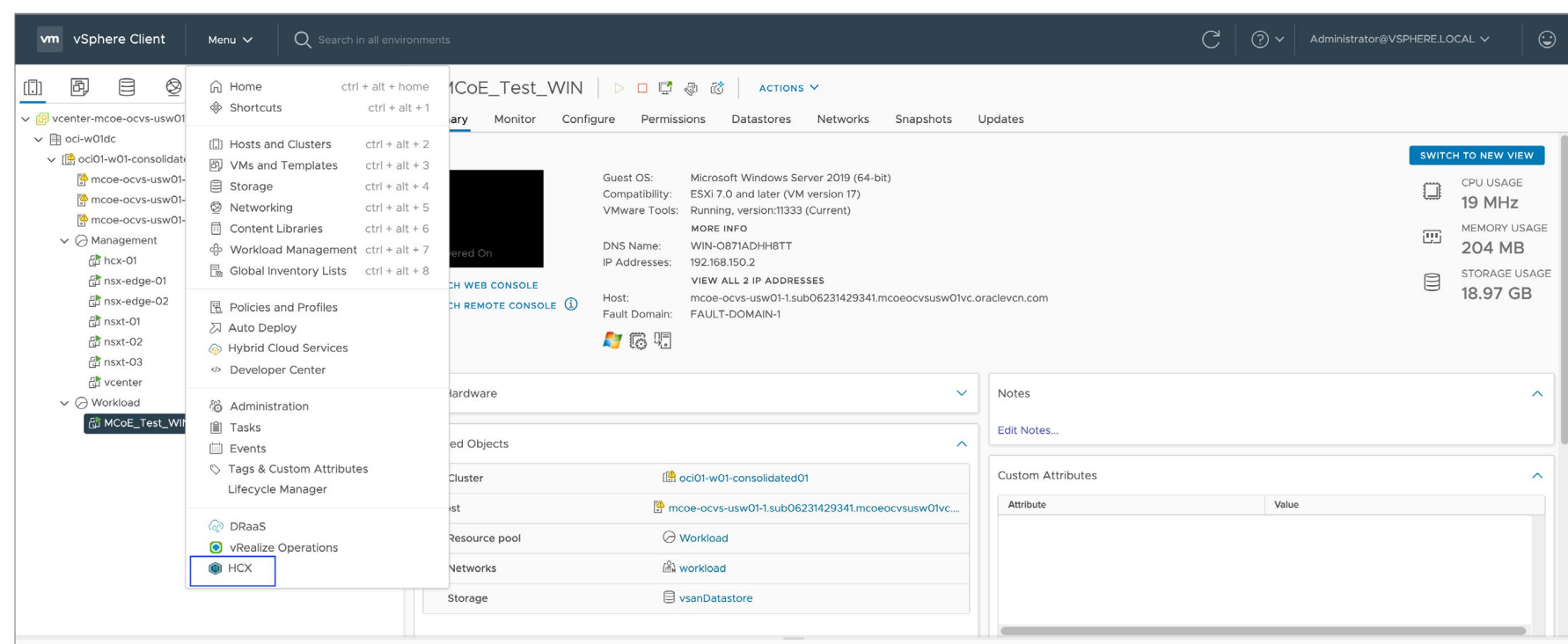
FIGURE 50. Installing the HCX connector

   c. Click **Request Download Link**

   d. Either download the OVA directly or copy the link to the OVA and paste it into a browser to begin the download process.
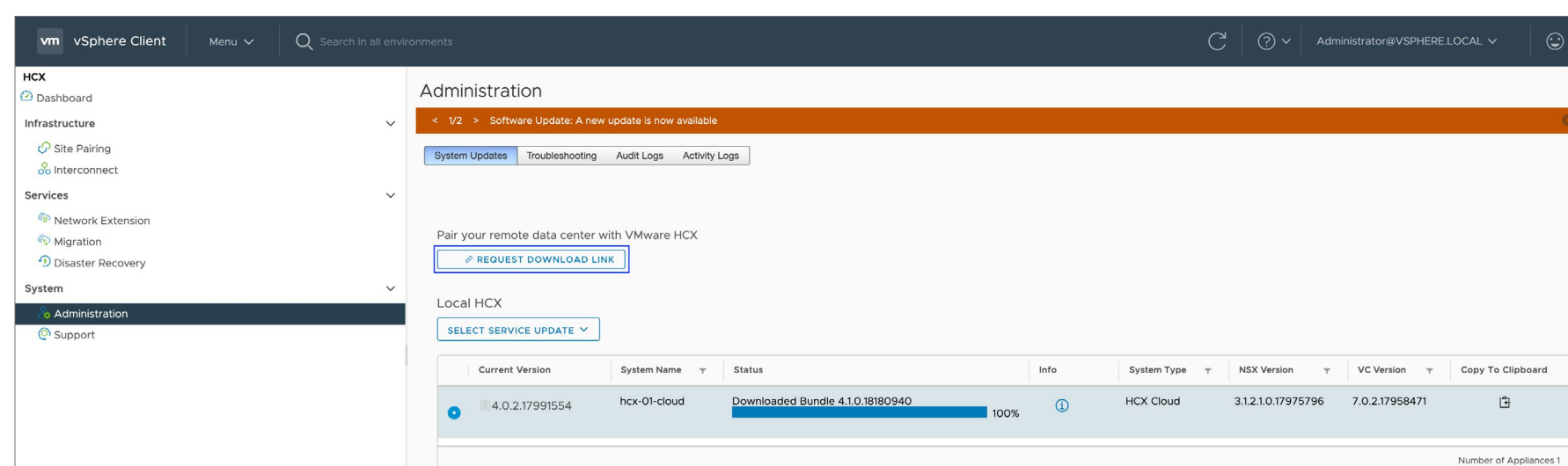

FIGURE 51. VMware HCX administration

Once the OVA has been downloaded, deploy the OVA in the on-premises vSphere environment. See the VMware HCX documentation *Deploying the Installer OVA in the vSphere Client* for more information.

