

Deployment

22 AUG 2017

VMware Validated Design 4.1

VMware Validated Design for Management and Workload Consolidation 4.1

You can find the most up-to-date technical documentation on the VMware Web site at:

<https://docs.vmware.com/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2016, 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1	About VMware Validated Design for Consolidated SDDC	5
2	Virtual Infrastructure Implementation for Consolidated SDDC	7
	Install and Configure ESXi Hosts for Consolidated SDDC	7
	Deploy and Configure the vCenter Server Components for Consolidated SDDC	11
	Deploy and Configure Components in the NSX Instance of the Consolidated SDDC	38
	Deploy vSphere Data Protection in the Consolidated SDDC	78
3	Cloud Management Platform Implementation for Consolidated SDDC	89
	Prerequisites for Cloud Management Platform Implementation for Consolidated SDDC	89
	Configure Service Account Privileges for Consolidated SDDC	97
	vRealize Automation Installation for Consolidated SDDC	99
	vRealize Automation Default Tenant Configuration for Consolidated SDDC	122
	vRealize Automation Tenant Creation for Consolidated SDDC	125
	Embedded vRealize Orchestrator Configuration for Consolidated SDDC	135
	Install vRealize Business for Consolidated SDDC	145
	Cloud Management Platform Post-Installation Tasks for Consolidated SDDC	153
	Tenant Content Creation for Consolidated SDDC	155
4	Operations Implementation for Consolidated SDDC	181
	vRealize Operations Manager Implementation for Consolidated SDDC	181
	vRealize Log Insight Implementation for Consolidated SDDC	216
	vSphere Update Manager Download Service Implementation for Consolidated SDDC	253

About VMware Validated Design for Consolidated SDDC

1

VMware Validated Design Deployment for Management and Workload Consolidation (also referred to as the VMware Validated Design for Consolidated SDDC) provides step-by-step instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design for Software-Defined Data Center.

VMware Validated Design Deployment for Management and Workload Consolidation does not contain step-by-step instructions for performing all of the required post-configuration tasks because they often depend on customer requirements.

Intended Audience

The *VMware Validated Design Deployment for Management and Workload Consolidation* document is intended for cloud architects, infrastructure administrators and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

VMware Validated Design Deployment for Management and Workload Consolidation is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Virtual Infrastructure Implementation for Consolidated SDDC

2

The virtual infrastructure is the foundation of an operational SDDC and consists primarily of the physical host's hypervisor and the control of these hypervisors. The management workloads consist of elements in the virtual management layer itself, along with elements in the cloud management layer, service management, business continuity, and security areas.

The following procedures describe the validated flow of installation and configuration for the virtual infrastructure for consolidated SDDC deployments.

Procedure

- 1 [Install and Configure ESXi Hosts for Consolidated SDDC](#) on page 7
Start the deployment of the virtual infrastructure in your consolidated SDDC deployment by installing and configuring all of the ESXi hosts.
- 2 [Deploy and Configure the vCenter Server Components for Consolidated SDDC](#) on page 11
Deploy and configure the vCenter Server and cluster components.
- 3 [Deploy and Configure Components in the NSX Instance of the Consolidated SDDC](#) on page 38
Deploy and configure the NSX instance for the consolidated cluster in your consolidated SDDC deployment.
- 4 [Deploy vSphere Data Protection in the Consolidated SDDC](#) on page 78
Deploy vSphere Data Protection to provide the capability for backup and restore of SDDC management components.

Install and Configure ESXi Hosts for Consolidated SDDC

Start the deployment of the virtual infrastructure in your consolidated SDDC deployment by installing and configuring all of the ESXi hosts.

Procedure

- 1 [Prerequisites for Installation of ESXi Hosts for Consolidated SDDC](#) on page 8
Install and configure the ESXi hosts for your workload and management consolidation deployment.
- 2 [Install ESXi Interactively on All Hosts for Consolidated SDDC](#) on page 8
Install all ESXi hosts for all of the clusters in your consolidated SDDC deployment interactively.
- 3 [Configure the Network on All Hosts for Consolidated SDDC](#) on page 9
After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access for all hosts in the workload and management consolidated pod.

4 [Configure a vSphere Standard Switch on a Host for Consolidated SDDC](#) on page 10

You must perform network configuration from the VMware Host Client for one host. You perform networking configuration for the other hosts after the deployment of the vCenter Server system that manages the hosts.

5 [Configure SSH and NTP on the First Host for Consolidated SDDC](#) on page 11

Time synchronization issues can result in serious problems with your environment. Configure NTP and SSH on the first host in your consolidated pod. NTP and SSH configuration for the other hosts will take place after installation of Virtual Center Server.

Prerequisites for Installation of ESXi Hosts for Consolidated SDDC

Install and configure the ESXi hosts for your workload and management consolidation deployment.

Before you start:

- Make sure that you have a Windows host that has access to your data center. You use this host to connect to your hosts and perform configuration steps.

You must also prepare the installation files.

- Download the ESXi ISO installer.
- Create a bootable USB drive that contains the ESXi Installation. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade" in *vSphere Installation and Setup*.

IP Addresses, Hostnames, and Network Configuration

The following tables contain all the values needed to configure your ESXi hosts.

Table 2-1. Remote Office Hosts

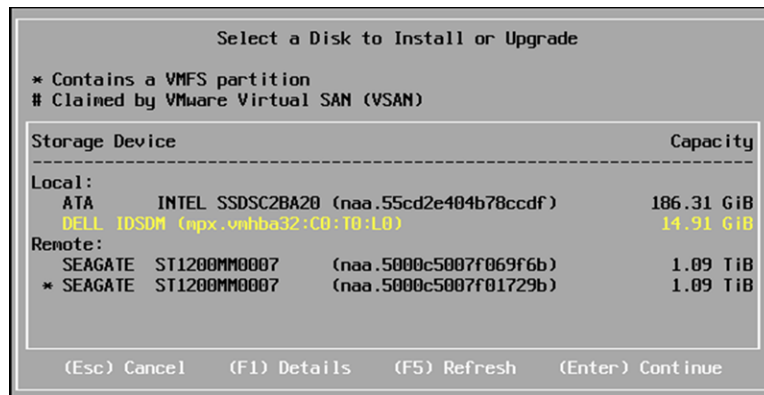
FQDN	IP	Management VLAN	Default Gateway	NTP Server
sfo01w01esx01.sfo01.rainpole.local	172.16.31.101	1631	172.16.31.253	■ ntp.sfo01.rainpole.local
sfo01w01esx02.sfo01.rainpole.local	172.16.31.102	1631	172.16.31.253	■ ntp.sfo01.rainpole.local
sfo01w01esx03.sfo01.rainpole.local	172.16.31.103	1631	172.16.31.253	■ ntp.sfo01.rainpole.local
sfo01w01esx04.sfo01.rainpole.local	172.16.31.104	1631	172.16.31.253	■ ntp.sfo01.rainpole.local

Install ESXi Interactively on All Hosts for Consolidated SDDC

Install all ESXi hosts for all of the clusters in your consolidated SDDC deployment interactively.

Procedure

- 1 Power on the sfo01w01esx01 host.
- 2 Mount the USB drive containing the ESXi ISO file, and boot from that USB drive.
- 3 On the Welcome to the VMware 6.5.0 Installation screen, press Enter to start the installation.
- 4 On the End User License Agreement (EULA) screen, press F11 to accept the EULA.
- 5 On the Select a Disk to Install or Upgrade screen, select the USB drive or SD card under local storage to install ESXi, and press Enter to continue.



- 6 Select the keyboard layout, and press Enter.
- 7 Enter the **esxi_root_user_password**, enter the password a second time to confirm you are typing the correct password, and press Enter.
- 8 On the Confirm Install screen, press F11 to start the installation.
- 9 After the installation has completed unmount the USB drive, and press Enter to reboot the host.
- 10 Repeat this procedure for all hosts in the consolidated pod, using the respective values for each host you configure.

Configure the Network on All Hosts for Consolidated SDDC

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access for all hosts in the workload and management consolidated pod.

Perform the following tasks to configure the host network settings:

- Configure the network adapter (vmk0) and VLAN ID for the Management Network.
- Configure the IP address, subnet mask, gateway, DNS server and host FQDN for the ESXi host.

Repeat this procedure for all hosts in the consolidated pod. Enter the respective values from the prerequisites section for each host that you configure. See [“Prerequisites for Installation of ESXi Hosts for Consolidated SDDC,”](#) on page 8.

Procedure

- 1 Open the DCUI on the physical ESXi host sfo01w01esx01.
 - a Open a console window to the host.
 - b Press F2 to enter the DCUI.
 - c Enter **root** as login name, and **esxi_root_user_password**, and press Enter.
- 2 Configure the network.
 - a Select **Configure Management Network** and press Enter.
 - b Select **VLAN (Optional)** and press Enter.
 - c Enter **1631** as the VLAN ID for the Management Network, and press Enter.
 - d Select **IPv4 Configuration** and press Enter.

- e Configure the IPv4 network using the following settings, and press **Enter**.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.31.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.31.253

- f Select **DNS Configuration** and press **Enter**.

- g Configure the DNS using the following settings, and press **Enter**.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	sfo01w01esx01.sfo01.rainpole.local

- h Select **Custom DNS Suffixes** and press **Enter**.

- i Ensure there are no suffixes listed, and press **Enter**.

- 3 After completing all host network settings press **Escape** to exit, and press **Y** to confirm the changes.
- 4 Repeat this procedure for all hosts in the consolidated SDDC pod.

Configure a vSphere Standard Switch on a Host for Consolidated SDDC

You must perform network configuration from the VMware Host Client for one host. You perform networking configuration for the other hosts after the deployment of the vCenter Server system that manages the hosts.

You configure a vSphere Standard Switch with two port groups:

- The existing virtual machine port group.
- VMkernel port group.

This configuration provides connectivity and common network configuration for virtual machines that reside on each host.

Procedure

- 1 Log in to the vSphere host using the VMware Host Client
 - a Open a Web browser and go to **https://sfo01w01esx01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	esxi_root_user_password

- 2 Click **OK** to Join the Customer Experience Improvement Program.

- 3 Configure a VLAN for the VM Network Portgroup.
 - a In the Navigator, click **Networking**, click the **Port Groups** tab, choose the **VM Network** port group, and click **Edit Settings**.
 - b On the Edit port group - VM Network window, input **1631** for **VLAN ID**, and click **OK**.

Configure SSH and NTP on the First Host for Consolidated SDDC

Time synchronization issues can result in serious problems with your environment. Configure NTP and SSH on the first host in your consolidated pod. NTP and SSH configuration for the other hosts will take place after installation of Virtual Center Server.

Procedure

- 1 Log in to the ESX host `sfo01w01esx01.sfo01.rainpole.local` by using the VMware Host Client.
 - a Open a Web browser and go to `https://sfo01w01esx01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>esxi_root_user_password</i>
- 2 Configure SSH options.
 - a In the Navigator, click **Manage**, click the **Services** tab, select the **TSM-SSH** service, and click the **Actions** menu. Choose **Policy** and click **Start and stop with host**.
 - b Click **Start** to start the service.
- 3 Configure the NTP Daemon (ntpd) options.
 - a In the Navigator, click **Manage**, click the **System** tab, click **Time & date**, and click **Edit Settings**.
 - b In the Edit Time configuration dialog box, select the **Use Network Time Protocol (enable NTP client)** radio button, change the NTP service startup policy to **Start and stop with host**, and enter `ntp.sfo01.rainpole.local` as the NTP server.
 - c Click **Save** to save these changes.
 - d Start the service by clicking **Actions**, hover over **NTP service**, and choose **Start**.

Deploy and Configure the vCenter Server Components for Consolidated SDDC

Deploy and configure the vCenter Server and cluster components.

Procedure

- 1 [Deploy the External Platform Services Controller for Consolidated SDDC](#) on page 13
The Platform Services Controller contains common infrastructure services such as vCenter Single Sign-On (SSO), VMware Certificate Authority (VMCA), licensing, and server reservation and registration services.
- 2 [Join the Platform Services Controller to Active Directory for Consolidated SDDC](#) on page 15
After you have successfully installed the Platform Services Controller, you must add the appliance to your Active Directory domain. After that, add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components.

- 3 [Replace the Platform Services Controller Certificates for Consolidated SDDC](#) on page 16
You replace the machine SSL certificate on the Platform Services Controller with a custom certificate that is signed by a certificate authority.
- 4 [Deploy the vCenter Server Instance for Consolidated SDDC](#) on page 17
You can now install the vCenter Server appliance and configure licensing and security.
- 5 [Set SDDC Deployment Details on vCenter Server for Consolidated SDDC](#) on page 20
Set an identity of your SDDC deployment on vCenter Server in the Consolidated SDDC. You can also use this identity as a label in tools for automated SDDC deployment.
- 6 [Replace the vCenter Server Certificates for Consolidated SDDC](#) on page 20
You replace the machine SSL certificate on vCenter Server with a custom certificate that is signed by a certificate authority.
- 7 [Configure the vSphere Cluster for Consolidated SDDC](#) on page 22
Configure the vSphere cluster for the consolidated SDDC.
- 8 [Create a vSphere Distributed Switch for Consolidated SDDC](#) on page 24
After adding all ESXi hosts to the clusters, you create a vSphere Distributed Switch. You will also create port groups to prepare your environment to migrate the vCenter Server instance to the distributed switch.
- 9 [Create vSAN Disk Groups for Consolidated SDDC](#) on page 28
vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.
- 10 [Enable vSphere HA for Consolidated SDDC](#) on page 29
Before creating the host profile for the management cluster, enable vSphere HA for the consolidated cluster.
- 11 [Change Advanced Options on the ESXi Hosts for Consolidated SDDC](#) on page 30
Change the default ESX Admins group to achieve greater levels of security, and enable vSAN to provision the Virtual Machine Swap files as thin to save space in the vSAN datastore.
- 12 [Mount NFS Storage for Consolidated SDDC](#) on page 31
You must mount an NFS datastore where vSphere Data Protection will later be deployed.
- 13 [Create and Apply the Host Profile for Consolidated SDDC](#) on page 31
Host Profiles ensure all hosts in the cluster have the same configuration.
- 14 [Set vSAN Policy on Management Virtual Machines for Consolidated SDDC](#) on page 34
After you apply the host profile to all the hosts, set the storage policy of the vCenter Server and the Platform Services Controller to the vSAN Default Storage Policy.
- 15 [Create the VM and Template Folders for Consolidated SDDC](#) on page 35
Create folders to group objects of the same type for easier management.
- 16 [Create VM Groups to Define the Startup Order for Consolidated SDDC](#) on page 36
VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.
- 17 [Create Host Groups to Keep vCenter and the Platform Services Controller on Specific Hosts for Consolidated SDDC](#) on page 37
Create a rule that keeps vCenter Server and the Platform Services Controller on the first four hosts so they are easy to locate in the event of an outage.

Deploy the External Platform Services Controller for Consolidated SDDC

The Platform Services Controller contains common infrastructure services such as vCenter Single Sign-On (SSO), VMware Certificate Authority (VMCA), licensing, and server reservation and registration services.

Procedure

- 1 Log in to the Windows host that has access to your data center as an administrator.
- 2 Start the vCenter Server Appliance Installer wizard.
 - a Browse to the vCenter Server Appliance ISO file.
 - b Open the <dvd-drive>:\vcsa-ui-installer\win32\Installer.exe application file.
- 3 Complete Stage 1 of the vCenter Server Appliance Deployment wizard.
 - a Click **Install** to start the installation.
 - b Click **Next** on the Introduction page.
 - c On the End User License Agreement page, select the **I accept the terms of the license agreement** check box, and click **Next**.
 - d On the Select deployment type page, click **Platform Services Controller** and click **Next**.
 - e On the Appliance deployment target page, enter the following settings and click **Next**.

Setting	Value
ESXi host or vCenter Server name	sfo01w01esx01.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	<i>esxi_root_user_password</i>

- f In the Certificate Warning dialog box, click **Yes** to accept the host certificate.
- g On the Set up appliance VM page, enter the following settings, and click **Next**.

Setting	Value
VM name	sfo01w01psc01
Root password	<i>psc_root_password</i>
Confirm root password	<i>psc_root_password</i>

- h On the Select datastore page, select **Install on a new Virtual SAN datastore on the target host**, and click **Next**.
- i Confirm at least one **Cache tier** and two **Capacity tier** disks have been claimed, select **Enable Thin Disk Mode**, and click **Next**.

- j On the Configure network settings page, enter the following settings and click **Next**.

Setting	Value
Network	VM Network
IP version	IPv4
IP assignment	static
System name	sfo01w01psc01.sfo01.rainpole.local
IP address	172.16.11.63
Subnet mask or prefix length	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4

- k On the Ready to complete stage 1 page, review the configuration and click **Finish** to start the deployment.
- l When the deployment completes, click **Continue** to proceed to second stage of the installation, setting up the Platform Services Controller Appliance.
- 4 Complete Stage 2 of the Set Up Platform Services Controller Appliance wizard.
- a Click **Next** on the Introduction page.
- b On the Appliance configuration page, enter the following settings and click **Next**.