For the on-premises HCX Connector to connect to the HCX Manager in Oracle Cloud VMware Solution, ensure that the following *Firewall ports* are open on your on-premises environment.

To activate the on-premises HCX Connector, you need the HCX License Key from the OCI console.

1. Log in to the **Oracle Cloud VMware Solution console**

2. Select the correct **region** where the software-defined datacenter and Bastion Host were deployed.

3. Select the name of your **software-defined datacenter**

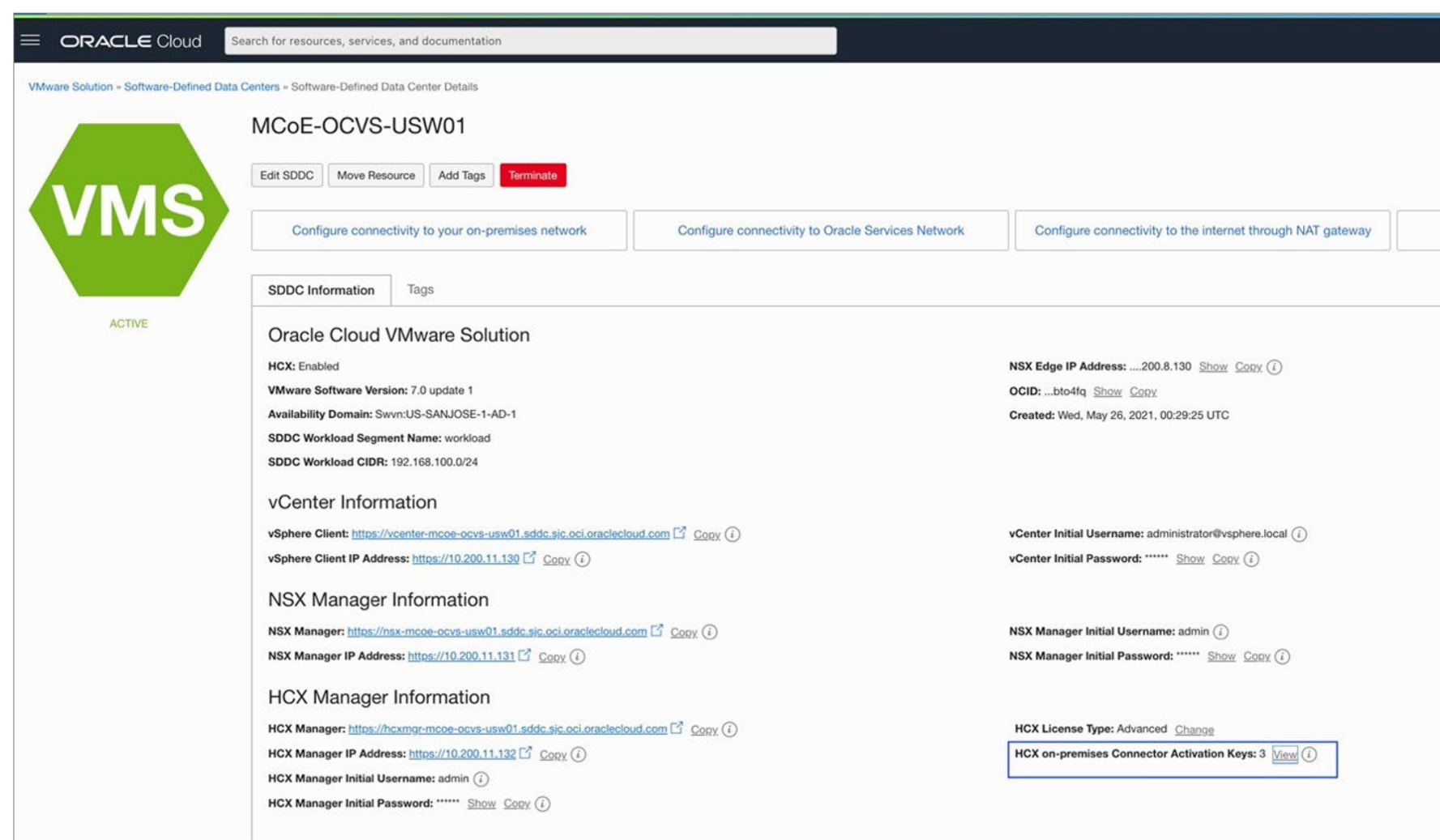4. Copy the **HCX On-premises Connector Activation Key**

FIGURE 52. HCX license key

To activate the HCX Connector, follow the steps in the following link, using the HCX Activation key you just copied from the Oracle Cloud VMware Solution software-defined datacenter interface. For additional information, visit *Activating and Configuring HCX*

Create a site pairing to Oracle Cloud VMware Solution

When creating the site pairing between software-defined datacenters, you'll need to specify the HCX Manager FQDN or IP address and then use the vCenter Initial Username and Password. Do not try and use the HCX Manager Initial Username and Password, as you'll end up with an authentication error.
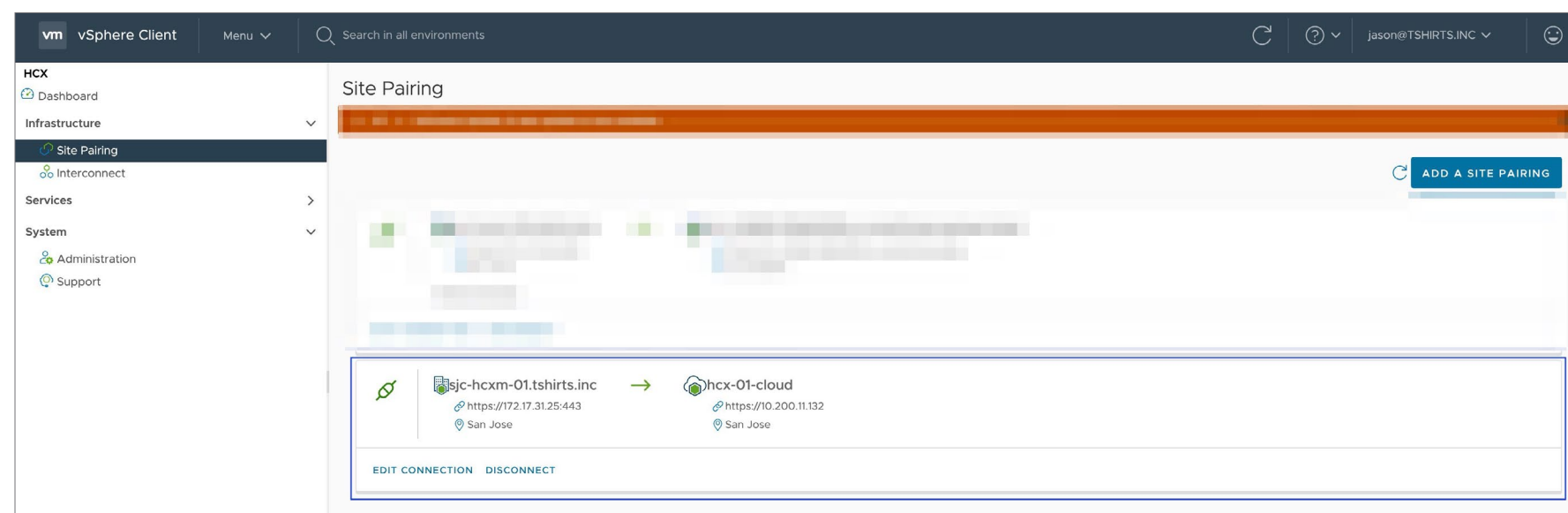

FIGURE 53. Creating a site pairing

Create an HCX service mesh

With the site pairing created, you can now config the service mesh. The service mesh is the deployment of virtual appliances used by HCX at both the source and destination to facilitate the functioning of HCX. If you are not familiar with this process, follow the VMware documentation: *Creating a Service Mesh*
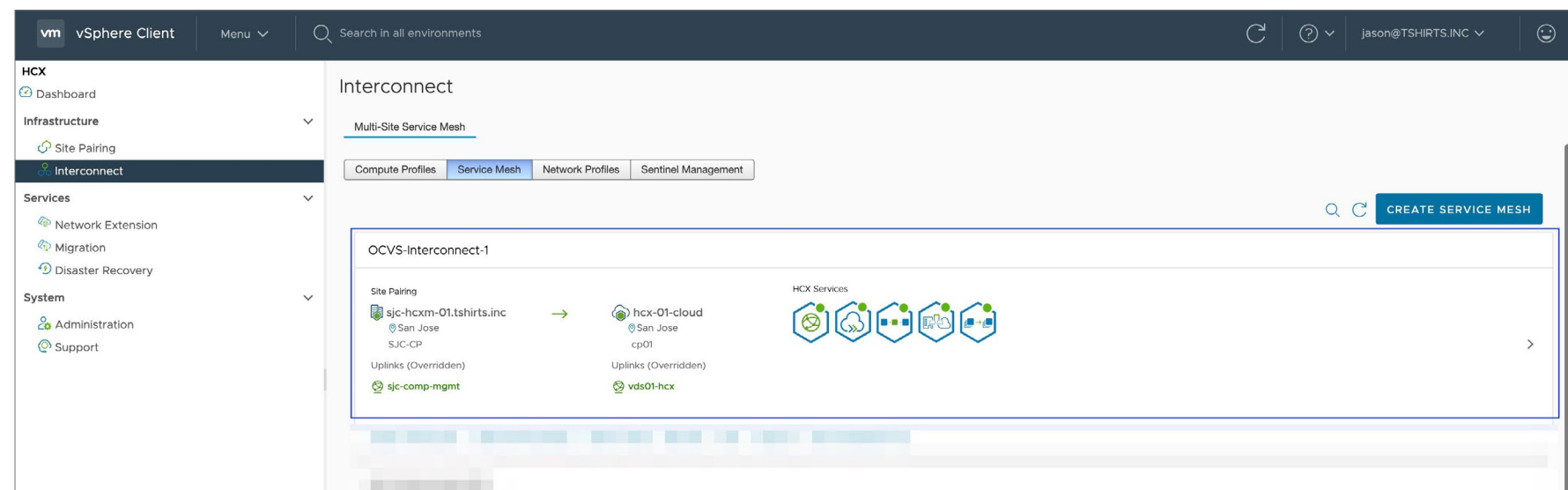

FIGURE 54. Creating a service mesh

Workload migration

Bulk migration

With the site pairing and service mesh configured between your on-premises vSphere environment and Oracle Cloud VMware Solution software-defined datacenter, it's time to start migrating some workloads. This example is a simple bulk migration of a single virtual machine from an on-premises environment to an Oracle Cloud VMware Solution. In a production environment, multiple Virtual machines can be moved at once.