Setting	Value
Time synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.sfo01.rainpole.local
SSH access	Enabled

- c On the SSO configuration page, enter the following settings, and click **Next**.

Setting	Value
SSO configuration	Create a new SSO domain
SSO domain name	vsphere.local
SSO password	<i>sso_password</i>
Confirm password	<i>sso_password</i>
Site name	SFO01

- d On the Configure CEIP page, verify that the **Join the VMware's Customer Experience Improvement Program (CEIP)** check box is checked and click **Next**.
- e On the Ready to complete page, review the configuration and click **Finish** to complete the setup.
- f Click **OK** on the Warning dialog box.

Join the Platform Services Controller to Active Directory for Consolidated SDDC

After you have successfully installed the Platform Services Controller, you must add the appliance to your Active Directory domain. After that, add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components.

Procedure

- 1 Log in to the Platform Services Controller administration interface.
 - a Open a Web browser and go to **https://sfo01w01psc01.sfo01.rainpole.local**.
 - b Click the link for **Platform Services Controller web interface**.
 - c Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add the Platform Services Controller instance to the Active Directory domain.
 - a In the Navigator, click **Appliance Settings**, click the **Manage** tab, and click **Join**.
 - b In the Join Active Directory Domain dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	sfo01.rainpole.local
User name	ad_admin_acct@sfo01.rainpole.local
Password	ad_admin_password

- 3 Reboot the Platform Services Controller instance to apply the changes
 - a Click the **Appliance settings** tab, and click the **VMware Platform Services Appliance** link.
 - b Log in to the VMware vCenter Server Appliance administration interface with the following credentials.

Setting	Value
User name	root
Password	psc_root_password

- c On the Summary page, click **Reboot**.
 - d In the System Reboot dialog box, click **Yes**.
 - e Wait for the reboot process to finish.
- 4 After the reboot process finishes, log in to **https://sfo01w01psc01.sfo01.rainpole.local** again using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 5 Verify that the Platform Services Controller has successfully joined the domain, click **Appliance Settings** and click the **Manage** tab.
- 6 Add Active Directory as a vCenter Single Sign-On identity source.

- a In the Navigator, click **Configuration** and click the **Identity Sources** tab.
- b Click the **Add** icon to add a new identity source.
- c In the Add Identity Source dialog box, select the following settings and click **OK**.

Setting	Value
Identity source type	Active Directory (Integrated Windows Authentication)
Domain name	SFO01.RAINPOLE.LOCAL
Use machine account	Selected

- d Under Identity Sources, select the **rainpole.local** identity source and click **Set as Default Domain** to make rainpole.local the default domain.
- e In the confirmation dialog box, click **Yes**.

Replace the Platform Services Controller Certificates for Consolidated SDDC

You replace the machine SSL certificate on the Platform Services Controller with a custom certificate that is signed by a certificate authority.

Table 2-2. Certificate-Related Files on Platform Services Controller

Platform Services Controller	Certificate File Name
sfo01w01psc01.sfo01.rainpole.local	<ul style="list-style-type: none"> ■ sfo01w01psc01.sfo01.1.cer ■ sfo01w01psc01.sfo01.key ■ Root64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (CertGenVVD). See the *VMware Validated Design Planning and Preparation* documentation.
- A Windows host with an SSH terminal access software such as PuTTY and an scp software such as WinSCP installed.

Procedure

- 1 Change the Platform Services Controller command shell to the Bash shell to allow secure copy (scp) connections.
 - a Open an SSH connection to sfo01w01psc01.sfo01.rainpole.local and log in using the following credentials.

Setting	Value
Username	root
Password	psc_root_password

- b Run the following commands to enable Bash shell access for the root user.

```
shell
chsh -s "/bin/bash" root
```

- 2 Copy the generated certificates to the Platform Services Controller.
 - a Run the following command to create a new temporary folder.


```
mkdir -p /root/certs
```
 - b Copy the certificate files `sfo01w01psc01.sfo01.1.cer`, `sfo01w01psc01.sfo01.key` and `Root64.cer` to the `/root/certs` folder.

You can use an scp software like WinSCP.
- 3 Replace the certificate on the Platform Services Controller.
 - a Start the vSphere Certificate Manager utility on the Platform Services Controller.


```
/usr/lib/vmware-vmca/bin/certificate-manager
```
 - b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**.
 - c Enter the default vCenter Single Sign-On user name `administrator@vsphere.local` and the `vsphere_admin` password.
 - d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.
 - e When prompted for the custom certificate, enter `/tmp/certs/sfo01w01psc01.sfo01.1.cer`.
 - f When prompted for the custom key, enter `/tmp/certs/sfo01w01psc01.sfo01.key`.
 - g When prompted for the signing certificate, enter `/tmp/certs/Root64.cer`.
 - h When prompted to continue operation, enter `Y`.

The Platform Services Controller services restart automatically.
- 4 After Certificate Manager replaces the certificates, run the following commands to restart the vami-httpd service and to remove certificate files.


```
service vami-httpd restart
cd /root/certs
rm sfo01psc01.1.cer sfo01psc01.key Root64.cer
```
- 5 Verify that the certificates have been updated.

Deploy the vCenter Server Instance for Consolidated SDDC

You can now install the vCenter Server appliance and configure licensing and security.

Procedure

- 1 Start the vCenter Server Appliance Installer wizard.
 - a Browse to the vCenter Server Appliance ISO file.
 - b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer` application file.
- 2 Complete the vCenter Server Appliance 6.5 Installer wizard.
 - a Click **Install** to start the installation.
 - b Click **Next** on the Introduction page.
 - c On the End User License Agreement page, select the **I accept the terms of the license agreement** check box and click **Next**.
 - d On the Select deployment type page, under **External Platform Services Controller**, verify that the **vCenter Server(Requires External Platform Services Controller)** radio button is selected, and click **Next**.

- e On the Appliance deployment target page, enter the following settings and click **Next**.

Setting	Value
ESXi host or vCenter Server name	sfo01w01esx01.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	<i>esxi_root_password</i>

- f In the Certificate Warning dialog box, click **Yes** to accept the host certificate.

- g On the Set up appliance VM page, enter the following settings and click **Next**.

Setting	Value
VM name	sfo01w01vc01
Root password	<i>vc_root_password</i>
Confirm root password	<i>vc_root_password</i>

- h On the Select deployment size page, select **Small** Deployment size and click **Next**.

- i On the Select datastore page, select the **vsanDatastore** datastore, select the **Enable Thin Disk Mode** check box, enter **sfo01-w01dc** for the **Datacenter Name**, **sfo01-w01-consolidated01** for the **Cluster Name**, and click **Next**.

- j On the Configure network settings page, enter the following settings and click **Next**.

Setting	Value
Network	VM Network
IP version	IPv4
IP assignment	static
System name	sfo01w01vc01.sfo01.rainpole.local
IP address	172.16.11.64
Subnet mask or prefix length	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4

- k On the Ready to complete stage 1 page, review the configuration and click **Finish** to start the deployment.

- l Once the deployment completes, click **Continue** to proceed to stage 2 of the installation.

3 Install - Stage 2: Complete the Set Up vCenter Server Appliance wizard.

- a Click **Next** on the Introduction page.

- b On the Appliance configuration page, enter the following settings and click **Next**.

Setting	Value
Time Synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.sfo01.rainpole.local
SSH access	Enabled

- c On the SSO configuration page, enter the following settings and click **Next**.

Setting	Value
Platform Services Controller	sfo01w01psc01.sfo01.rainpole.local
HTTPS port	443
Single Sign-On domain name	vsphere.local
Single Sign-On user name	administrator
Single Sign-On password	<i>vsphere_admin_password</i>

- d On the Ready to complete page, review the configuration and click **Finish**.
- e Click **OK** on the Warning dialog box.
- f Once the set up completes, click **Close** to shut down the wizard.
- 4 Once the appliance has completed rebooting, log in to vCenter Server.
- a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 5 Add new licenses for this vCenter Server instance and the ESXi hosts, if needed.
- a Click the **Home** icon above the Navigator and choose the **Administration** menu item.
- b On the Administration page, click **Licenses** and click the **Licenses** tab.
- c Click the **Create New Licenses** icon to add license keys.
- d On the Enter license keys page, enter license keys for vCenter Server, ESXi and vSAN, one per line and click **Next**.
- e On the Edit license name page, enter a descriptive name for each license key and click **Next**.
- f On the Ready to complete page, review your entries and click **Finish**.
- 6 Assign the newly added licenses to the respective assets.
- a Click the **Assets** tab.
- b Select the vCenter Server instance, and click the **Assign License** icon.
- c Select the vCenter Server license that you entered in the previous step, and click **OK**.
- 7 Assign the vCenterAdmins domain group to the vCenter Server Administrator role.
- a In the Navigator, click **Administration**.
- b In the Administration window, click **Global Permissions**.
- c In the Global Permissions box, click the **Manage** tab, then click the **Add permission** button.
- d In the Global Permissions Root - Add Permissions window, click the **Add** button.
- e Select **sfo01.rainpole.local** from the **Domain** drop down list.
- f Enter **vCenterAdmins** in the **Search** field and press **Enter**.

- g Select the **vCenterAdmins** group, click the **Add** button, and then click **OK**.
- h Ensure **Administrator** is selected and the **Propagate to Children** check box is selected under Assigned Role and click **OK**.

Set SDDC Deployment Details on vCenter Server for Consolidated SDDC

Set an identity of your SDDC deployment on vCenter Server in the Consolidated SDDC. You can also use this identity as a label in tools for automated SDDC deployment.

Procedure

- 1 Log in to the Consolidated vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.
- 3 In the Navigator, click **vCenter Servers** under Resources.
- 4 Click the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.
- 5 Under the Settings pane, click **Advanced Settings** and click the **Edit** button.
- 6 In the Edit Advanced vCenter Server Settings dialog box, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Consolidated
config.SDDC.Deployed.Version	4.1.0
config.SDDC.Deployed.Method	DIY

- 7 Click **OK** to close the window.

Replace the vCenter Server Certificates for Consolidated SDDC

You replace the machine SSL certificate on vCenter Server with a custom certificate that is signed by a certificate authority.

Table 2-3. Certificate-Related Files on the vCenter Server Instance

vCenter Server FQDN	Files for Certificate Replacement
sfo01w01vc01.sfo01.rainpole.local	<ul style="list-style-type: none"> ■ sfo01w01vc01.sfo01.key ■ sfo01w01vc01.sfo01.1.cer ■ Root64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (CertGenVVD). See the *VMware Validated Design Planning and Preparation* documentation.

- A Windows host with an SSH terminal access software such as PuTTY and an scp software such as WinSCP installed.

Procedure

- 1 Change the vCenter Server appliance command shell to the Bash shell to allow secure copy (scp) connections.
 - a Open an SSH connection to sfo01w01vc01.sfo01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	vcenter_server_root_password
 - c Run the following commands to enable Bash shell access for the root user.


```
shell
chsh -s "/bin/bash" root
```
- 2 Copy the generated certificates to the vCenter Server Appliance.
 - a Run the following command to create a new temporary folder.


```
mkdir -p /root/certs
```
 - b Copy the certificate files sfo01w01vc01.1.cer, sfo01w01vc01.key and Root64.cer to the /root/certs folder.

You can use an scp software such as WinSCP.
- 3 Replace the certificate on the vCenter Server instance.
 - a Start the vSphere Certificate Manager utility on the vCenter Server instance.


```
/usr/lib/vmware-vmca/bin/certificate-manager
```
 - b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**, enter the default vCenter Single Sign-On user name **administrator@vsphere.local** and the **vsphere_admin_password** password.
 - c When prompted for the Infrastructure Server IP, enter the IP address of the Platform Services Controller **172.16.11.63**.
 - d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.
 - e When prompted for the custom certificate, enter **/tmp/certs/sfo01w01vc01.sfo01.1.cer**.
 - f When prompted for the custom key, enter **/tmp/certs/sfo01w01vc01.sfo01.key**.
 - g When prompted for the signing certificate, enter **/tmp/certs/Root64.cer**.
 - h When prompted to Continue operation, enter **Y**.
- 4 After Status shows 100% Completed, wait several minutes until all vCenter Server services are restarted.
- 5 Run the following commands to restart the vami-lighttpd service and to remove certificate files.


```
service vami-lighttpd restart
cd /root/certs/
rm sfo01w01vc01.1.cer sfo01w01vc01.key Root64.cer
```

Configure the vSphere Cluster for Consolidated SDDC

Configure the vSphere cluster for the consolidated SDDC.

To configure the vSphere cluster, you complete the following configuration tasks:

- Enable DRS.
- Enable EVC.
- Add the hosts to the cluster.
- Add a host to the active directory domain.
- Rename the vSAN datastore.
- Create, configure, and populate resource pools.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Enable vSphere DRS.
 - a Expand the **sfo01-w01dc** Datacenter object.
 - b Click the **sfo01-w01-consolidated01** cluster object then click the **Configure** tab.
 - c Select the vSphere DRS page, and click **Edit**.
 - d Select the **Turn On vSphere DRS** checkbox then click **OK**.
- 3 Enable VMware EVC.
 - a Select the VMware EVC page, and click **Edit**.
 - b Set EVC mode to the highest available setting supported for the hosts in the cluster, and click **OK**.
- 4 Add a host to the cluster.
 - a Right-click the **sfo01-w01-consolidated01** cluster, and click **Add Host**.
 - b On the Name and location page, enter **sfo01w01esx01.sfo01.rainpole.local** in the **Host name or IP address** text box and click **Next**.
 - c On the Connection settings page, enter the following credentials and click **Next**.

Setting	Value
User name	root
Password	esxi_root_user_password

- d In the Security Alert dialog box, click **Yes**.
- e On the Host summary page, review the host information and click **Next**.
- f On the Assign license page, select the ESXi license key that you entered during the vCenter Server deployment and click **Next**.

- g On the Lockdown Mode page, click **Next**.
 - h On the Resource pool page, click **Next**.
 - i On the Ready to complete page, review your entries and click **Finish**.
- 5 Repeat the previous step for the three remaining hosts to add them to the cluster.

Setting	Value
Host 2	sfo01w01esx02.sfo01.rainpole.local
Host 3	sfo01w01esx03.sfo01.rainpole.local
Host 4	sfo01w01esx04.sfo01.rainpole.local

- 6 Add an ESXi host to the active directory domain.
- a In the Navigator, click **Hosts and Clusters** and expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Select the **sfo01w01esx01.sfo01.rainpole.local** host.
 - c Click the **Configure** tab.
 - d Under System, select **Authentication Services**.
 - e In the Authentication Services panel, click the **Join Domain** button.
 - f In the Join Domain dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	sfo01.rainpole.local
Using credentials	Selected
User name	ad_admin_acct@sfo01.rainpole.local
Password	ad_admin_password

- 7 Set the Active Directory Service to Start and stop with host.
- a In the Navigator, click **Hosts and Clusters** and expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Select the **sfo01w01esx01.sfo01.rainpole.local** host.
 - c Click the **Configure** tab.
 - d Under System, select **Security Profile**.
 - e Click the **Edit** button next to Services.
 - f Select the **Active Directory** service and change the **Startup Policy** to **Start** and stop with host and click **OK**.
- 8 Rename the vSAN datastore.
- a Select the **sfo01-w01-consolidated01** cluster.
 - b Click the **Datastores** tab.
 - c Select **vsanDatastore**, and select **Actions > Rename..**
 - d In the Datastore - Rename dialog box, enter **sfo01-w01-vsan01** as the datastore name, and click **OK**.

- 9 Configure resource pools for the consolidated cluster.
 - a Right-click the **sfo01-w01-consolidated01** cluster and select **New Resource Pool**.
 - b In the New Resource Pool dialog box, enter the following values and click **OK**.
 - c Repeat for each of the resource pools needed.

Setting	Resource Pool 1	Resource Pool 2	Resource Pool 3	Resource Pool 4
Name	sfo01-w01rp-sddc-mgmt	sfo01-w01rp-sddc-edge	sfo01-w01rp-user-edge	sfo01-w01rp-user-vm
CPU-Shares	High	High	Normal	Normal
CPU-Reservation	0	0	0	0
CPU-Reservation Type	Expandable selected	Expandable selected	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited	Unlimited	Unlimited
Memory-Shares	Normal	Normal	Normal	Normal
Memory-Reservation	146 GB	17 GB	0	0
Memory-Reservation Type	Expandable selected	Expandable selected	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited	Unlimited	Unlimited

- 10 Move the vCenter Server and Platform Services Controller to the sfo01-w01rp-sddc-mgmt resource pool.
 - a In the Navigator, click **Hosts and Clusters** and expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Select **sfo01w01vc01** and drag it to the **sfo01-w01rp-sddc-mgmt** resource pool.
 - c Select **sfo01w01psc01** and drag it to the **sfo01-w01rp-sddc-mgmt** resource pool.

Create a vSphere Distributed Switch for Consolidated SDDC

After adding all ESXi hosts to the clusters, you create a vSphere Distributed Switch. You will also create port groups to prepare your environment to migrate the vCenter Server instance to the distributed switch.