1. In the Software-Defined Datacenter Information section, Copy the **vCenter Client URL**

2. **Open a browser window** either on the Bastion Host or on a machine that has access to the Bastion Host via an SSL Tunnel

3. Paste the **vSphere Client URL** into a new browser tab

4. Copy/Paste the **vCenter Initial Username** and **vCenter Initial password** to log in to vCenter

5. Click Menu in the vSphere client and select **Host and Cluster**

6. Right-click the **Virtual Machine>HCX Actions> Migrate to HCX Target Site** (Figure 55)
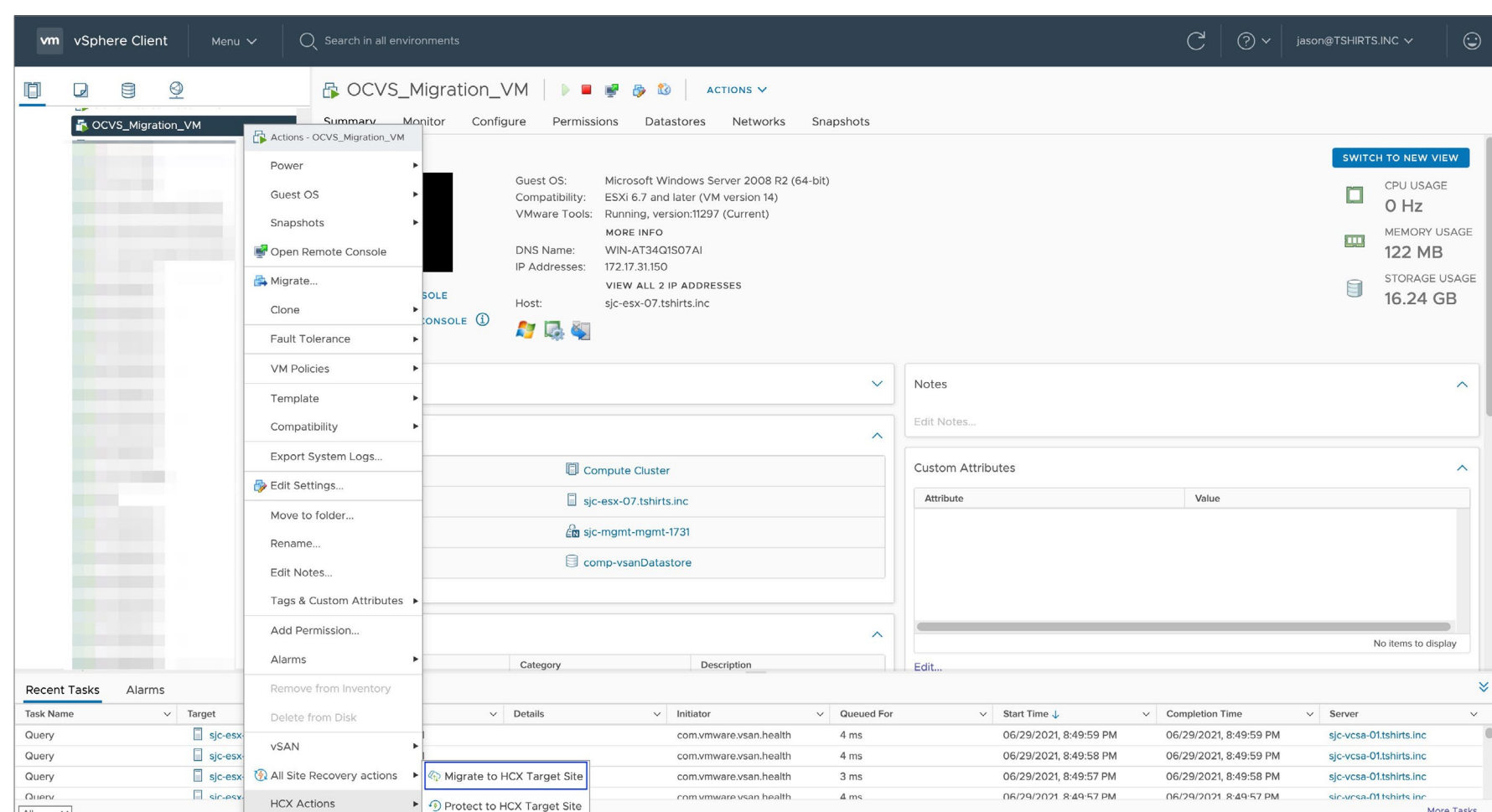

FIGURE 55. Migrate to HCX Target Site

a. **Expand Remote Site Connection** and select the **remote site** (if you only have one site pairing, this step is not required)
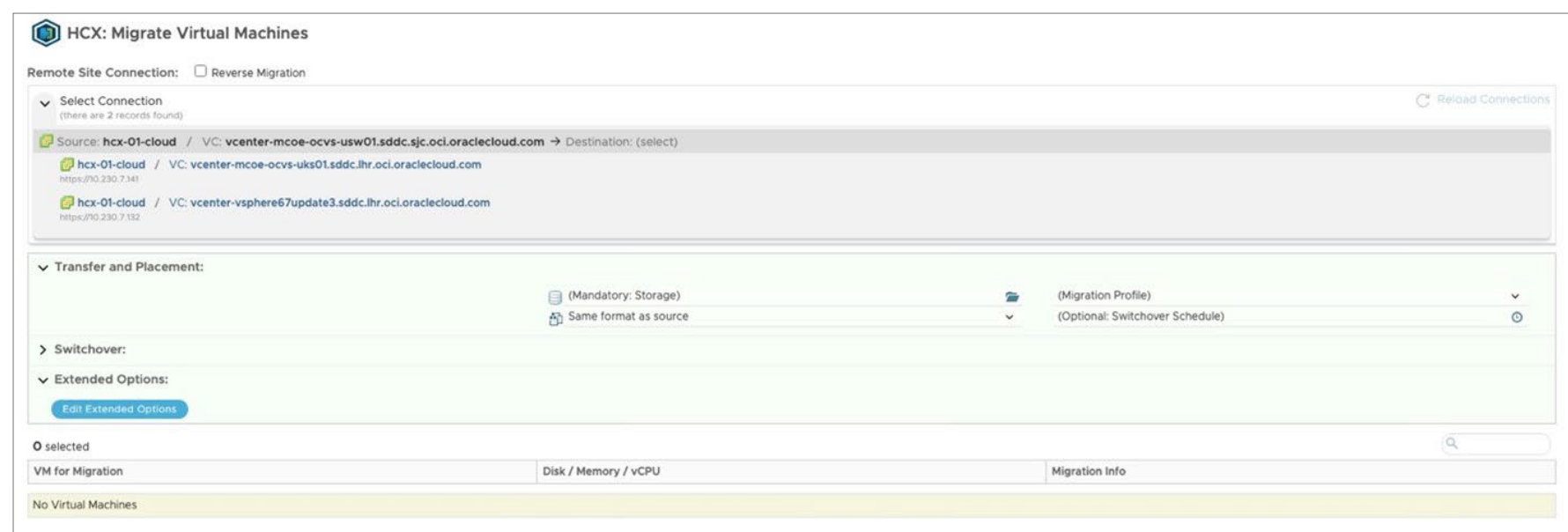