Procedure

- 1 Login to the vCenter Server by using the vSphere Web Client.
 - a Open a web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 Create vSphere Distributed Virtual Switch.
 - a In the Navigator, click **Networking** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Right-click the **sfo01-w01dc** datacenter, and select **Distributed Switch > New Distributed Switch** to start the New Distributed Switch wizard .
 - c On the Name and location page, enter **sfo01-w01-vds01** as the name and click **Next**.

- d On the Select version page, ensure the **Distributed switch: 6.5.0** radio button is selected and click **Next**.
- e On the Edit settings page, enter the following values and click **Next**.

Setting	Value
Number of uplinks	2
Network I/O Control	Enabled
Create a default port group	Deselected

- f On the Ready to complete page, review your entries and click **Finish**.
- 3 Edit the settings of the sfo01-w01-vds01 distributed switch.
 - a Right-click the **sfo01-w01-vds01** distributed switch, and select **Settings > Edit Settings**.
 - b Click the **Advanced** tab.
 - c Enter **9000** as MTU (Bytes) value, and click **OK**.
 - 4 Create port groups in the sfo01-w01-vds01 distributed switch for the management traffic types.
 - a Right-click the **sfo01-w01-vds01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.
 - b Create port groups with the following settings and click **Next**.

Port Group Name	Port Binding	VLAN Type	VLAN ID
sfo01-w01-vds01-management	Ephemeral - no binding	VLAN	1631
sfo01-w01-vds01-management-vm	Ephemeral - no binding	VLAN	1611
sfo01-w01-vds01-vMotion	Static binding	VLAN	1632
sfo01-w01-vds01-vSAN	Static binding	VLAN	1633
sfo01-w01-vds01-uplink01	Static binding	VLAN	1635
sfo01-w01-vds01-uplink02	Static binding	VLAN	2713

NOTE The port group for VXLAN traffic is automatically created later during the configuration of the NSX Manager.

- c On the Ready to complete page, review your entries, and click **Finish**.
 - d Repeat this step for each port group.
- 5 Change the port groups to use the Route Based on Physical NIC Load teaming algorithm.
 - a Right-click the **sfo01-w01-vds01** distributed switch and select **Distributed Port Group > Manage Distributed Port Groups**.
 - b On the Select port group policies page, select **Teaming and failover** and click **Next**.
 - c Click the **Select distributed port groups** button, add all port groups and click **Next**.
 - d On the Teaming and failover page, select **Route based on physical NIC load** from the **Load balancing** drop-down menu and click **Next**.
 - e Click **Finish**.

- 6 Connect the ESXi host, `sfo01w01esx01.sfo01.rainpole.local`, to the `sfo01-w01-vds01` distributed switch by migrating its VMkernel and virtual machine network adapters.
 - a Right-click the **sfo01-w01-vds01** distributed switch, and click **Add and Manage Hosts**.
 - b On the Select task page, select **Add hosts** and click **Next**.
 - c On the Select hosts page, click **New hosts**.
 - d In the Select new hosts dialog box, select **sfo01w01esx01.sfo01.rainpole.local** and click **OK**.
 - e On the Select hosts page, click **Next**.
 - f On the Select network adapter tasks page, ensure that **Manage physical adapters** and **Manage VMkernel adapters** check boxes are selected, and click **Next**.
 - g On the Manage physical network adapters page, click **vmnic1** and click **Assign uplink**.
 - h In the Select an Uplink for vmnic1 dialog box, select **Uplink 1** and click **OK**.
 - i On the Manage physical network adapters page, click **Next**.
- 7 Configure the VMkernel ports.
 - a On the Manage VMkernel network adapters page, click **vmk0** and click **Assign port group**.
 - b Select **sfo01-w01-vds01-management** and click **OK**.
 - c On the Manage VMkernel network adapters page, click **On this switch** and click **New adapter**.
 - d On the Add Networking page, select **Select an existing network**, browse to select the **sfo01-w01-vds01-vSAN** port group, click **OK**, and click **Next**.
 - e On the Port properties page, select the **vSAN** check box and click **Next**.
 - f On the IPv4 settings page, select **Use static IPv4 settings**, enter the IP address **172.16.33.101**, enter the subnet **255.255.255.0**, and click **Next**.
 - g Click **Finish**.
 - h On the Analyze impact page, click **Next**.
 - i On the Ready to complete page, review your entries and click **Finish**.
- 8 Create the vMotion VMkernel adapter.
 - a In the Navigator, click **Host and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Click **sfo01w01esx01.sfo01.rainpole.local**.
 - c Click the **Configure** tab then select **VMkernel adapters**.
 - d Click the **Add host networking** icon, select **VMkernel Netowrk Adapter**, and click **Next**.
 - e On the Add Networking page, select **Select an existing network**, browse to select the **sfo01-w01-vds01-vMotion** port group, click **OK**, and click **Next**.
 - f On the Port properties page, select **vMotion** from the TCP/IP Stack drop-down menu and click **Next**.
 - g On the IPv4 settings page, select **Use static IPv4 settings**, enter the IP address **172.16.32.101**, enter the subnet **255.255.255.0**, and click **Next**.
 - h Click **Finish**.

- 9 Configure the MTU on the vMotion VMkernel adapter.
 - a Select the vMotion VMkernel adapter created in the previous step, and click **Edit Settings**.
 - b Click the NIC Settings page.
 - c Enter **9000** for the **MTU** value and click **OK**.
- 10 Configure the vMotion TCP/IP stack.
 - a Click **TCP/IP configuration**.
 - b Select **vMotion** and click the **Edit** icon.
 - c Click **Routing** and enter **172.16.32.253** for the **VMkernel gateway** and click **OK**.
- 11 Migrate the Platform Services Controller and vCenter Server instances from the standard switch to the distributed switch.
 - a In the Navigator, click **Networking** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Right-click the **sfo01-w01-vds01** distributed switch and click **Migrate VM to Another Network**.
 - c On the Select source and destination networks page, browse the following networks and click **Next**.

Setting	Value
Source network	VM Network
Destination network	sfo01-w01-vds01-management-vm

- d On the Select VMs to migrate page, select **sfo01w01psc01.sfo01.rainpole.local** and **sfo01w01vc01.sfo01.rainpole.local**, and click **Next**.
 - e On the Ready to complete page, review your entries and click **Finish**.
- 12 Define Network I/O Control shares for the different traffic types on the sfo01-w01-vds01 distributed switch.
 - a Click the **sfo01-w01-vds01** distributed switch, click the **Configure** tab, and click **Resource Allocation > System traffic**.
 - b Under System Traffic, configure each of the following traffic types with the following values.

Traffic Type	Physical adapter Shares
vSAN Traffic	High
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication (VR) Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance (FT) Traffic	Low
iSCSI Traffic	Low

- 13 Migrate the last physical adapter from the standard switch to the sfo01-w01-vds01 distributed switch.
 - a In the Navigator, click **Networking** and expand the **sfo01-w01dc** datacenter.
 - b Right-click the **sfo01-w01-vds01** distributed switch and select **Add and Manage Hosts**.
 - c On the Select task page, select **Manage host networking**, and click **Next**.

- d On the Select hosts page, click **Attached hosts**.
 - e In the Select member hosts dialog box, select *sfo01w01esx01.sfo01.rainpole.local*, and click **OK**.
 - f On the Select hosts page, click **Next**.
 - g On the Select network adapter tasks page, select **Manage physical adapters** only, and click **Next**.
 - h On the Manage physical network adapters page, select **vmnic0**, and click **Assign uplink**.
 - i In the Select an Uplink for vmnic1 dialog box, select **Uplink 2**, and click **OK**, and click **Next**.
 - j On the Analyze Impact page, click **Next**.
 - k On the Ready to complete page, click **Finish**.
- 14 Enable vSphere Distributed Switch Health Check.
 - a In the Navigator, click **Networking** and expand the **sfo01-w01dc** datacenter.
 - b Select the **sfo01-w01-vds01** distributed switch and click the **Configure** tab.
 - c In the Navigator, select **Health check** and click the **Edit** button.
 - d Select **Enabled** for **VLAN and MTU** and **Teaming and failover** and click **OK**.
 - 15 Delete the vSphere Standard Switch.
 - a In the Navigator, click on **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Click on **sfo01w01esx01.sfo01.rainpole.local** and then click the **Configure** tab.
 - c On the Configure page, select **Virtual switches**, choose **vSwitch0**, and then click on the **Remove selected standard switch** icon.
 - d In the Remove Standard Switch dialog box, click **Yes** to confirm the removal.

Create vSAN Disk Groups for Consolidated SDDC

vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 3 Click on the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
- 4 Under vSAN, click **Disk Management**.
- 5 Click on **sfo01w01esx02.sfo01.rainpole.local** and click on the **Create a new disk group** button.
- 6 In the Create Disk Group window, select a flash disk for the cache tier, two hard disk drives for the capacity tier and click **OK**.
- 7 Repeat steps 5 and 6 for **sfo01w01esx03.sfo01.rainpole.local** and **sfo01w01esx04.sfo01rainpole.local**.

- 8 Assign a license to vSAN.
 - a Right click the **sfo01-w01-consolidated01** cluster and select **Assign License**.
 - b In the sfo01-w01-consolidated01 - Assign License window select the previously added **VSAN License** and click **OK**.

Enable vSphere HA for Consolidated SDDC

Before creating the host profile for the management cluster, enable vSphere HA for the consolidated cluster.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click **Hosts and Clusters**.
 - a Expand the **sfo01w01vc01.sfo01.rainpole.local** inventory.
 - b Select the **sfo01-w01-consolidated01** cluster.
- 3 Click the **Configure** tab, click **vSphere Availability**, and click **Edit**.
- 4 In the Edit Cluster Settings dialog box, select the **Turn on vSphere HA** check box.
- 5 Select **Failures and Responses** and select the following values from the drop-down menus.

Setting	Value
Enable Host Monitoring	Selected
Host Failure Response	Restart VMs
Response for Host Isolation	Power off and restart VMs
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	VM Monitoring Only

- 6 Click **Admission Control**.
- 7 In the Admission Control page enter following settings.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

- 8 Click **OK**.

Change Advanced Options on the ESXi Hosts for Consolidated SDDC

Change the default ESX Admins group to achieve greater levels of security, and enable vSAN to provision the Virtual Machine Swap files as thin to save space in the vSAN datastore.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Change the default ESX Admins group.
 - a In the Navigator, click **Hosts and Clusters**.
 - b Expand the entire **sfo01w01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **sfo01w01esx01.sfo01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **filter** box, enter **esxAdmins** and wait for the search results.
 - f Change the value of **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** to **SDDC-Admins** and click **OK**.
- 3 Provision Virtual Machine swap files on vSAN as thin.
 - a In the Navigator, click **Hosts and Clusters**.
 - b Expand the entire **sfo01w01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **sfo01w01esx01.sfo01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **filter** box, enter **vsan.swap** and wait for the search results.
 - f Change the value of **VSAN.SwapThickProvisionDisabled** to **1** and click **OK**.
- 4 Disable the SSH warning banner.
 - a In the Navigator, click **Hosts and Clusters**.
 - b Expand the entire **sfo01w01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **sfo01w01esx01.sfo01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **Filter** search field, enter **ssh** and wait for the search results.
 - f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

Mount NFS Storage for Consolidated SDDC

You must mount an NFS datastore where vSphere Data Protection will later be deployed.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click **Host and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 3 Click on **sfo01w01esx01.sfo01.rainpole.local**.
- 4 Click on **Datastores**.
- 5 Click the **Create a New Datastore** icon.
- 6 On the Location page, click **Next**.
- 7 On the Type page, select **NFS** and click **Next**.
- 8 On the Select NFS version page, select **NFS 3** and click **Next**.
- 9 On the Name and configuration page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	sfo01-w01-vdp01
Folder	/V2D_vDP_Consolidated_6TB
Server	172.16.15.251

- 10 On the Ready to complete page, review the configuration and click **Finish**.

Create and Apply the Host Profile for Consolidated SDDC

Host Profiles ensure all hosts in the cluster have the same configuration.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Host Profile from *sfo01w01esx01.sfo01.rainpole.local*
 - a In the Navigator, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Right-click the ESXi host **sfo01w01esx01.sfo01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.
 - c In the Extract Host Profile window, enter **sfo01-w01-consolidated01** for the **Name** and click **Next**.
 - d In the Ready to complete page, click **Finish**.
- 3 Attach the Host Profile to the consolidated cluster.
 - a In the Navigator, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - b Right-click on the **sfo01-w01-consolidated01** cluster and choose **Host Profiles > Attach Host Profile**.
 - c In the Attach Host Profile window, click the **sfo01-w01-consolidated01** Host Profile, select the **Skip Host Customization** checkbox and click **Finish**.
- 4 Create a host customization profile for the hosts in the consolidated cluster.
 - a In the Navigator, select **Policies and Profiles**.
 - b Click **Host Profiles**, then right click **sfo01-w01-consolidated01** and choose **Export Host Customizations**.
 - c Click **Save**.
 - d Choose a file location to save the *sfo01-w01-consolidated01_host_customizations.csv* file.
 - e Open the *sfo01-w01-consolidated01_host_customizations.csv* in Excel.

- f Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
sfo01w01esx01.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	sfo01w01esx01
sfo01w01esx02.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	sfo01w01esx02
sfo01w01esx03.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	sfo01w01esx03
sfo01w01esx04.sfo01.rainpole.local	ad_admin_password	ad_admin_acct@sfo01.rainpole.local	sfo01w01esx04

ESXi Host	NetStack Instance vmotion->DNS configuration Name for this host
sfo01w01esx01.sfo01.rainpole.local	sfo01w01esx01
sfo01w01esx02.sfo01.rainpole.local	sfo01w01esx02
sfo01w01esx03.sfo01.rainpole.local	sfo01w01esx03
sfo01w01esx04.sfo01.rainpole.local	sfo01w01esx04

ESXi Host	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-Management:management->IP address settings Host IPv4 address	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-management:management->IP address settings SubnetMask
sfo01w01esx01.sfo01.rainpole.local	172.16.31.101	255.255.255.0
sfo01w01esx02.sfo01.rainpole.local	172.16.31.102	255.255.255.0
sfo01w01esx03.sfo01.rainpole.local	172.16.31.103	255.255.255.0
sfo01w01esx04.sfo01.rainpole.local	172.16.31.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-vSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-vSAN:vsan->IP address settings SubnetMask
sfo01w01esx01.sfo01.rainpole.local	172.16.33.101	255.255.255.0
sfo01w01esx02.sfo01.rainpole.local	172.16.33.102	255.255.255.0
sfo01w01esx03.sfo01.rainpole.local	172.16.33.103	255.255.255.0
sfo01w01esx04.sfo01.rainpole.local	172.16.33.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-vMotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC sfo01-w01-vds01:sfo01-w01-vds01-vMotion:vmotion->IP address settings SubnetMask
sfo01w01esx01.sfo01.rainpole.local	172.16.32.101	255.255.255.0
sfo01w01esx02.sfo01.rainpole.local	172.16.32.102	255.255.255.0
sfo01w01esx03.sfo01.rainpole.local	172.16.32.103	255.255.255.0
sfo01w01esx04.sfo01.rainpole.local	172.16.32.104	255.255.255.0

- g When you have updated the Excel file, save it in the CSV file format and close Excel.

- h Click **sfo01-w01-consolidated01** and select the **Configure** tab.
 - i Click the **Edit Host Customizations** button.
 - j In the Edit Host Customizations window select all hosts and click **Next**.
 - k Click the **Browse** button to use a customization file, locate the *sfo01-w01-consolidated01_host_customizations.csv* file saved earlier and select it and click **Open** then click **Finish**.
- 5 Remediate the hosts in the consolidated cluster.
- a Click the **Monitor** tab and click **Compliance**.
 - b Select **sfo01-w01-consolidated01** and click the **Check Host Profile Compliance** button.
 - c Select **sfo01w01esx02.sfo01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the Ready to complete window.
 - d Select **sfo01w01esx03.sfo01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the Ready to complete window.
 - e Select **sfo01w01esx04.sfo01.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the Ready to complete window.
- 6 Verify the Host Compliance.
- a Click the **Monitor** tab and click **Compliance**.
 - b Select **sfo01-w01-consolidated01** and click the **Check Host Profile Compliance** button.
All hosts should show a **Compliant** status in the Host Compliance column.
- 7 Schedule nightly compliance checks.
- a On the Policies and Profiles page, click **sfo01-w01-consolidated01**, click the **Monitor** tab, and then click the **Scheduled Tasks** subtab.
 - b Click **Schedule a New Task** then click **Check Host Profile Compliance**.
 - c In the Check Host Profile Compliance (scheduled) window click **Scheduling Options**.
 - d Enter **sfo01-w01-consolidated01 compliance Check** in the **Task Name** field.
 - e Click the **Change** button on the Configured Scheduler line.
 - f In the Configure Scheduler window select **Setup a recurring schedule for this action** and change the **Start time** to **10:00 PM** and click **OK**.
 - g Click **OK** in the Check Host Profile Compliance (scheduled) window.

Set vSAN Policy on Management Virtual Machines for Consolidated SDDC

After you apply the host profile to all the hosts, set the storage policy of the vCenter Server and the Platform Services Controller to the vSAN Default Storage Policy.

Set the Platform Services Controller and vCenter Server appliances to the default vSAN storage policy.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
- 2 In the Navigator, click **Hosts and Clusters**.
- 3 Expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 4 Select the **sfo01w01vc01** virtual machine.
 - a Click the **Configure** tab, click **Policies**, and click **Edit VM Storage Policies**.
 - b In the sfo01w01vc01:Manage VM Storage Policies dialog box, from the **VM storage policy** drop down menu, select **vSAN Default Storage Policy**, and click **Apply to all**.
 - c Click **OK** to apply the changes.
 - d Verify that the Compliance Status column shows a **Compliant** status for all items in the table.
- 5 Select the **sfo01w01psc01** virtual machine.
 - a Click the **Configure** tab, click **Policies**, and click **Edit VM Storage Policies**.
 - b In the sfo01w01psc01:Manage VM Storage Policies dialog box, from the **VM storage policy** drop down menu, select **vSAN Default Storage Policy**, and click **Apply to all**.
 - c Click **OK** to apply the changes.
 - d Verify that the Compliance Status column shows a **Compliant** status for all items in the table.

Create the VM and Template Folders for Consolidated SDDC

Create folders to group objects of the same type for easier management.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
- 2 Create folders for the management applications.
 - a In the Navigator, click **VMs and Templates**.
 - b Expand the **sfo01w01vc01.rainpole.local** tree.
 - c Right-click the **sfo01-w01dc** data center, and select **New Folder > New VM and Template Folder**.

- d In the New Folder dialog box enter **sfo01-w01fd-mgmt** as the name to label the folder, and click **OK**.
- e Repeat this step to create the remaining folders.

Management Applications	Folder
vCenter Server Appliance + Platform Services Controller + Update Manager Download Service	sfo01-w01fd-mgmt
vRealize Log Insight	sfo01-w01fd-vrli
vRealize Automation and vRealize Business	sfo01-w01fd-vra
vRealize Automation (Proxy Agent) + vRealize Business (Data Collector)	sfo01-w01fd-vraias
vRealize Operations Manager	sfo01-w01fd-vrops
vRealize Operations Manager (Remote Collectors)	sfo01-w01fd-vropsrc
NSX Manager + Controllers + Edges	sfo01-w01fd-nsx
vSphere Data Protection	sfo01-w01fd-bcdr

- 3 Move the vCenter Server and Platform Services Controller virtual machines to the sfo01-w01fd-mgmt folder.
 - a In the Navigator, click **VMs and Templates**.
 - b Expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - c Expand the **Discovered Virtual Machines** folder.
 - d Drag **sfo01w01vc01** and **sfo01w01psc01** to the **sfo01-w01fd-mgmt** folder.
- 4 Delete the **Discovered Virtual Machines** folder.
 - a In the Navigator, click **VMs and Templates**.
 - b Expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
 - c Right click the **Discovered Virtual Machines** folder and choose **Remove from Inventory**.

Create VM Groups to Define the Startup Order for Consolidated SDDC

VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, select **Host and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 3 Create a VM Group for the Platform Services Controller.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Groups**.
 - c On the VM/Host Groups page, click the **Add** button.

- d In the Create VM/Host Group dialog, enter **Platform Services Controllers** in the Name field, select **VM Group** from the Type drop down, and click the **Add** button.
- e In the Add VM/Host Group Member dialog, select **sfo01w01psc01** and click **OK**.
- 4 Create a VM Group for the vCenter Server virtual machine.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Groups**.
 - c On the VM/Host Groups page, click the **Add** button.
 - d In the Create VM/Host Group dialog, enter **vCenter Servers** in the Name field, select **VM Group** from the Type drop down, and click the **Add** button.
 - e In the Add VM/Host Group Member dialog, select **sfo01w01vc01** and click **OK**.
- 5 Create a Rule to power on the Platform Services Controllers followed by the vCenter Servers.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Rules**.
 - c On the VM/Host Rules page, click the **Add** button.
 - d In the Create VM/Host Rule dialog, enter **SDDC Management Virtual Machines** in the Name field, ensure the **Enable rule** check box is selected, select **Virtual Machines to Virtual Machines** from the Type drop down.
 - e Select **Platform Services Controllers** from the **First restart VMs in VM group** drop down.
 - f Select **vCenter Servers** from the **Then restart VMs in VM group** and click **OK**.

Create Host Groups to Keep vCenter and the Platform Services Controller on Specific Hosts for Consolidated SDDC

Create a rule that keeps vCenter Server and the Platform Services Controller on the first four hosts so they are easy to locate in the event of an outage.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Value	Setting
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, select **Host and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 3 Create a Host Group containing the first four hosts in the cluster.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Groups**.
 - c On the VM/Host Groups page, click the **Add** button.

- d In the Create VM/Host Group dialog, enter **vCenter and PSC Host Group** in the Name field, select **Host Group** from the Type drop down, and click the **Add** button.
- e In the Add VM/Host Group Member dialog, select **sfo01w01esx01.sfo01.rainpole.local**, **sfo01w01esx02.sfo01.rainpole.local**, **sfo01w01esx03.sfo01.rainpole.local**, and **sfo01w01esx04.sfo01.rainpole.local** and click **OK**.
- 4 Create a rule to run the Platform Services Controller on the hosts in the vCenter and PSC Host Group.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Rules**.
 - c On the VM/Host Rules page, click the **Add** button.
 - d In the Create VM/Host Rule dialog, enter **host-group-rule-psc** in the Name field, ensure the **Enable rule** check box is selected, select **Virtual Machines to Hosts** from the Type drop down.
 - e Select **Platform Services Controllers** from the **VM group** drop down.
 - f Select **Should run on hosts in group**.
 - g Select **vCenter and PSC Host Group** from the **Host Group** drop down, and click **OK**.
- 5 Create a rule to run the vCenter Server on the hosts in the vCenter and PSC Host Group.
 - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
 - b On the Configure page, click **VM/Host Rules**.
 - c On the VM/Host Rules page, click the **Add** button.
 - d In the Create VM/Host Rule dialog, enter **host-group-rule-vc** in the Name field, ensure the **Enable rule** check box is selected, select **Virtual Machines to Hosts** from the Type drop down.
 - e Select **vCenter Servers** from the **VM group** drop down.
 - f Select **Should run on hosts in group**.
 - g Select **vCenter and PSC Host Group** from the **Host Group** drop down, and click **OK**.

Deploy and Configure Components in the NSX Instance of the Consolidated SDDC

Deploy and configure the NSX instance for the consolidated cluster in your consolidated SDDC deployment.

Procedure

- 1 [Deploy the NSX Manager for Consolidated SDDC](#) on page 39
For this consolidated SDDC implementation, NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.
- 2 [Assign Licensing for NSX Instance for Consolidated SDDC](#) on page 43
Assign licensing for the NSX instance in your consolidated SDDC location.
- 3 [Deploy the NSX Controllers for the NSX Instance for Consolidated SDDC](#) on page 44
After the NSX Manager is successfully connected to the vCenter Server, you must deploy the three NSX Controller nodes that form the NSX Controller cluster. You must deploy every node only after the previous one is successfully deployed.
- 4 [Prepare the ESXi Hosts in the Consolidated Cluster for NSX for Consolidated SDDC](#) on page 46
NSX kernel modules packaged in VIB files run within the hypervisor kernel, and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts in the consolidated cluster.

- 5 [Configure the NSX Logical Network for the Consolidated Cluster for Consolidated SDDC](#) on page 46
After all the deployment tasks are ready, you can configure the NSX logical network for use with your management and workload consolidation deployment.
- 6 [Update the Host Profile for the Consolidated Cluster for Consolidated SDDC](#) on page 48
When an authorized change is made to a host, the host profile must be updated to reflect the changes.
- 7 [Configure NSX Dynamic Routing for Consolidated SDDC](#) on page 48
NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the consolidated cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).
- 8 [Distributed Firewall Configuration for Consolidated SDDC](#) on page 65
You define explicit rules for the distributed firewall which allows access to management applications and workloads in the consolidated cluster.
- 9 [Test the Consolidated Cluster NSX Configuration for Consolidated SDDC](#) on page 70
Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other over the network.
- 10 [Deploy Application Virtual Networks for Consolidated SDDC](#) on page 70
Deploy the application virtual networks for your management and workload consolidation deployment.
- 11 [Deploy the NSX Load Balancer for Consolidated SDDC](#) on page 74
Deploy a load balancer for use by the management applications connected to the application virtual network, Mgmt-xRegion01-VXLAN

Deploy the NSX Manager for Consolidated SDDC

For this consolidated SDDC implementation, NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

To deploy the NSX Manager virtual appliance for the consolidated SDDC, you first assign a domain service account which NSX uses as the vCenter Server Administrator role. You then deploy the NSX Manager virtual appliance for the consolidated SDDC. After you deploy the NSX Manager, you connect it to the vCenter Server instance.

Assign an NSX Domain Service Account and Deploy the NSX Manager Appliance for Consolidated SDDC

Assign a domain service account for use by NSX to access the vCenter Server Administrator role. Deploy the NSX Manager appliance from the OVF file to the sfo01-w01rp-sddc-mgmt resource pool.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click the **Home** icon and choose **Administration**. Click **Global Permissions**.

- 3 Click **Manage** tab and click the **Add** icon.
- 4 In the Global Permission Root - Add Permission dialog box, click **Add**.
- 5 In the Select Users/Groups dialog box, select **rainpole.local** from the **Domain** drop-down menu.
- 6 In the Search box, enter **svc-nsxmanager** and press Enter.
- 7 Select **svc-nsxmanager** and click **Add**. Press **OK** to return to the Global Permission Root - Add Permission window.
- 8 Click **OK** to give the svc-nsxmanager account vCenter Administrative privileges.
- 9 Click the **Home** icon and choose **Hosts and Clusters** to return to that page in the Navigator.
- 10 In the Navigator pane, expand the **sfo01w01vc01.sfo01.rainpole.local** control tree.
- 11 Expand the **sfo01-w01-consolidated01** cluster.
- 12 Right-click the **sfo01-w01rp-sddc-mgmt** resource pool and click **Deploy OVF Template**.
- 13 On the Select template page, click the **Browse** button, select the VMware NSX Manager .ova file, and click **Next**.
- 14 On the Select name and location page, enter the following settings, and click **Next**.

Setting	Value
Name	sfo01w01nsx01
Select a datacenter or folder	sfo01-w01fd-nsx

- 15 On the Select a resource page, select the following values, and click **Next**.

Setting	Value
Cluster	sfo01-w01-consolidated01
Resource Pool	sfo01-w01rp-sddc-mgmt

- 16 On the Review details page, click **Next**.
- 17 On the Accept license agreements page, click **Accept** and click **Next**.
- 18 On the Select storage page, enter the following settings, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM storage policy	vSAN Default Storage Policy
Datastore	sfo01-w01-vsan01

- 19 On the Setup networks page, under **Destination Network**, select **sfo01-w01-vds01-managment-vm** and click **Next**.
- 20 On the Customize template page, expand all options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.16.11.5,172.16.11.4
Domain Search List	sfo01.rainpole.local
Default IPv4 Gateway	172.16.11.253
Hostname	sfo01w01nsx01.sfo01.rainpole.local
Network 1 IPv4 Address	172.16.11.66
Network 1 Netmask	255.255.255.0

Setting	Value
Enable SSH	Selected
NTP Server List	ntp.sfo01.rainpole.local
CLI "admin" User Password / enter	sfo01nsx_admin_password
CLI "admin" User Password / confirm	sfo01nsx_admin_password
CLI Privilege Mode Password / enter	sfo01nsx_privilege_password
CLI Privilege Mode Password / confirm	sfo01nsx_privilege_password

- 21 On the Ready to Complete page, click **Finish**.
- 22 In the Navigator, expand the **sfo01w01vc01.sfo01.rainpole.local** control tree, select the virtual machine **sfo01w01nsx01**, and click the **Power on** button.

Replace the NSX Manager Certificate for Consolidated SDDC

After you install NSX Manager, you replace its certificate with a CA-signed certificate.

You generate certificates for the SDDC management components on a Windows host by using VMware Validated Design Certificate Generation Utility (CertGenVVD).

Table 2-4. Certificate-Related Files on the NSX Manager Instance

NSX Manager FQDN	Certificate File Name	Replacement Time
sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.sfo01.4.p12 from the automation generation.	Right after deployment of the NSX Manager instance.

Procedure

- 1 On the Windows host that has access to the data center and contains the generated certificates, log in to the NSX Manager Web interface.
 - a Open a Web Browser and go to following URL **https://sfo01w01nsx01.sfo01.rainpole.local**
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	nsx_manager_admin_password

- 2 Click the **Manage Appliance Settings** button.
- 3 On the **Manage** tab, click **SSL Certificates** and click **Upload PKCS#12 Keystore**.
- 4 Browse to the certificate chain file **sfo01w01nsx01.sfo01.4.p12**, provide the keystore password or passphrase and click **Import**.
- 5 In the right corner of the NSX Manager user interface, click the **Settings** icon.
- 6 From the drop-down menu, select **Reboot Appliance**.

The NSX Manager restarts, which in turn propagates the CA-signed certificate.

Connect NSX Manager to the vCenter Server for Consolidated SDDC

After you deploy the NSX Manager and replace its certificate, connect the NSX Manager to the vCenter Server.

Procedure

- 1 Connect the NSX Manager to the vCenter Server for the consolidated SDDC cluster.
 - a Open a Web browser and go to **https://sfo01w01nsx01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 Click **Manage vCenter Registration**.
- 3 Under **Lookup Service URL**, click the **Edit** button.
- 4 In the Lookup Service URL dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service Host	sfo01w01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 5 In the Trust Certificate? dialog box, click **Yes**.
- 6 Under vCenter Server, click the **Edit** button.
- 7 In the vCenter Server dialog box, enter the following settings and click **OK**.

Setting	Value
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	<i>svc-nsxmanager_password</i>

- 8 In the Trust Certificate? dialog box, click **Yes**.
- 9 Wait for the Status indicators for the Lookup Service and vCenter Server to change to a Connected status.

Assign Administrative Access to NSX for Consolidated SDDC

Assign the administrator@vsphere.local account access to NSX for your consolidated SDDC deployment.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	svc-nsxmanager_password

- 2 In the Navigator, click **Networking & Security** and click **NSX Managers**.
- 3 Under NSX Managers, click the **172.16.11.66** instance.
- 4 Click the **Manage** tab, click **Users** and click the **Add** icon.
- 5 On the Identify User page, enter **administrator@vsphere.local** in the **User** text field and click **Next**.
- 6 On the Select Roles page, select the **Enterprise Administrator** radio button and click **Finish**.

Assign Licensing for NSX Instance for Consolidated SDDC

Assign licensing for the NSX instance in your consolidated SDDC location.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add new licenses for this NSX instance.
 - a Click the Home icon above the Navigator and choose the Administration menu item.
 - b On the Administration page, under Licensing and select **Licenses**.
 - c Under Licenses , click on the **Licenses** tab.
 - d Click the **Create New Licenses** icon to add license keys.
 - e On the Enter license keys page, enter license keys for **NSX**, and click **Next**.
 - f On the Edit license name page, enter License name and click **Next**.
 - g On the Ready to complete page, review your entries and click **Finish**.
- 3 Assign the new license to NSX.
 - a Click the Home icon above the Navigator and choose the Administration menu item.
 - b On the Administration page, under Licensing and select **Licenses**.
 - c Under Licenses , click on the **Assets** tab then click the **Solutions** tab.

- d Select **NSX for vSphere** and click the **Assign License** icon.
- e On the NSX for vSphere - Assign License page select the license created in step 2 and click **OK**.

Deploy the NSX Controllers for the NSX Instance for Consolidated SDDC

After the NSX Manager is successfully connected to the vCenter Server, you must deploy the three NSX Controller nodes that form the NSX Controller cluster. You must deploy every node only after the previous one is successfully deployed.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Promote the NSX Manager to the primary role.
 - a Under Inventories, click **Networking & Security**.
 - b In the Navigator, click **Installation**.
 - c On the **Management** tab, click the **172.16.11.66** instance.
 - d Click the **Actions** menu and click **Assign Primary Role**.
 - e In the Assign Primary Role confirmation dialog box, click **Yes**.
- 3 Configure an IP pool for the NSX Controller cluster
 - a Click the **Home** icon and choose **Networking & Security**.
 - b In the Navigator, click **NSX Managers**.
 - c Under NSX Managers, click the **172.16.11.66** instance.
 - d Click the **Manage** tab, click **Grouping Objects**, click **IP Pools**, and click the **Add New IP Pool** icon.
 - e In the Add Static IP Pool dialog box, enter the following settings and click **OK**.

Setting	Value
Name	sfo01w01-nsxc01
Gateway	172.16.31.253
Prefix Length	24
Primary DNS	172.16.11.5
Secondary DNS	172.16.11.4
DNS Suffix	sfo01.rainpole.local
Static IP Pool	172.16.31.118-172.16.31.120

- 4 Deploy the NSX Controller cluster.
 - a In the Navigator, click the **Home** icon and choose **Networking & Security** to go back, then click **Installation**.