FIGURE 56. Remote Site Connection

b. A new window will appear.
   • Select the VM to be migrated
c. Complete Mandatory Transfer and Placement and VM Migration mandatory fields at a minimum and then select **Validate**. If validation is successful, you can proceed with the migration.
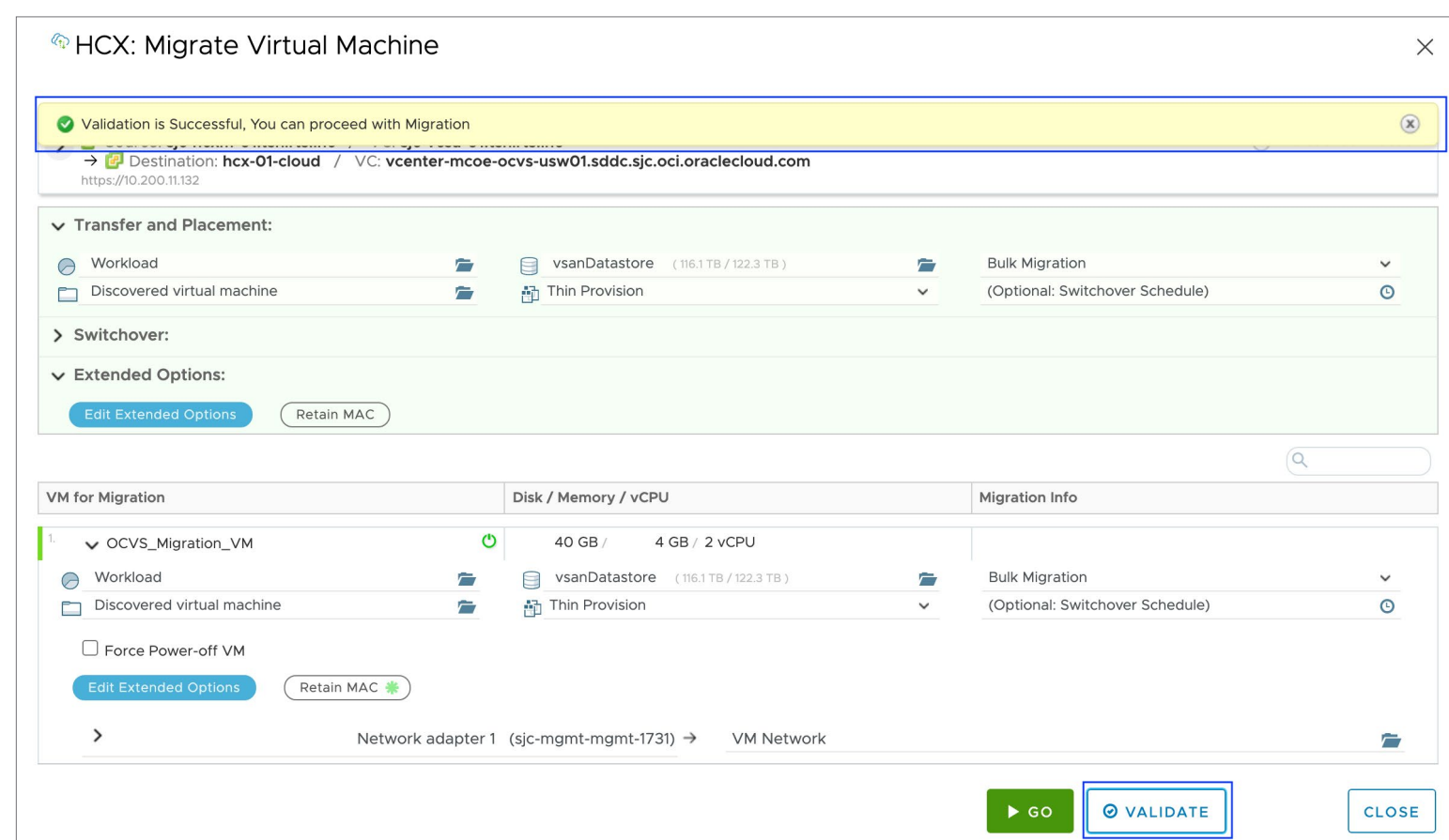