- b On the Management tab, under NSX Controller nodes, click the **Add** icon to deploy three NSX Controller nodes with the same configuration.
- c In the Add Controller page, enter the following settings and click **OK**. You configure a password only during the deployment of the first controller. The other controllers will use the same password.

Setting	Value
Name	nsx-controller-w01-01
NSX Manager	172.16.11.66
Datacenter	sfo01-w01dc
Cluster/Resource Pool	sfo01-w01rp-sddc-edge
Datastore	sfo01-w01-vsan01
Folder	sfo01-w01fd-nsx
Connected To	sfo01-w01-vds01-Management
IP Pool	sfo01w01-nsxc01
Password	sfonsx_controllers_password
Confirm Password	sfonsx_controllers_password

- d When the status of the controller node changes to Connected, repeat the step and deploy the two remaining NSX Controller nodes in the controller cluster using the same configuration, incrementing the name by 1 each time.
- 5 Configure DRS affinity rules for the NSX Controller nodes.
- a Return to the Home page.
 - b In the Navigator, click **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree control.
 - c Select the **sfo01-w01-consolidated01** cluster, and click the **Configure** tab.
 - d Under Configuration click **VM/Host Rules**.
 - e Click **Add**.
 - f In the sfo01-w01-consolidated01 - Create VM/Host Rule dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machine

- g In the Add Rule Member dialog box, select the check box next to each of the three NSX Controller virtual machines and click **OK**.
- h In the sfo01-w01-consolidated01 - Create VM/Host Rule dialog box, click **OK**.

Prepare the ESXi Hosts in the Consolidated Cluster for NSX for Consolidated SDDC

NSX kernel modules packaged in VIB files run within the hypervisor kernel, and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the ESXi hosts in the consolidated cluster.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click the **Home** icon and choose **Networking & Security**.
- 3 Click **Installation** and click the **Host Preparation** tab.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Under Installation Status, select **sfo01-w01-consolidated01** cluster, click **Actions** and **Install**. Click **Yes** in the confirmation dialog box..
- 6 Expand **sfo01-w01-consolidated01** cluster. Verify that the Installation Status column displays the NSX version for all hosts in the cluster, confirming that you have successfully installed the NSX kernel modules.

Configure the NSX Logical Network for the Consolidated Cluster for Consolidated SDDC

After all the deployment tasks are ready, you can configure the NSX logical network for use with your management and workload consolidation deployment.

To configure the NSX logical network, perform the following tasks:

- Configure the Segment ID allocation.
- Configure the VXLAN networking.
- Configure the Transport Zone.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Configure the Segment ID allocation.

- a In the Navigator, click the **Home** icon and choose **Networking & Security**.
- b Click **Installation**, click the **Logical Network Preparation** tab, and click **Segment ID**.
- c Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- d Click **Edit**, enter the following values, and click **OK**.

Setting	Value
Segment ID pool	5300-9000
Enable Multicast addressing	Selected
Multicast addresses	239.3.0.0-239.3.255.255
Universal Segment ID Pool	20000-29000
Enable Universal Multicast addressing	Selected
Universal Multicast addresses	239.4.0.0-239.4.255.255

3 Configure the VXLAN networking.

- a Click the **Host Preparation** tab.
- b Under VXLAN, click **Not Configured**, enter the following values, and click **OK**.

Setting	Value
Switch	sfo01-w01-vds01
VLAN	1634
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the transport zone.

- a On the Installation page, click the **Logical Network Preparation** tab and click **Transport Zones**.
- b Click the **Add New Transport zone** icon.
- c In the New Transport Zone dialog box, enter the following settings and click **OK**.

Setting	Value
Mark this Object for Universal Synchronization	Selected
Name	SFO01W01 Universal Transport Zone
Replication mode	Hybrid
Select clusters that will be part of the Transport Zone	sfo01-w01-consolidated01

5 Enable CDO mode.

- a On the Installation page, click the **Logical Network Preparation** tab and click **Transport Zones**.
- b Select the Transport zone **SFO01W01 Universal Transport Zone**.
- c In the Actions, select **Enable CDO mode**.
- d Select **Yes** to enable CDO mode of SFO01W01 Universal Transport Zone.

Update the Host Profile for the Consolidated Cluster for Consolidated SDDC

When an authorized change is made to a host, the host profile must be updated to reflect the changes.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the host profile for the management cluster.
 - a In the Navigator, click the **Home** icon and select **Policies and Profiles**.
 - b Click **Host Profiles**, right click **sfo01-w01-consolidated01**, and select **Copy settings from Host**.
 - c Select **sfo01w01esx01.rainpole.local** and click **OK**.
- 3 Verify compliance for the hosts in the management cluster.
 - a Click the **Monitor** tab and click **Compliance**.
 - b Select **sfo01-w01-consolidated01** and click the **Check Host Profile Compliance** button.

All hosts must display a Host Compliance status of **Compliant**.

Configure NSX Dynamic Routing for Consolidated SDDC

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the consolidated cluster, deploying two NSX Edge devices and configure a Universal Distributed Logical Router (UDLR).

Procedure

- 1 [Create a Logical Switch for use as the Transit Network for Consolidated SDDC](#) on page 49
Create a Logical Switch for use as the transit network.
- 2 [Deploy NSX Edge Devices for North-South Routing for Consolidated SDDC](#) on page 49
- 3 [Disable the Firewall Service in ECMP Edges for Consolidated SDDC](#) on page 52
Disable the firewall of the NSX Edge devices. This is required for equal-cost multi-path (ECMP) to operate correctly.
- 4 [Enable and Configure BGP Routing for Consolidated SDDC](#) on page 53
The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).
- 5 [Verify Peering of Upstream Switches and Establishment of BGP for Consolidated SDDC](#) on page 58
The NSX Edge devices need to establish a connection to each of the upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.
- 6 [Deploy the Universal Distributed Logical Router for Consolidated SDDC](#) on page 59

- 7 [Configure Universal Distributed Logical Router for Dynamic Routing for Consolidated SDDC](#) on page 61
Configure the Universal distributed logical router (UDLR) to use dynamic routing in management and workload consolidation.
- 8 [Verify Establishment of BGP for the Universal Distributed Logical Router for Consolidated SDDC](#) on page 64
Verify that the UDLR is successfully peering, and that BGP routing has been established.

Create a Logical Switch for use as the Transit Network for Consolidated SDDC

Create a Logical Switch for use as the transit network.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to <https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click the **Home** icon and choose **Networking & Security**.
- 3 In the Navigator, click **Logical Switches**.
- 4 Select the NSX Manager instance labelled **172.16.11.66**.
- 5 Click the **Add** icon.
The New Logical Switch dialogue box appears.
- 6 In the New Logical Switch dialogue box, enter the following settings and click **OK**.

Setting	Value
Name	SFO01W01 Universal Transit Network
Transport Zone	SFO01W01 Universal Transport Zone
Replication Mode	Hybrid
Enable IP Discovery	Checked
Enable MAC Learning	Unchecked

Deploy NSX Edge Devices for North-South Routing for Consolidated SDDC

Perform this procedure twice to deploy two identical NSX Edge devices. Enter the name and IP addresses for the respective device using the values shown in the tables.

NSX Edge Device	Device Name
NSX Edge Device 1	sfo01w01esg01
NSX Edge Device 2	sfo01w01esg02

Interface	Primary IP Address sfo01w01esg01	Primary IP Address sfo01w01esg02
Uplink01	172.16.35.2	172.16.35.3

Interface	Primary IP Address sfo01w01esg01	Primary IP Address sfo01w01esg02
Uplink02	172.27.13.3	172.27.13.2
sfo01w01udlr01	192.168.100.1	192.168.100.2

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to deploy a new NSX Edge.

The New NSX Edge wizard appears.

- a On the Name and description page, enter the following settings and click **Next**.

Settings	Value
Install Type	Edge Service Gateway
Name	sfo01w01esg01
Deploy NSX Edge	Selected
Enable High Availability	Deselected

- b On the Settings page, enter the following settings and click **Next**.

Settings	Value
User Name	admin
Password	edge_admin_password
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

- c On the Configure deployment page, select the **Large** radio button to specify the **Appliance Size** and click the **Add** icon.

The Add NSX Edge Appliance dialog box appears.

- d In the Add NSX Edge Appliance dialog box, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Cluster/Resource Pool	sfo01-w01rp-sddc-edge
Datastore	sfo01-w01-vsan01
Folder	sfo01-w01fd-nsx

- e On the **Configure Interfaces** page, click the **Add** icon to configure the Uplink01 interface, enter the following settings, and click **OK**.

Setting	Value
Name	Uplink01
Type	Uplink
Connected To	sfo01-w01-vds01-Uplink01
Connectivity Status	Connected
Primary IP Address	172.16.35.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- f Click the **Add** icon once again to configure the Uplink02 interface, enter the following settings, and click **OK**.

Setting	Value
Name	Uplink02
Type	Uplink
Connected To	sfo01-w01-vds01-Uplink02
Connectivity Status	Connected
Primary IP Address	172.27.13.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- g Click the **Add** icon a third time to configure the UDLR interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	sfo01w01udlr01
Type	Internal
Connected To	SFO01W01 Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.100.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- h On the Default Gateway Settings page, deselect the **Configure Default Gateway** check box and click **Next**.
- i On the Firewall and HA page, click **Next**.
- j On the Ready to Complete page, review the configuration settings you entered and click **Finish**.
- 6 Repeat this procedure to configure another NSX edge using the settings for the second NSX Edge device **sfo01w01esg02**.

- 7 Configure DRS anti-affinity rules for the Edge Services Gateways.
 - a Go back to the Home page.
 - b In the Navigator, click **Hosts and Clusters**, and expand the **sfo01w01vc01.sfo01.rainpole.local** tree control.
 - c Select the **sfo01-w01-consolidated01** cluster, and click the **Configure** tab.
 - d Under Configuration, click **VM/Host Rules**.
 - e Click **Add**.
 - f In the sfo01-w01-consolidated01 - Create VM/Host Rule dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-ecmpedges
Enable rule	Selected
Type	Separate Virtual Machine

- g In the Add Rule Member dialog box, select the check box next to each of the two, newly deployed NSX ESGs, and click **OK**.
- h In the sfo01-w01-consolidated01 - Create VM/Host Rule dialog box, click **OK**.

Disable the Firewall Service in ECMP Edges for Consolidated SDDC

Disable the firewall of the NSX Edge devices. This is required for equal-cost multi-path (ECMP) to operate correctly.

Perform this procedure twice for each of the NSX Edge devices sfo01w01esg01 and sfo01w01esg02.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **sfo01w01esg01** NSX Edge device.
- 6 Click the **Manage** tab and click **Firewall**.
- 7 On the Firewall page, click the **Disable** button.
- 8 Click the **Publish Changes** button.
- 9 Repeat this procedure for the NSX Edge device **sfo01w01esg02**.

Enable and Configure BGP Routing for Consolidated SDDC

The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).

Repeat this procedure two times to enable BGP for both NSX Edge devices: sfo01w01esg01 and sfo01w01esg02.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Double-click the **sfo01w01esg01** NSX Edge device.
- 6 Click the **Manage** tab, and click **Routing**.
- 7 On the Global Configuration page, enter the following settings.
 - a Click the **Enable** button for ECMP.
 - b Click the **Edit** button for Dynamic Routing Configuration.
 - c Choose **Uplink01** as the Router ID.
 - d Click **Publish Changes**.

- 8 On the **Routing** tab, select **Static Routes** to configure it.

- a Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.11.0/24
Next Hop	192.168.100.3
Interfaces	sfo01w01udlr01
MTU	9000
Admin Distance	210

- b Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.31.0/24
Next Hop	192.168.100.3
Interfaces	sfo01w01udlr01
MTU	9000
Admin Distance	210

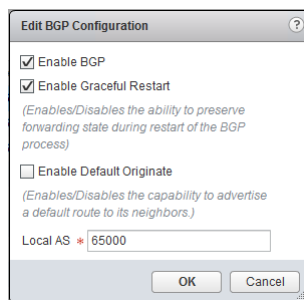
NOTE You must add all subnets that are behind the UDLR.

- c Click **Publish Changes**.

- 9 On the **Routing** tab, select **BGP** to configure it.

- a Click the **Edit** button, enter the following settings, and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Enable Default Originate	Deselected
Local AS	65000



- b Click the **Add** icon to add a neighbor.

The New Neighbor dialog box appears. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

- c In the New Neighbor dialog box, enter the following values for the first Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.16.35.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

New Neighbour

IP Address : * 172.16.35.1

Remote AS : * 65001

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

(BGP Keep alive timer value needs to be one third of hold down timer)

Password : *****

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items Copy

OK Cancel

- d Click the **Add** icon to add another neighbor.

The New Neighbor dialog box appears. Add the second Top of Rack switch, whose IP address is 172.27.13.1.

- e In the New Neighbor dialog box, enter the following values for the second Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.27.13.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

New Neighbour

IP Address : * 172.27.13.1

Remote AS : * 65001

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

(BGP Keep alive timer value needs to be one third of hold down timer)

Password : *****

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items Copy

OK Cancel

- f Click the **Add** icon to add another Neighbor.

The New Neighbor dialog box appears. Configure the universal distributed logical router (UDLR) as a neighbor.

- g In the New Neighbor dialog box, enter the following values, and click **OK**.

Setting	Value
IP Address	192.168.100.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- h Click **Publish Changes**.

The three neighbors you added are now visible in the Neighbors table.

- 10 On the **Routing** tab, select **Route Redistribution** to configure it.
 - a On the Route Redistribution page, click the **Edit** button.
 - b In the Change Redistribution Settings dialog box, select the **BGP** check box and click **OK**.
 - c Under Route Redistribution table, click the **Add** icon.
 - d In the New Redistribution Criteria dialog box, enter the following settings and click **OK**.

Setting	Value
Prefix	Any
Learner Protocol	BGP
OSPF	Deselected
Static routes	Selected
Connected	Selected
Action	Permit

- e Click **Publish Changes**.

The route redistribution configuration is now visible in the Route Redistribution table.

- 11 Repeat this procedure for the **sfo01w01esg02** NSX Edge.

Verify Peering of Upstream Switches and Establishment of BGP for Consolidated SDDC

The NSX Edge devices need to establish a connection to each of the upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.

You repeat this procedure two times for each of the NSX Edge devices: sfo01w01esg01 and sfo01w01esg02.

Procedure

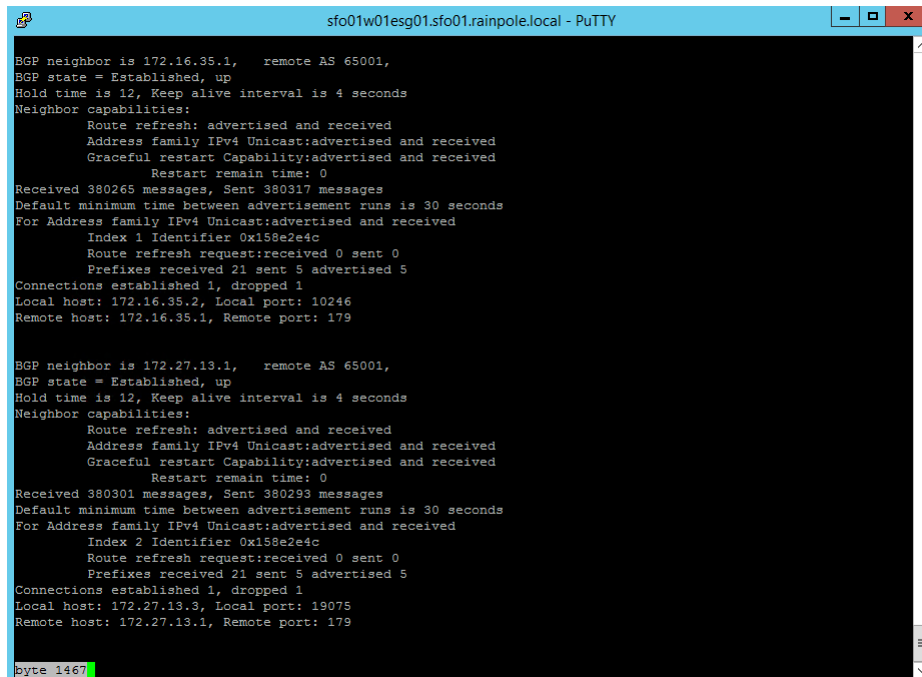
- 1 Log in to the NSX Edge device using a Secure Shell (SSH) client.
 - a Open an SSH connection to the **sfo01w01esg01** NSX Edge device.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	edge_admin_password

- 2 Run the `show ip bgp neighbors` command to display information about the BGP connections to neighbors.

The BGP State will display **Established, UP** if you have peered with the upstream switches.

NOTE You have not yet created the universal distributed logical router (UDLR), so it will not display the **Established, UP** status message.



```

sfo01w01esg01.sfo01.rainpole.local - PuTTY

BGP neighbor is 172.16.35.1, remote AS 65001,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 380265 messages, Sent 380317 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x158e2e4c
  Route refresh request:received 0 sent 0
  Prefixes received 21 sent 5 advertised 5
Connections established 1, dropped 1
Local host: 172.16.35.2, Local port: 10246
Remote host: 172.16.35.1, Remote port: 179

BGP neighbor is 172.27.13.1, remote AS 65001,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 380301 messages, Sent 380293 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 2 Identifier 0x158e2e4c
  Route refresh request:received 0 sent 0
  Prefixes received 21 sent 5 advertised 5
Connections established 1, dropped 1
Local host: 172.27.13.3, Local port: 19075
Remote host: 172.27.13.1, Remote port: 179

byte 1467
  
```

- 3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that there are multiple routes to BGP learned networks.

You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word *via* in the right-side column of the routing table output. In the image below there are two different routes to the following BGP networks: `0.0.0.0/0, 172.16.35.0`. You can identify BGP networks by the letter B in the left-side column. Lines beginning with C (connected) have only a single route.

```

sfo01w01esg01.sfo01.rainpole.local - PuTTY
Codes: 0 - OSPF derived, 1 - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
Total number of routes: 25
B    0.0.0.0/0          [20/0]      via 172.16.35.1
B    0.0.0.0/0          [20/0]      via 172.27.13.1
B   10.159.4.0/23       [20/0]      via 172.16.35.1
B   10.159.4.0/23       [20/0]      via 172.27.13.1
B   172.11.10.0/24      [20/0]      via 172.16.35.1
B   172.11.10.0/24      [20/0]      via 172.27.13.1
B   172.11.11.0/24      [20/0]      via 172.16.35.1
B   172.11.11.0/24      [20/0]      via 172.27.13.1
B   172.11.12.0/24      [20/0]      via 172.16.35.1
B   172.11.12.0/24      [20/0]      via 172.27.13.1
B   172.16.11.0/24      [20/0]      via 172.16.35.1
B   172.16.11.0/24      [20/0]      via 172.27.13.1
B   172.16.31.0/24      [20/0]      via 172.16.35.1
B   172.16.31.0/24      [20/0]      via 172.27.13.1
C   172.16.35.0/24      [0/0]       via 172.16.35.2
B   172.17.11.0/24      [20/0]      via 172.16.35.1
B   172.17.11.0/24      [20/0]      via 172.27.13.1
B   172.17.35.0/24      [20/0]      via 172.16.35.1
B   172.17.35.0/24      [20/0]      via 172.27.13.1
B   172.18.11.0/24      [20/0]      via 172.16.35.1
B   172.18.11.0/24      [20/0]      via 172.27.13.1
B   172.18.12.0/24      [20/0]      via 172.16.35.1
B   172.18.12.0/24      [20/0]      via 172.27.13.1
B   172.18.16.0/24      [20/0]      via 172.16.35.1
B   172.18.16.0/24      [20/0]      via 172.27.13.1
B   172.18.17.0/24      [20/0]      via 172.16.35.1
B   172.18.17.0/24      [20/0]      via 172.27.13.1
B   172.18.18.0/24      [20/0]      via 172.16.35.1
B   172.18.18.0/24      [20/0]      via 172.27.13.1
B   172.18.19.0/24      [20/0]      via 172.16.35.1
B   172.18.19.0/24      [20/0]      via 172.27.13.1
C   172.27.13.0/24      [0/0]       via 172.27.13.3
B   172.27.14.0/24      [20/0]      via 172.16.35.1
B   172.27.14.0/24      [20/0]      via 172.27.13.1
B   172.27.15.0/24      [20/0]      via 172.16.35.1
byte 2537

```

- 4 Repeat this procedure for the NSX Edge device `sfo01w01esg02`.

Deploy the Universal Distributed Logical Router for Consolidated SDDC

Deploy the Universal distributed logical router (UDLR).

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to <https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>
 - b Log i.n using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to create a new UDLR,
The New NSX Edge wizard appears.

- 6 On the Name and description page, enter the following settings, and click **Next**.

Setting	Value
Universal Logical (Distributed) Router	Selected
Name	sfo01w01udlr01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

- 7 On the Settings page, enter the following settings, and click **Next**.

Setting	Value
User Name	admin
Password	<i>udlr_admin_password</i>
Confirm password	<i>udlr_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

- 8 On the Configure deployment page, and click the **Add** icon.

The Add NSX Edge Appliance dialog box appears.

- 9 In the Add NSX Edge Appliance dialog box, enter the following settings and click **Next**.

Setting	Value
Cluster/Resource Pool	sfo01-w01rp-sddc-edge
Datastore	sfo01-w01-vsan01
Folder	sfo01-w01fd-nsx

- 10 On the Configure deployment page, and click the **Add** icon a second time to add a second NSX Edge device.

The Add NSX Edge Appliance dialog box appears.

- 11 In the Add NSX Edge Appliance dialog box, enter the following settings and click **Next**.

Setting	Value
Resource Pool	sfo01-w01rp-sddc-edge
Datastore	sfo01-w01-vsan01
Folder	sfo01-w01fd-nsx

- 12 On the Configure interfaces page, under **HA Interface Configuration**, click **Select** and connect to **sfo01-w01-vds01-Management**.

- 13 On the Configure interfaces page enter the following configuration settings and click **Next**.

Setting	Value
Primary IP Address	1.1.1.1
Subnet Prefix Length	29

Setting	Value
---------	-------

- a Click the **Add** icon. The Add Interface dialog box appears.
- b Enter the following settings in the Add Interface dialog box, and click **OK**.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	SFO01W01 Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.100.3
Subnet Prefix Length	24
MTU	9000

- 14 In the Default gateway settings page, deselect **Configure Default Gateway** and click **Next**.
- 15 In the Ready to complete page, click **Finish**.

Configure Universal Distributed Logical Router for Dynamic Routing for Consolidated SDDC

Configure the Universal distributed logical router (UDLR) to use dynamic routing in management and workload consolidation.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Enable HA logging.
 - a Double-click the device labeled **sfo01w01udlr01**.
 - b Click the **Manage** tab and click the **Settings** tab.
 - c Click **Change** in the HA Configuration window.
 - d Select the **Enable Logging** checkbox and click **OK**.
- 6 Create a firewall rule to allow SSH access to sfo01w01udlr01.
 - a Click the **Manage** tab and click the **Firewall** tab.
 - b Click **Add rule** in the **Firewall Section**.
 - c In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to **SSH**.
 - d In the **Source** column, leave the default **any**.

- e In the **Destination** column, leave the default **any**
 - f Click the **Edit** icon in the **Service** column, enter **SSH** in the filter, add **SSH** to the **Selected Objects** list, and click **OK**.
 - g Click **Publish Changes**.
- 7 Configure the routing for the Universal Distributed Logical Router.
- a Double-click **sfo01w01udlr01**.
 - b Click the **Manage** tab, click **Routing** and select **Global Configuration**.
 - c Click the **Edit** button under **Routing Configuration**, select **Enable ECMP**, and click **OK**.
 - d Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK**.
 - e Click **Publish Changes**.
- 8 On the left, select **BGP** to configure it.
- a On the BGP page, click the **Edit** button.
The Edit BGP Configuration dialog box appears.
 - b In the Edit BGP Configuration dialog box, enter the following settings and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

☒ Enable BGP
☒ Enable Graceful Restart
(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)
☐ Enable Default Originate
(Enables/Disables the capability to advertise a default route to its neighbors.)
 Local AS * 65000

OK Cancel

- c Click the **Add** icon to add a Neighbor.
The New Neighbor dialog box appears.

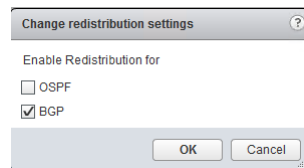
- d In the New Neighbor dialog box, enter the following values for both NSX Edge devices, and click **OK**.

Repeat this step two times to configure the UDLR for both NSX Edge devices: **sfo01w01esg01** and **sfo01w01esg02**.

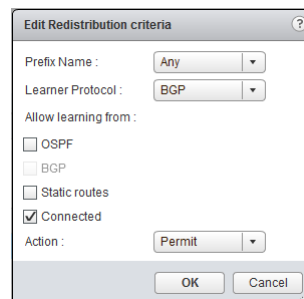
Setting	sfo01w01esg01 Value	sfo01w01esg02 Value
IP Address	192.168.100.1	192.168.100.2
Forwarding Address	192.168.100.3	192.168.100.3
Protocol Address	192.168.100.4	192.168.100.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- e Click **Publish Changes**.
- 9 On the left, select **Route Redistribution** to configure it.
- a Click the **Edit** button. In the Change redistribution settings dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected



- b On the Route Redistribution table, select the default **OSPF** entry and click the **Edit** button.
- c Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



- d Click **Publish Changes**.

Verify Establishment of BGP for the Universal Distributed Logical Router for Consolidated SDDC

Verify that the UDLR is successfully peering, and that BGP routing has been established.

Procedure

- 1 Log in to the sfo01w01udlr01 by using a Secure Shell (SSH) client.
 - a Open an SSH connection to sfo01w01udlr01, the UDLR whose peering and BGP configuration you want to verify.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	udlr_admin_password

- 2 Run the `show ip bgp neighbors` command to display information about the BGP and TCP connections to neighbors. The BGP State will display Established, UP if you have successfully peered with the Edge Service Gateway.

```

sfo01w01udlr01.sfo01.rainpole.local - PuTTY
NSX-edge-737e0e7b-8b99-430b-91fe-664f8ed64c4d-0> show ip bgp neighbors

BGP neighbor is 192.168.100.1, remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 1320054 messages, Sent 1320111 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0xd93dcffc
  Route refresh request:received 0 sent 0
  Prefixes received 25 sent 3 advertised 3
Connections established 2, dropped 3
Local host: 192.168.100.4, Local port: 179
Remote host: 192.168.100.1, Remote port: 50098

BGP neighbor is 192.168.100.2, remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 1320032 messages, Sent 1320100 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 2 Identifier 0xd93dcffc
  Route refresh request:received 0 sent 0
  Prefixes received 25 sent 3 advertised 3
Connections established 3, dropped 5
Local host: 192.168.100.4, Local port: 179
Remote host: 192.168.100.2, Remote port: 37125

NSX-edge-737e0e7b-8b99-430b-91fe-664f8ed64c4d-0>
  
```

- 3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that there are multiple routes to BGP learned networks. You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word `via` in the right-side column of the routing table output. In the image below there are two different routes to the following BGP networks: 0.0.0.0/0, 172.16.35.0/24, 172.16.31.0/24. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.

```

Codes: O - OSPF derived, I - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 27

B      0.0.0.0/0      [200/0]      via 192.168.100.1
B      0.0.0.0/0      [200/0]      via 192.168.100.2
C      1.1.1.0/29      [0/0]        via 1.1.1.1
B      10.159.4.0/23   [200/0]      via 192.168.100.1
B      10.159.4.0/23   [200/0]      via 192.168.100.2
C      169.254.1.0/30  [0/0]        via 169.254.1.1
B      172.11.10.0/24  [200/0]      via 192.168.100.1
B      172.11.10.0/24  [200/0]      via 192.168.100.2
B      172.11.11.0/24  [200/0]      via 192.168.100.1
B      172.11.11.0/24  [200/0]      via 192.168.100.2
B      172.11.12.0/24  [200/0]      via 192.168.100.1
B      172.11.12.0/24  [200/0]      via 192.168.100.2
B      172.16.11.0/24  [200/0]      via 192.168.100.1
B      172.16.11.0/24  [200/0]      via 192.168.100.2
B      172.16.31.0/24  [200/0]      via 192.168.100.1
B      172.16.31.0/24  [200/0]      via 192.168.100.2
B      172.16.35.0/24  [200/0]      via 192.168.100.1
B      172.16.35.0/24  [200/0]      via 192.168.100.2
B      172.17.11.0/24  [200/0]      via 192.168.100.1
B      172.17.11.0/24  [200/0]      via 192.168.100.2
B      172.17.35.0/24  [200/0]      via 192.168.100.1
B      172.17.35.0/24  [200/0]      via 192.168.100.2
B      172.18.11.0/24  [200/0]      via 192.168.100.1
B      172.18.11.0/24  [200/0]      via 192.168.100.2
B      172.18.12.0/24  [200/0]      via 192.168.100.1
B      172.18.12.0/24  [200/0]      via 192.168.100.2
B      172.18.16.0/24  [200/0]      via 192.168.100.1
B      172.18.16.0/24  [200/0]      via 192.168.100.2
B      172.18.17.0/24  [200/0]      via 192.168.100.1
B      172.18.17.0/24  [200/0]      via 192.168.100.2
B      172.18.18.0/24  [200/0]      via 192.168.100.1
byte 2281

```

Distributed Firewall Configuration for Consolidated SDDC

You define explicit rules for the distributed firewall which allows access to management applications and workloads in the consolidated cluster.

Add vCenter Server Instances to the NSX Distributed Firewall Exclusion List for Consolidated SDDC

Exclude vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX is not blocked.

You configure NSX Distributed Firewall using vCenter Server. If a rule prevents access between NSX Manager and vCenter Server, you will not be able to manage the distributed firewall. For this reason, you must exclude vCenter Server from all of your distributed firewall rules, ensuring that access between the two products is not blocked.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to <https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Exclude vCenter Server instance from firewall protection.
 - a In the Navigator, click **Networking & Security**.
 - b Click **NSX Managers** and select the **172.16.11.65** instance.
 - c Click **Manage** and then click **Exclusion List**.
 - d Click the **Add** button.
 - e Add **sfo01w01vc01** to the **Selected Objects** list, and click **OK**.

Create IP Sets for Management Components in the Consolidated Cluster for Consolidated SDDC

Create IP sets for all management applications in the consolidated cluster. You use the IP sets later to create security groups for use with the distributed firewall rules.

You perform this procedure multiple times to configure all of the necessary IP sets. You allocate one IP set per group of applications.

Table 2-5. IP Sets for the Management Components in the Consolidated Cluster

Name	IP Addresses
Platform Services Controller Instances	Platform-Service-Controller_IP's
vCenter Server Instances	vCenter-Server_IP's
vRealize Automation Appliances	vRealize-Automation-Appliances_IP's
vRealize Automation Windows	vRealize-Automation-Windows_IP's
vRealize Business Server	vRealize-Business_IP
vRealize Business Data Collector	vRealize-Business-Data-Collector_IP's
vSphere Data Protection	vSphere-Data-Protection_IP's
vRealize Operations Manager	vRealize-Operations-Manager_IP's
vRealize Operations Manager Remote Collectors	vRealize-Operations-Manager-Remote-Collectors_IP's
vRealize Log Insight	vRealize-Log-Insight_IP's
Update Manager Download Service	UMDS_IP's
SDDC	Management-VLAN_Subnets, Management-VXLAN_Subnets
Administrators	Administrator-Desktops_Subnet

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator, click **Networking & Security**.
- 3 Click **NSX Managers** and click the **172.16.11.66** instance.
- 4 Select **Manage** tab, click **Grouping Objects**, and click **IP Sets**.
- 5 Click the **Add** icon.

- 6 In the New IP Set dialog box, configure the values for the IP set that you are adding, and click **OK**.

Setting	Value
Name	Platform Services Controller Instances
IP Addresses	172.16.11.63
Mark this object for Universal Synchronization	Selected

- 7 Repeat this procedure to create IP sets for all of the remaining components.

Create Security Groups for Consolidated SDDC

Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

A security group is a collection of assets (or objects) from your vSphere inventory that you group together.

You perform this procedure multiple times to configure all of the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

Security Groups for the Management Clusters Components in the SDDC

Name	Object Type	Selected Object
Platform Services Controller Instances	IP Sets	Platform Services Controller Instances
vCenter Server Instances	IP Sets	vCenter Server Instances
vRealize Automation Appliances	IP Sets	vRealize Automation Appliances
vRealize Automation Windows	IP Sets	vRealize Automation Windows
vRealize Business Server	IP Sets	vRealize Business Server
vRealize Business Data Collector	IP Sets	vRealize Business Data Collector
vSphere Data Protection	IP Sets	vSphere Data Protection
vRealize Operations Manager	IP Sets	vRealize Operations Manager
vRealize Operations Manager Remote Collectors	IP Sets	vRealize Operations Manager Remote Collectors
vRealize Log Insight	IP Sets	vRealize Log Insight
Update Manager Download Service	IP Sets	Update Manager Download Service
SDDC	IP Sets	SDDC
Administrators	IP Sets	Administrators
Windows Servers	Security Groups	vRealize Automation Windows
VMware Appliances	Security Groups	<ul style="list-style-type: none"> ■ Platform Services Controller Instances ■ vCenter Server Instances ■ vRealize Automation Appliances ■ vRealize Business Server ■ vRealize Business Data Collector ■ vSphere Data Protection ■ vRealize Operations Manager ■ vRealize Operations Manager Remote Collectors ■ vRealize Log Insight

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.
- 3 Select the **172.16.11.66** NSX Manager instance, and click the **Manage** tab.
- 4 Click **Grouping Objects**, select **Security Group**, and click the **Add new Security Group** icon.
The Add Security Group wizard appears.
- 5 On the Name and description page, enter **Platform Services Controller Instances** in the **Name** text box, select **Mark this object for Universal Synchronization** and **Use for active standby deployments**. Click **Next**.
- 6 On the Define dynamic membership page, click **Next**.
- 7 On the Select objects to include page, select **IP Sets** from the **Object Type** drop-down menu, select **Platform Services Controller Instances** from the list of **Available objects**, click the **Add** button, and click **Next**.
- 8 On the Ready to Complete page, verify the configuration values that you entered and click **Finish**.
- 9 Repeat this procedure to create all of the necessary security groups.