FIGURE 57. Migrate Virtual Machine

The virtual machine data is copied to the remote site. Once the data transfer is complete, the virtual machine is powered off on the on-premises environment and moved into a folder named 'VMs migrated to cloud.' The virtual machine is then added into the inventory of the Oracle Cloud VMware Solution software-defined datacenter and powered on if it was powered on before the migration has been initiated.
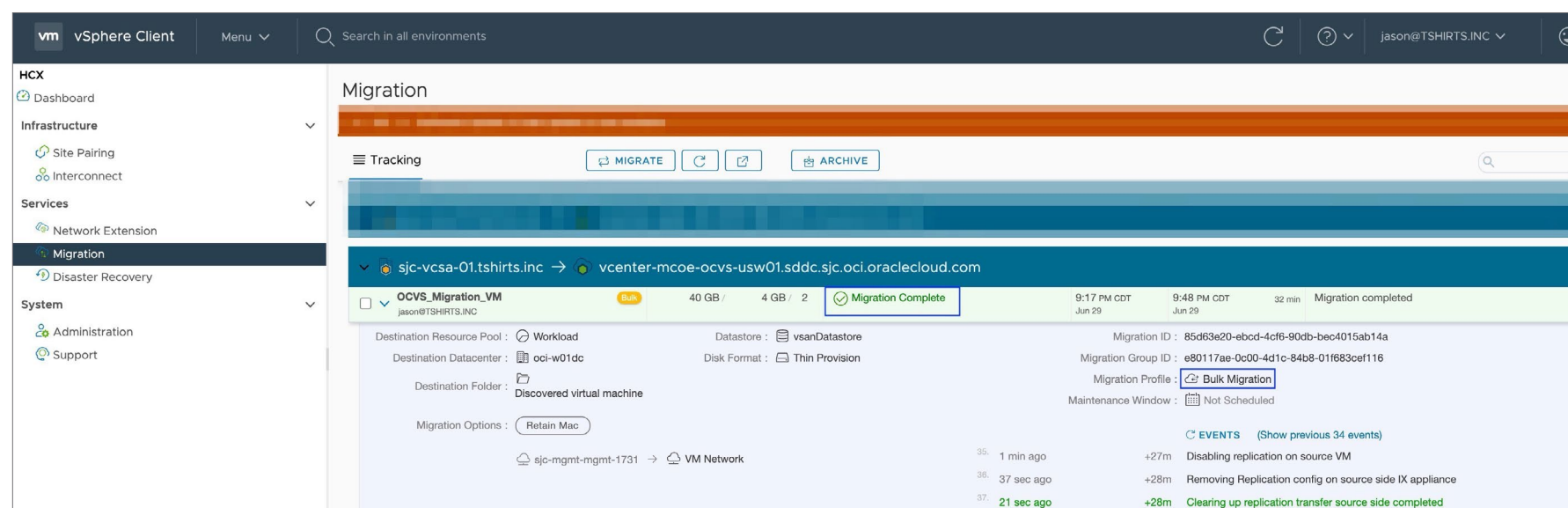

FIGURE 58. Migration complete

Network extension

Before attempting a vMotion of an on-premises virtual machine to the Oracle Cloud VMware Solution SDDC, an extension of the on-premises Network the virtual machine is connected should be completed. An HCX Network Extension, also known as a stretched Layer 2 network, allows extending virtual machine networks to a VMware HCX-enabled remote site. Virtual machines migrated or created on the extended segment at the remote site are on the same Layer 2 network as virtual machines placed on the origin network.

Creating the network extension is a straightforward process performed via the HCX interface.

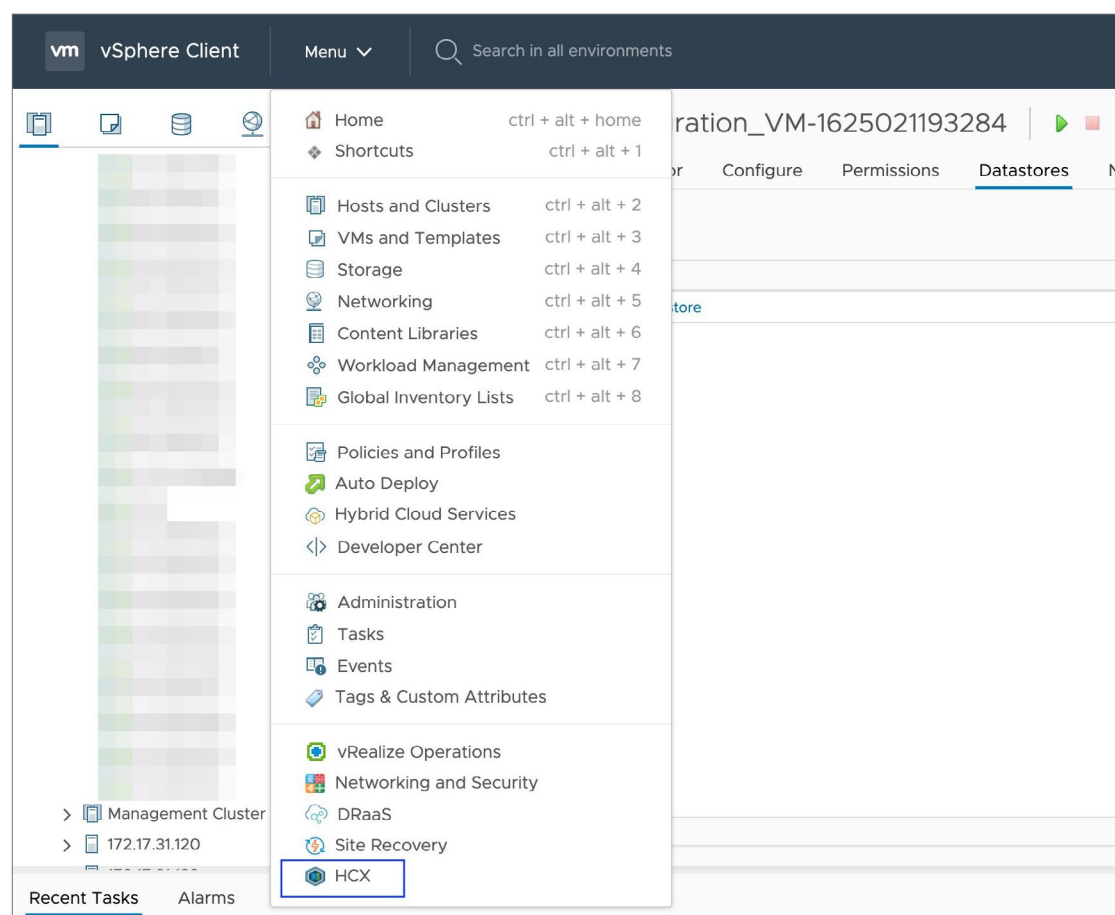1. Click Menu in the vSphere client and select **HCX**

FIGURE 59. Select HCX in vSphere Client

2. In the Services Section on the left, Select **Network Extension**

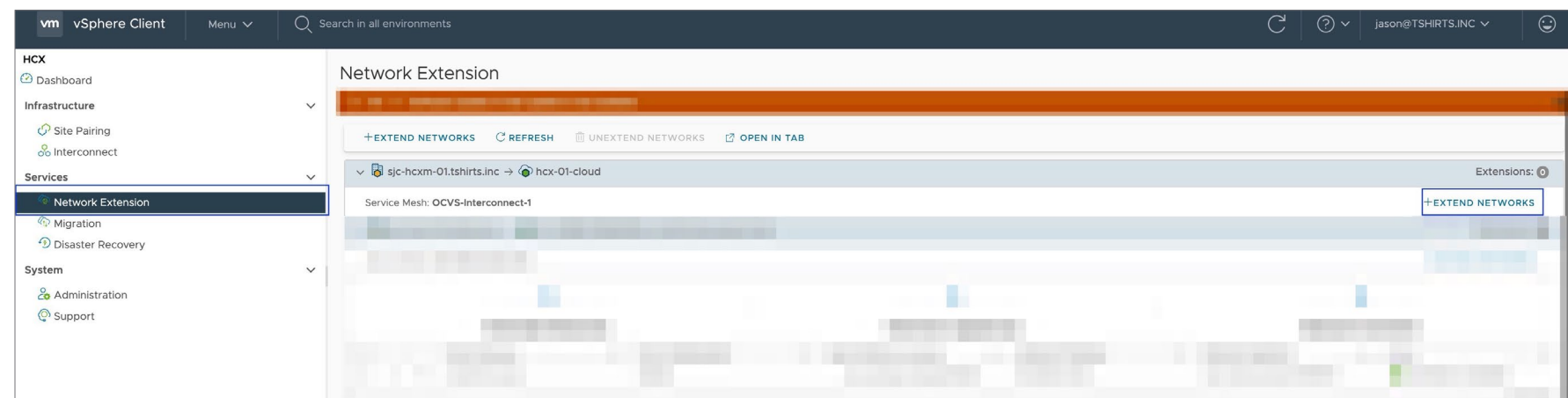3. In the Network Extension Window, Select **Extend Networks**

FIGURE 60. Network extension

    a. Select the **Network** to be extended

    b. Click **Next**

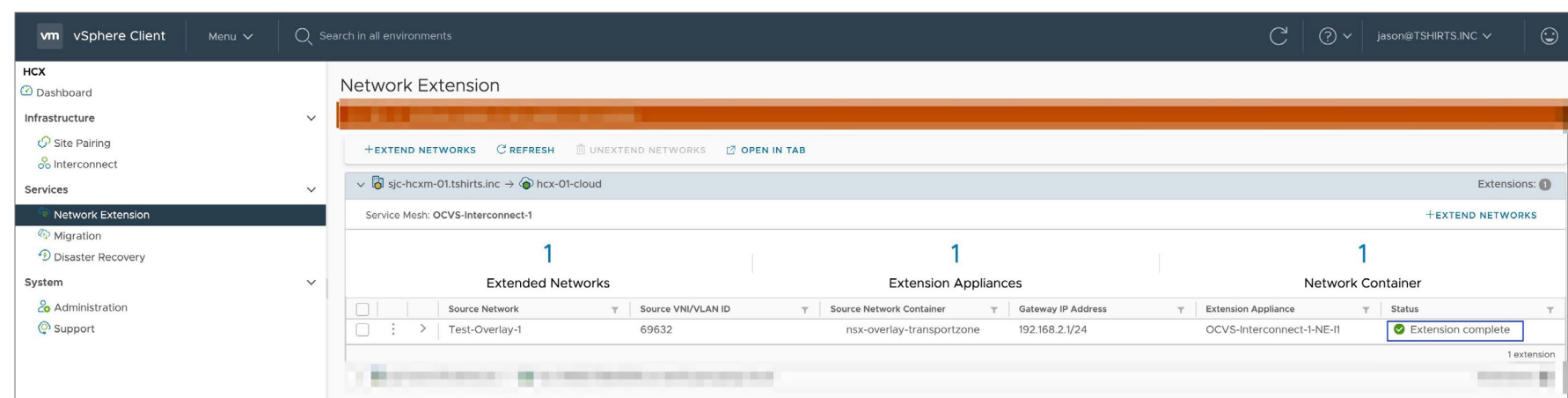   c. Enter **Gateway IP Address** for Network