Create Distributed Firewall Rules for Consolidated SDDC

Create firewall rules that allow administrators to connect to the different VMware solutions.

Also create rules to allow user access to the vRealize Automation portal and to provide external connectivity to the SDDC.

A firewall rule consists of a section to segregate the firewall rules and the rule itself, which defines what network traffic is, or is not, blocked.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add a section for the rules for the management applications.
 - a In the **Navigator**, click **Networking & Security** and click **Firewall**.
 - b From the **NSX Manager** drop-down menu, select **172.16.11.66**.

- c Click the **Add Section** icon.
- d In the Add New Section dialog box, enter **VMware Management Services** in the **Section Name** text box, select the **Mark this section for Universal Synchronization** check box. Click **Save**.
- 3 Create a distributed firewall rule to allow SSH access to administrators for the different VMware appliances.
 - a Click **Add rule** in the VMware Management Services section.
 - b In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to **Allow SSH to admins**.
 - c Click the **Edit** icon in the **Source** column, change the **Object Type** to **Security Groups**, add **Administrators** to the **Selected Objects** list, and click **OK**.
 - d Click the **Edit** icon in the **Destination** column, change the **Object Type** to **Security Groups**, add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **OK**.
 - e Click the **Edit** icon in the **Service** column, enter **SSH** in the filter, add **SSH** to the **Selected Objects** list, and click **OK**.
 - f Click **Publish Changes**.
- 4 Repeat the previous step to create the following distributed firewall rules.

Name	Source	Destination	Service / Port
Allow vRA Portal to end users	* any	vRealize Automation Appliances	HTTP, HTTPS
Allow vRA Console Proxy to end users	* any	vRealize Automation Appliances	TCP:8444
Allow SDDC to any	SDDC	* any	* any
Allow PSC to admins	Administrators	Platform Services Controller Instances	HTTPS
Allow SSH to admins	Administrators	<ul style="list-style-type: none"> ■ VMware Appliances ■ Update Manager Download Service 	SSH
Allow RDP to admins	Administrators	Windows Servers	RDP
Allow Orchestrator to admins	Administrators	vRealize Automation Appliances	TCP:8281,8283
Allow vROPs to admins	Administrators	vRealize Operations Manager	HTTP, HTTPS
Allow vRLI to admins	Administrators	vRealize Log Insight	HTTP, HTTPS
Allow VAMI to admins	Administrators	VMware Appliances	TCP:5480
Allow VDP to admins	Administrators	vSphere Data Protection	TCP:8543

- 5 Create a distributed firewall rule to deny all other traffic to the management subnets.
 - a Click **Add rule** in the VMware Management Services section.
 - b In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to **Deny Management subnets**.
 - c Click the **IP** icon in the **Destination** column, enter **172.16.11.0/24,192.168.11.0/24,192.168.31.0/24** and click **OK**.
 - d Click the **Edit** icon in the **Action** column and change the action to **Block** and click **Save**.
 - e Click **Publish Changes**.

By allowing only the network traffic that is required by the SDDC to pass, network security is improved.

Test the Consolidated Cluster NSX Configuration for Consolidated SDDC

Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other over the network.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Use the Ping Monitor to test connectivity.
 - a In the Navigator, click **Networking & Security** and click **Logical Switches**
 - b Double-click **SFO01W01 Universal Transit Network**.
 - c Click the **Monitor** tab.
 - d From the **Source host** drop-down menu select **sfo01w01esx01.sfo01.rainpole.local**.
 - e From the **Destination host** drop-down menu select **sfo01w01esx03.sfo01.rainpole.local**.
 - f Click **Start Test** button.

The host-to-host ping test results are displayed in the **Results** text box. Verify that there are no error messages.

Deploy Application Virtual Networks for Consolidated SDDC

Deploy the application virtual networks for your management and workload consolidation deployment.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Universal Logical Switch for workloads that move between sites.
 - a In the Navigator, click **Networking & Security** and click **Logical Switches**.
 - b Select **172.16.11.66** from the **NSX Manager** drop-down menu.

- c Click the **Add** icon to create a new Logical Switch.
- d In the New Logical Switch dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-xRegion01-VXLAN
Transport Zone	SFO01W01 Universal Transport Zone
Replication Mode	Hybrid

New Logical Switch

Name: * Mgmt-xRegion01-VXLAN

Description:

Transport Zone: * SFO01W01 Universal Transport Zone [Change](#) [Remove](#)

Replication mode:

- ☐ Multicast
Multicast on Physical network used for VXLAN control plane.
- ☐ Unicast
VXLAN control plane handled by NSX Controller Cluster.
- ☒ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

☒ Enable IP Discovery

☐ Enable MAC Learning

OK **Cancel**

- 3 Create a Universal Logical Switch for workloads that specific to Workload and Management Consolidation.
 - a In the Navigator, click **Networking & Security** and click **Logical Switches**.
 - b Select **172.16.11.66** from the **NSX Manager** drop-down menu.

- c Click the **Add** icon to create a new Logical Switch.
- d In the New Logical Switch dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-RegionA01-VXLAN
Transport Zone	SFO01W01 Universal Transport Zone
Replication Mode	Hybrid

- 4 Connect the **Mgmt-xRegion01-VXLAN** to the **UDLR01** Universal Distributed Logical Router.
 - a On the Logical Switches page, select the **Mgmt-xRegion01-VXLAN** logical switch.
 - b Click the **Connect Edge** icon.
 - c On the Connect an Edge page, select **sfo01w01udlr01** and click **Next**.
 - d On the Edit NSX Edge Interface page, enter the following settings and click **Next**.

Setting	Value
Name	Mgmt-xRegion01-VXLAN
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.1
Subnet Prefix Length	24

- e On the Ready to Complete page click **Finish**.
- 5 Connect the **Mgmt-RegionA01-VXLAN** to the **UDLR01** Universal Distributed Logical Router.
 - a On the Logical Switches page, select the **Mgmt-RegionA01-VXLAN** logical switch.
 - b Click the **Connect Edge** icon.
 - c On the Connect an Edge page, select **sfo01w01udlr01** and click **Next**.

- d On the Edit NSX Edge Interface page, enter the following settings and click **Next**.

Setting	Value
Name	Mgmt-RegionA01-VXLAN
Type	Internal
Connected To	Mgmt-RegionA01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.31.1
Subnet Prefix Length	24

- e On the Ready to Complete page click **Finish**.

6 Configure the MTU for the Logical Switches.

- a On the NSX Edges page, double-click **sfo01w01udlr01**.
- b Click the **Manage** tab, and click **Settings**.
- c On the Settings page, click **Interfaces**.
- d Under Interfaces, select **Mgmt-xRegion01-VXLAN**, and click **Edit**.
- e On the Edit Logical Router Interface dialog box, specify a value of **9000** for the **MTU** value, and click **OK**.
- f Repeat the same steps to change **MTU** value for **Mgmt-RegionA01-VXLAN**.

Setting	Value
Mgmt-xRegion01-VXLAN	9000
Mgmt-RegionA01-VXLAN	9000

Edit Logical Router Interface

Name: * Mgmt-xRegion01-VXLAN

Type: ☒ Internal ☐ Uplink

Connected To: * Mgmt-xRegion01-VXLAN [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Configure Subnets:

Primary IP Address	Subnet Prefix Length
192.168.11.1	24

1 items [Copy](#)

MTU: 9000

[OK](#) [Cancel](#)

Deploy the NSX Load Balancer for Consolidated SDDC

Deploy a load balancer for use by the management applications connected to the application virtual network, Mgmt-xRegion01-VXLAN

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under Inventories, click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to create an NSX Edge.
The New NSX Edge wizard appears.
- 6 On the Name and description page, enter the following settings and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	sfo01w01lb01
Deploy NSX Edge	Selected
Enable High Availability	Selected

- 7 On the Settings page, enter the following settings and click **Next**.

Setting	Value
User Name	admin
Password	edge_admin_password
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

- 8 On the Configure deployment page, perform the following configuration steps and click **Next**.
 - a Select **sfo01-w01dc**, from the **Datacenter** drop-down menu.
 - b Click **Large** to specify the **Appliance Size**.

- c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	sfo01-w01rp-sddc-edge
Datastore	sfo01-w01-vsan01
Folder	sfo01-w01fd-nsx

- d To create a second appliance, click the **Add** icon again, make the same selections in the New NSX Appliance dialog box, and click **OK**.

- 9 On the Configure Interfaces page, click the **Add** icon to configure the OneArmLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

Add NSX Edge Interface

vNIC#: 0

Name: * OneArmLB

Type: ☒ Internal ☐ Uplink

Connected To: Mgmt-xRegion01-VXLAN [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.11.2		24

1 items [Copy](#)

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 9000

Options: ☐ Enable Proxy ARP ☒ Send ICMP Redirect

Reverse Path Filter: **Enabled**

Fence Parameters:

Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

- 10 On the Default gateway settings page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	192.168.11.1
MTU	9000

- 11 On the Firewall and HA page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable

Setting	Value
vNIC	any
Declare Dead Time	15

- 12 On the Ready to complete page, review the configuration settings you entered and click **Finish**.
- 13 Enable HA logging.
 - a In the Navigator, click **NSX Edges**.
 - b Select **172.16.11.66** from the **NSX Manager** drop-down menu.
 - c Double-click the device labeled **sfo01w01lb01**.
 - d Click the **Manage** tab and click the **Settings** tab, and select **Configuration**.
 - e Click **Change** in the HA Configuration window.
 - f Select the **Enable Logging** checkbox and click **OK**.
- 14 Enable the Load Balancer service.
 - a In the Navigator, click **NSX Edges**.
 - b Select **172.16.11.66** from the **NSX Manager** drop-down menu.
 - c Double-click the device labeled **sfo01w01lb01**.
 - d Click the **Manage** tab, click the **Load Balancer** tab, click **Global Configuration**, and click **Edit**.
 - e In the Edit load balancer global configuration dialog box, select **Enable Load Balancer**, select **Logging** and select **Info** as the **Log Level** and click **OK**.

Deploy vSphere Data Protection in the Consolidated SDDC

Deploy vSphere Data Protection to provide the capability for backup and restore of SDDC management components.

vSphere Data Protection enables the backup and restore of virtual machines associated with the following components.

- vCenter Server
- Platform Services Controller
- vRealize Automation
- vRealize Operations Manager
- vRealize Log Insight
- vSphere Update Manager Download Service (UMDS)

Procedure

- 1 [Prerequisites for Deploying vSphere Data Protection for Consolidated SDDC](#) on page 78
Before you deploy vSphere Data Protection, verify that your environment satisfies the requirements for this deployment.
- 2 [Deploy the vSphere Data Protection Virtual Appliance for Consolidated SDDC](#) on page 79
Deploy vSphere Data Protection as a virtual appliance on the consolidated pod.
- 3 [Enable SSH Root User Access on the vSphere Data Protection Appliance for Consolidated SDDC](#) on page 81
Enable the login to the vSphere Data Protection appliance in the Consolidated SDDC over Secure Shell (SSH) as the root user. You connect to the appliance over SSH to install custom certificates and to perform troubleshooting operations.
- 4 [Replace vSphere Data Protection Certificates for Consolidated SDDC](#) on page 82
After you use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in the Consolidated SDDC with the certificate that is generated by CertGenVVD.
- 5 [Configure a Service Account in vSphere for Integration with vSphere Data Protection for Consolidated SDDC](#) on page 83
Configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on vCenter Server in the Consolidated SDDC.
- 6 [Register vSphere Data Protection with vCenter Server for Consolidated SDDC](#) on page 86
After you deploy the virtual appliance for vSphere Data Protection on the consolidated cluster, complete the initial configuration of vSphere Data Protection.

Prerequisites for Deploying vSphere Data Protection for Consolidated SDDC

Before you deploy vSphere Data Protection, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP address and FQDN for vSphere Data Protection are available for the SDDC deployment.

Table 2-6. IP Addresses and Host Names for vSphere Data Protection

Network Setting	Value
IP address	172.16.11.81
FQDN	sfo01w01vdp01.sfo01.rainpole.local
Primary DNS server	172.16.11.4
Secondary DNS server	172.16.11.5
Default gateway	172.16.11.253
Subnet mask	255.255.255.0

Deployment Prerequisites

Verify that you have fulfilled the following prerequisites in addition to the networking settings.

Prerequisite	Value
Initial Storage	<ul style="list-style-type: none"> ■ Virtual disk provisioning. <ul style="list-style-type: none"> ■ Thin ■ Required storage <ul style="list-style-type: none"> ■ 6 TB
Software Features	<ul style="list-style-type: none"> ■ vSphere <ul style="list-style-type: none"> ■ Consolidated vCenter Server ■ Consolidated cluster with enabled DRS and HA. ■ vSphere Distributed Switch configured for the vSphere management network
Installation Package	Download the vSphere Data Protection virtual appliance .ova file to the machine where you use the vSphere Web Client.

Deploy the vSphere Data Protection Virtual Appliance for Consolidated SDDC

Deploy vSphere Data Protection as a virtual appliance on the consolidated pod.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the vSphere Web Client, navigate to the sfo01-w01-consolidated01 cluster object.

Inventory Object	Value
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Data center	sfo01-w01dc
Cluster	sfo01-w01-consolidated01

- 3 Right-click the **sfo01-w01-consolidated01** object and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, browse to the location of the vSphere Data Protection OVA file on your file system, and click **Next**.

- 5 On the Select name and location page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	sfo01w01vdp01
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Data center	sfo01-w01dc

- 6 On the Select a resource page, click the **Browse** tab, select the **sfo01-w01-consolidated01** cluster, and click **Next**.
- 7 On the Review details page, examine the virtual appliance details, such as product name, product version, download size, and size on disk, and click **Next**.
- 8 On the Accept license agreements page, accept the end user license agreement and click **Next**.
- 9 On the Select storage page, select the NFS datastore that is provisioned for vSphere Data Protection, configure storage settings, and click **Next**.

Setting	Value
Datastore	<i>secondary_storage</i>
Select virtual disk format	Thin provision
VM storage policy	None

- 10 On the Select networks page, select the **sfo01-w01-vds01-management-vm** distributed port group from the **Isolated Network** drop-down menu, select **IPv4** from the **IP protocol** drop-down menu, and click **Next**.
- 11 On the Customize template page, enter the networking settings for the virtual appliance and click **Next**.

IPv4 Setting	Value
DNS	172.16.11.5, 172.16.11.4
Default Gateway	172.16.11.253
Network 1 IP address	172.16.11.81
Network 1 Netmask	255.255.255.0

- 12 On the Ready to complete page, verify that the settings are correct and click **Finish**.
- 13 After the virtual appliance is deployed, right-click the virtual appliance object in the vSphere Web Client and select **Power > Power On**.

Enable SSH Root User Access on the vSphere Data Protection Appliance for Consolidated SDDC

Enable the login to the vSphere Data Protection appliance in the Consolidated SDDC over Secure Shell (SSH) as the root user. You connect to the appliance over SSH to install custom certificates and to perform troubleshooting operations.

Procedure

- 1 Log in to the Consolidated vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 Navigate to the vSphere Data Protection virtual appliance sfo01w01vdp01.
- 3 Right-click **sfo01w01vdp01** and select **Open Console** to open the remote console to the appliance.
- 4 Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vdp_default_root_password</i>

- 5 Run the following console command to open the `sshd_config` file for editing.
`vi /etc/ssh/sshd_config`
- 6 Remove the # comment from the beginning of the line `#PermitRootLogin yes`.

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

- 7 Run the following command in the vi editor to save the file and exit the editor.
`:wq!`
- 8 In the console, restart the SSH service to update the running configuration.
`/etc/init.d/sshd restart`
- 9 Log out and close the console to the appliance.

Replace vSphere Data Protection Certificates for Consolidated SDDC

After you use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in the Consolidated SDDC with the certificate that is generated by CertGenVVD.

Procedure

- 1 Log in to the vSphere Data Protection appliance.
 - a Open an SSH connection to the virtual machine sfo01w01vdp01.sfo01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vdp_root_password</i>

- 2 Stop the vSphere Data Protection Web services by running the following command.

```
emwebapp.sh --stop
```

NOTE If you see errors related to database server, ignore them.

- 3 Delete the tomcat alias from the Java keystore by running the following command.
- 4 Copy the **.keystore** file generated by CertGenVVD tool to the /tmp folder on the vSphere Data Protection virtual appliance.

You can use FileZilla or WinSCP.

- 5 Run the following command to insert the new certification chain in to the keystore.

```
/usr/java/latest/bin/keytool -importkeystore -srckeystore /tmp/.keystore --
destkeystore /root/.keystore -srcstorepass changeit -deststorepass changeit
```

- 6 Run the following command and in the command output verify that the certificate entry with the tomcat alias exists in the keystore.

```
/usr/java/latest/bin/keytool -list -v -keystore /root/.keystore -storepass changeit -keypass
changeit
```

- 7 If the certificate entry exists in the keystore, run the addFingerprint.sh script to update the vSphere Data Protection server thumbprint.

```
/usr/local/avamar/bin/addFingerprint.sh
```

- 8 Start the vSphere Data Protection Web services by running the following command.

```
emwebapp.sh --start
```

- 9 Run the following command to remove the /tmp/.keystore file.

```
rm /tmp/.keystore
```

Configure a Service Account in vSphere for Integration with vSphere Data Protection for Consolidated SDDC

Configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on vCenter Server in the Consolidated SDDC.