    d. Click **Submit**

FIGURE 61. Network extension

With the Extended Network in place, the virtual machine to be vMotion to the Oracle Cloud VMware Solution SDDC can be moved. The steps are very similar to Bulk Migration. When selecting the migration profile, select "vMotion," and the destination network for the virtual machine should be the extended Network.
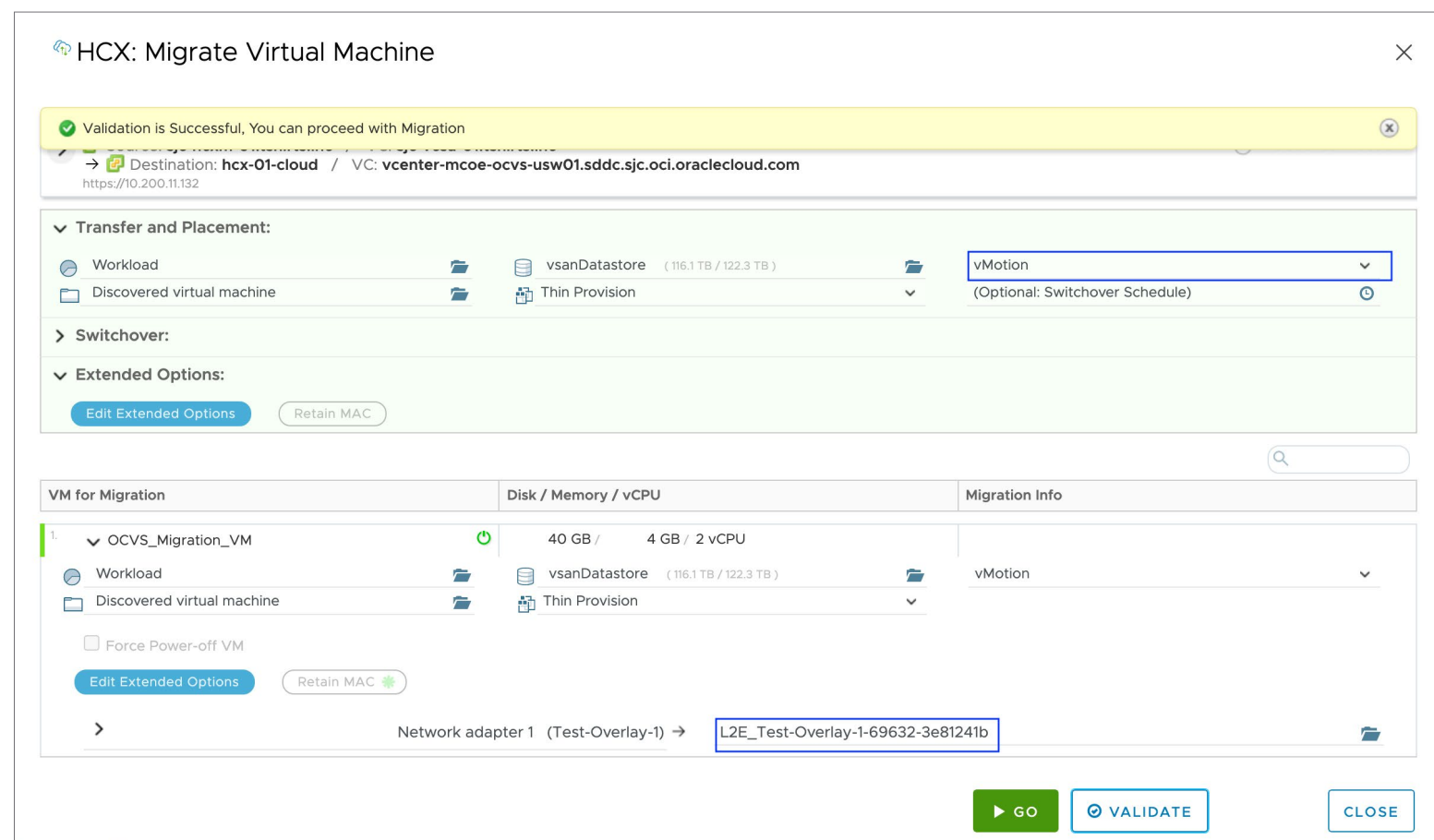

FIGURE 62. HCX: Migrate Virtual Machine

vMotion

Once the Migration plan has been validated, you can begin the replication. After some time, you will start to see the virtual machine being vMotioned into our Oracle Cloud VMware Solution software-defined datacenter.

Now that HCX is configured correctly, you can migrate workloads to and from your Oracle Cloud VMware Solution software-defined datacenter as necessary.

HELPFUL NOTE
Consult the *HCX Configuration Limits* documentation for migration limitations.
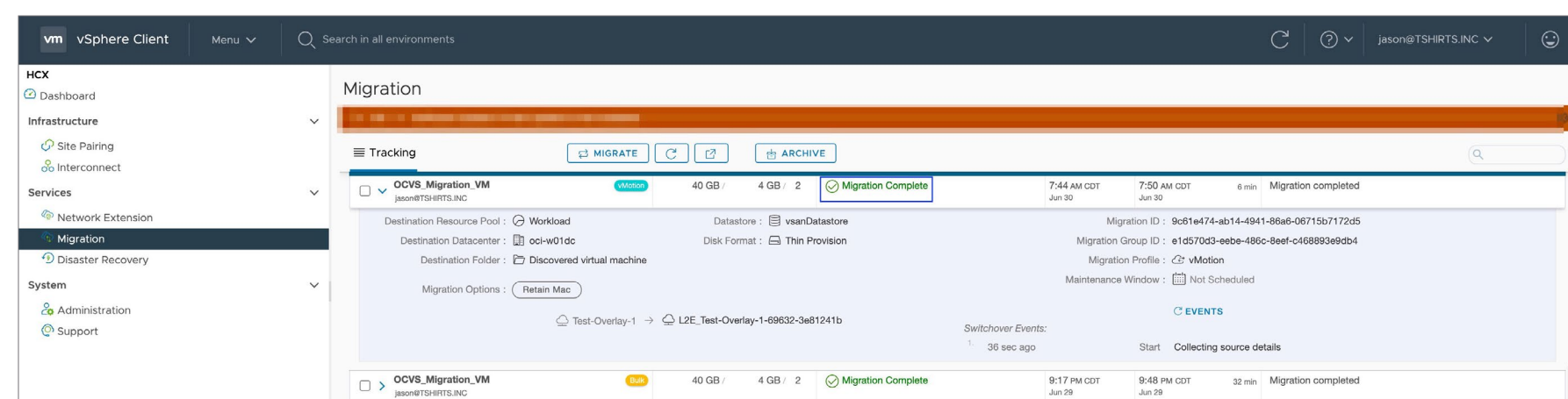

FIGURE 63. vMotion migration

Conclusion

Oracle Cloud VMware Solution accelerates and simplifies an organization's move to the Cloud, allowing the organization to embrace improved agility, scalability, and resiliency.

This eBook is the first step in the journey to Oracle Cloud with Oracle VMware Cloud Solution. To learn more about the solution, please visit our **Oracle Cloud VMware Solution website** or contact one of VMware's Cloud Experts at **OCVSsales@vmware.com**

vmware®