You associate the svc-udp service account in the Active Directory with a user role that has certain privileges. You assign the user to the Consolidated vCenter Server.

Define a User Role in vSphere for Integration with vSphere Data Protection for Consolidated SDDC

In vSphere, create a user role with privileges that are required for performing backup operations against the management virtual machines in vSphere Data Protection for the Consolidated SDDC.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 On the Home page of the vSphere Web Client, select **Roles** under Administration.

- 3 Create a new role for managing backups.
 - a On the Roles page, click the **Create role action** icon.
 - b In the Create Role dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	vSphere Data Protection User
Privilege	<ul style="list-style-type: none"> ■ Alarms.Create alarm ■ Alarms.Modify alarm ■ Datastore.Allocate space ■ Datastore.Browse datastore ■ Datastore.Configure datastore ■ Datastore.Low level file operations ■ Datastore.Move datastore ■ Datastore.Remove datastore ■ Datastore.Remove file ■ Datastore.Rename datastore ■ Extension.Register extension ■ Extension.Update extension ■ Folder.Create folder ■ Global.Cancel task ■ Global.Disable methods ■ Global.Enable methods ■ Global.Licenses ■ Global.Log event ■ Global.Manage custom attributes ■ Global.Settings ■ Network.Assign network ■ Network.Configure ■ Resource.Assign virtual machine to resource pool ■ Sessions.Validate session ■ Tasks.Create task ■ Tasks.Update task ■ Virtual Machine.Configuration.Add existing disk ■ Virtual Machine.Configuration.Add new disk ■ Virtual Machine.Configuration.Add or remove device ■ Virtual Machine.Configuration.Advanced ■ Virtual Machine.Configuration.Change CPU count ■ Virtual Machine.Configuration.Change resource ■ Virtual Machine.Configuration.Disk change tracking ■ Virtual Machine.Configuration.Disk lease ■ Virtual Machine.Configuration.Extend virtual disk ■ Virtual Machine.Configuration.Host USB device ■ Virtual Machine.Configuration.Memory ■ Virtual Machine.Configuration.Modify device settings ■ Virtual Machine.Configuration.Raw device ■ Virtual Machine.Configuration.Reload from path ■ Virtual Machine.Configuration.Remove disk ■ Virtual Machine.Configuration.Rename ■ Virtual Machine.Configuration.Reset guest information ■ Virtual Machine.Configuration.Set annotation ■ Virtual Machine.Configuration.Settings ■ Virtual Machine.Configuration.Swapfile placement

Setting	Value
	<ul style="list-style-type: none"> ■ Virtual Machine.Configuration.Upgrade virtual machine compatibility ■ Virtual Machine.Guest Operations.Guest operation modifications ■ Virtual Machine.Guest Operations.Guest operation program execution ■ Virtual Machine.Guest Operations.Guest operation queries ■ Virtual Machine.Interaction.Console interaction ■ Virtual Machine.Interaction.Device connection ■ Virtual Machine.Interaction.Guest operating system management by VIX API ■ Virtual Machine.Interaction.Power off ■ Virtual Machine.Interaction.Power on ■ Virtual Machine.Interaction.Reset ■ Virtual Machine.Interaction.VMware Tools install ■ Virtual Machine.Inventory.Create new ■ Virtual Machine.Inventory.Register ■ Virtual Machine.Inventory.Remove ■ Virtual Machine.Inventory.Unregister ■ Virtual Machine.Provisioning.Allow disk access ■ Virtual Machine.Provisioning.Allow read-only disk access ■ Virtual Machine.Provisioning.Allow virtual machine download ■ Virtual Machine.Provisioning.Mark as template ■ Virtual Machine.Snapshot management.Create snapshot ■ Virtual Machine.Snapshot management.Remove snapshot ■ Virtual Machine.Snapshot management.Revert to snapshot ■ vApp.Export ■ vApp.Import ■ vApp.vApp application configuration

This role inherits the **System.Anonymous System.View**, and **System.Read** permissions.

The Consolidated vCenter Server propagates the role to other linked vCenter Server instances.

Configure User Privileges in vSphere for Integration with vSphere Data Protection for Consolidated SDDC

Assign global permissions in the Consolidated SDDC to the operations service account svc-vdp so that you can manage and perform backups by using vSphere Data Protection.

The svc-vdp user has access rights that are specifically required for performing backups vCenter Server inventory.

Prerequisites

- Verify that the Consolidated vCenter Server is connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available on the Consolidated vCenter Server.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the svc-vdp@rainpole.local service account.
 - a In the vSphere Web Client, select navigate **Administration** from the **Home** menu and click **Global Permissions** under Access Control.
 - b On the **Manage** tab, click the **Add Permission** icon.
 - c In the Global Permissions Root - Add Permission dialog box, click the **Add** button to associate a user or a group with a role.
 - d In the Select Users/Groups dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
 - e From the list of users and groups, select the **svc-vdp** user, click **Add** button, and click **OK**.
 - f In the Global Permissions Root - Add Permission dialog box, from the **Assigned Role** drop-down menu, select **vSphere Data Protection User**, select **Propagate to children**, and click **OK**.

Register vSphere Data Protection with vCenter Server for Consolidated SDDC

After you deploy the virtual appliance for vSphere Data Protection on the consolidated cluster, complete the initial configuration of vSphere Data Protection.

Procedure

- 1 Log in to the vSphere Data Protection Configure Utility.
 - a Open a Web browser and go to **<https://sfo01w01vdp01.sfo01.rainpole.local:8543/vdp-configure>**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	changeme

- 2 On the Welcome page, click **Next**.
- 3 On the Network Settings page, verify that the network settings are populated correctly and click **Next**.
- 4 On the Time Zone page, select the **UTC** time zone and click **Next**.
- 5 On the VDP Credentials page, enter and confirm a new password for the root Linux appliance user, and click **Next**.

The password must satisfy the following requirements:

- If all four character classes are used, the password must be at least 6 characters.
- If three character classes are used, the password must be at least 7 characters.
- If one or two character classes are used, the password must be at least 8 characters.
- The four-character classes are as follows:
 - Upper case letters A-Z
 - Lower case letters a-z
 - Numbers 0-9
 - Special characters (for example: ~!@#%,.)

- 6 On the vCenter Registration page, configure the settings for registration with the Consolidated vCenter Server.

- a Enter the settings for connection to the Consolidated vCenter Server.

vCenter Server Setting	Value
vCenter username	rainpole.local\svc-vdp
vCenter password	<i>svc-vdp_password</i>
vCenter FQDN or IP	sfo01w01vc01.sfo01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter certificate	Deselected

- b Enter the settings for vCenter Single Sign-On on the Consolidated Platform Services Controller.

Single Sign-On Setting	Value
Use vCenter for SSO authentication	Deselected
SSO FQDN or IP	sfo01w01psc01.sfo01.rainpole.local
SSO port	443

- c Click **Test Connection**, and in the success message box, click **OK**.
 - d On the vCenter Registration page, click **Next**.
- 7 On the Create Storage page, select **Create new storage**, in the **Capacity** text box, enter **4 TiB** and click **Next**.
- 8 On the Device Allocation page, from the **Provision** drop-down menu, select **Thin** and click **Next**.
- 9 On the CPU and Memory page, leave the default settings and click **Next**.
- 10 On the Product Improvement page, select **Enable Customer Experience Improvement Program** and click **Next**.
- 11 On the Ready to Complete page, select the **Run performance analysis on storage configuration** and **Restart the appliance if successful** check boxes, and click **Next**.
- 12 In the Warning message box about storage configuration, click **Yes**.
vSphere Data Protection setup starts configuring data disks.
- 13 After disk configuration is complete, click **OK** in the success box.
- 14 Verify that the vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration of vSphere Data Protection.
 - a Open a Web browser and go to <https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- c On the vSphere Web Client Home page, verify that the **VDP** icon is available and that you can connect to the appliance.

Cloud Management Platform Implementation for Consolidated SDDC

3

The Cloud Management Platform (CMP) consists of integrated products that support the management of public, private and hybrid cloud environments. The VMware CMP consists of vRealize Automation, an embedded vRealize Orchestrator, and vRealize Business for Cloud.

vRealize Automation incorporates virtual machine provisioning and a self-service portal. vRealize Business enables billing and chargeback functions. vRealize Orchestrator provides workflow optimization. The following procedures describe the validated flow of installation and configuration.

This chapter includes the following topics:

- [“Prerequisites for Cloud Management Platform Implementation for Consolidated SDDC,”](#) on page 89
- [“Configure Service Account Privileges for Consolidated SDDC,”](#) on page 97
- [“vRealize Automation Installation for Consolidated SDDC,”](#) on page 99
- [“vRealize Automation Default Tenant Configuration for Consolidated SDDC,”](#) on page 122
- [“vRealize Automation Tenant Creation for Consolidated SDDC,”](#) on page 125
- [“Embedded vRealize Orchestrator Configuration for Consolidated SDDC,”](#) on page 135
- [“Install vRealize Business for Consolidated SDDC,”](#) on page 145
- [“Cloud Management Platform Post-Installation Tasks for Consolidated SDDC,”](#) on page 153
- [“Tenant Content Creation for Consolidated SDDC,”](#) on page 155

Prerequisites for Cloud Management Platform Implementation for Consolidated SDDC

Verify that the following configurations are established prior to beginning the procedures to deploy and configure the Cloud Management Platform (CMP).

DNS Entries and IP Address Mappings for Consolidated SDDC

Before you deploy vRealize Automation, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that the static IP address and FQDNs that are listed in the table below are available for the vRealize Automation application virtual network for the SDDC deployment.

Table 3-1. IP Addresses and FQDNs for the vRealize Automation Instance for Management and Workload Consolidation

Role	IP Address	FQDN
vRealize Automation Server Appliances	192.168.11.51	vra01svr01a.rainpole.local
vRealize Automation Server VIP	192.168.11.53	vra01svr01.rainpole.local
vRealize Automation for IWS	192.168.11.54	vra01iws01a.rainpole.local
vRealize Automation IWS VIP	192.168.11.56	vra01iws01.rainpole.local
vRealize Automation Model Manager IMS	192.168.11.57	vra01ims01a.rainpole.local
vRealize Automation IMS VIP	192.168.11.59	vra01ims01.rainpole.local
MS SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
vRealize Business for Cloud Server Appliance	192.168.11.66	vr01svr01.rainpole.local

Table 3-2. IP Address Information and FQDN for the Supporting Infrastructure for Management and Workload Consolidation

Role	IP Address	FQDN
vRealize Business for Cloud Data Collector	192.168.31.54	sfo01vrbc01.sfo01.rainpole.local
Default gateway	192.168.31.1	
DNS server	172.16.11.5	
Subnet mask	255.255.255.0	
ntp	172.16.11.251 172.16.11.252	ntp.sfo01.rainpole.local

vRealize Automation Deployment Prerequisites

Before you install and use vRealize Automation, your environment must meet the following prerequisites.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> Virtual disk provisioning. Required storage per node.
Operating system	Windows 2012 R2 Standard
Database	Microsoft SQL Server 2012 Standard Edition
Installation package	Download the vRealize Automation virtual appliance .ova file. Download the vRealize Business for Cloud virtual appliance .ova file.
License	Verify that you have obtained a license that covers the use of vRealize Automation. Verify that you have obtained a license that covers the use of vRealize Business for vRealize Automation.
Active directory	Verify that you have a parent Active Directory instance with the SDDC user roles configured for the rainpole.local domain. Verify the existence of the svc-vra user in the rainpole.local domain. Verify the existence of the svc-vro user in the rainpole.local domain.
Certification authority	Configure the root Active Directory domain controller as a certificate authority for the environment.
Java	Install Java SE Development Kit (JDK), which is required to run the vRealize Orchestrator Client.

Configure SQL Server for Use by the Cloud Management Platform for Consolidated SDDC

The Cloud Management Platform uses a Microsoft SQL Server database to store data for use by vRealize Automation.

Configuration Recommendations for Microsoft SQL Server for Consolidated SDDC

vRealize Automation and other VMware components use Microsoft SQL Server as a database to store information. While the specific configuration of SQL Server for use in your environment is not addressed in this implementation guide, high-level guidance is provided to ensure more reliable operation of your VMware components.

- Microsoft SQL Server should be configured with separate Operating System Level volumes (drive letters) for each of the following items. The separation of these items into separate logical volumes (drive letters) will help prevent database corruption should a single volume reach capacity.
 - Operating System
 - Database Application
 - SQL User Database Data Files
 - SQL User Database Log Files
 - SQL TempDB
 - SQL Backup Files
- To provide optimal performance for VMware vRealize databases, configure the SQL Server virtual machine (`vra01mssql01.rainpole.local`) with 8 vCPU and 16GB vRAM.
- Configure the SQL Server virtual machine's (`vra01mssql01.rainpole.local`) primary DNS to point to 172.16.11.4 and its secondary DNS to point to 172.16.11.5.

For further guidance on the deployment and operation of a production installation of Microsoft SQL Server, see the Microsoft SQL Server documentation, or consult with a qualified Microsoft SQL Server database administrator.

Assign the SQL Server System Role to vRealize Automation for Consolidated SDDC

Assign the SQL Server system role **sysadmin** to the vRealize Automation service account.

vRealize Automation uses the SQL Server system role privilege to create and execute scripts on the SQL Server database. By default, only users who are members of the **sysadmin** system role, or the **db_owner** and **db_ddladmin** database roles, can create objects in the database.

Procedure

- 1 Log in to the `VRA01MSSQL01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

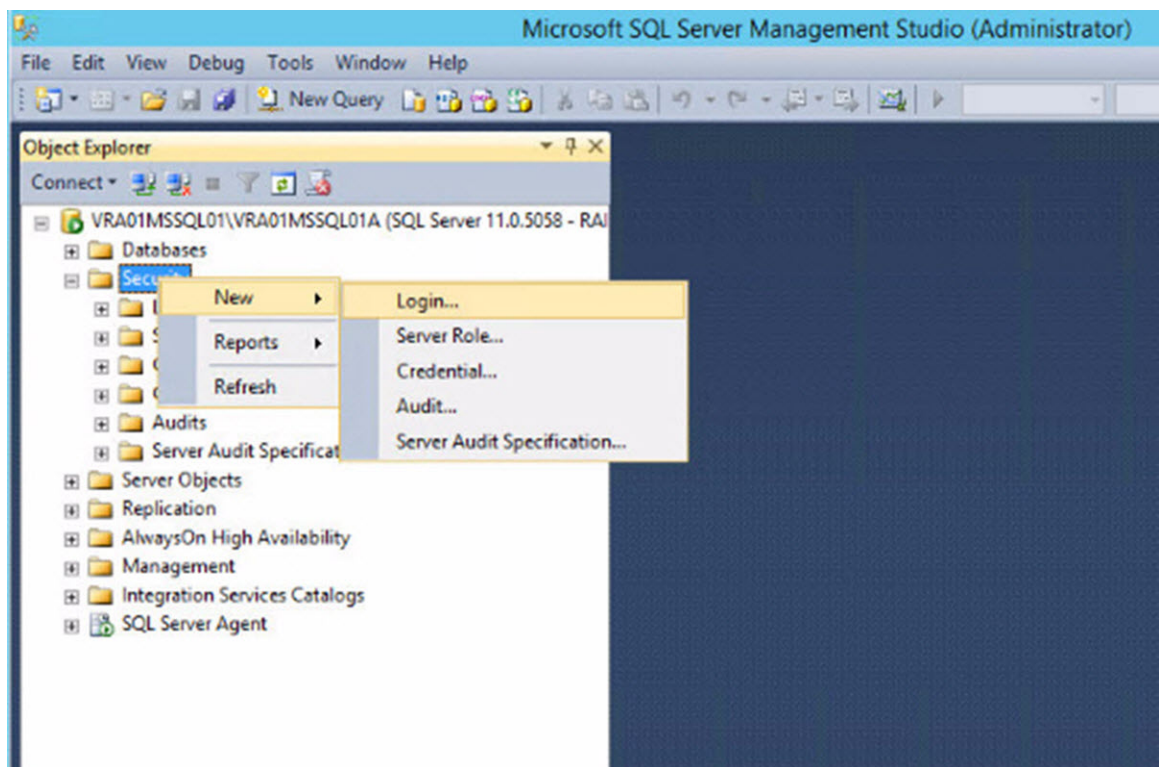
- 2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

NOTE If SQL Server Management Studio doesn't appear in your **All Programs** menu, you may not have successfully installed SQL Server Management Studio. Verify that you have successfully installed SQL Server Management Studio, and then continue with this procedure.

- 3 In the Connect to Server dialog box, leave the default value of the **Server Name** text box, select **Windows Authentication** from the **Authentication** drop-down menu, and click **Connect**.

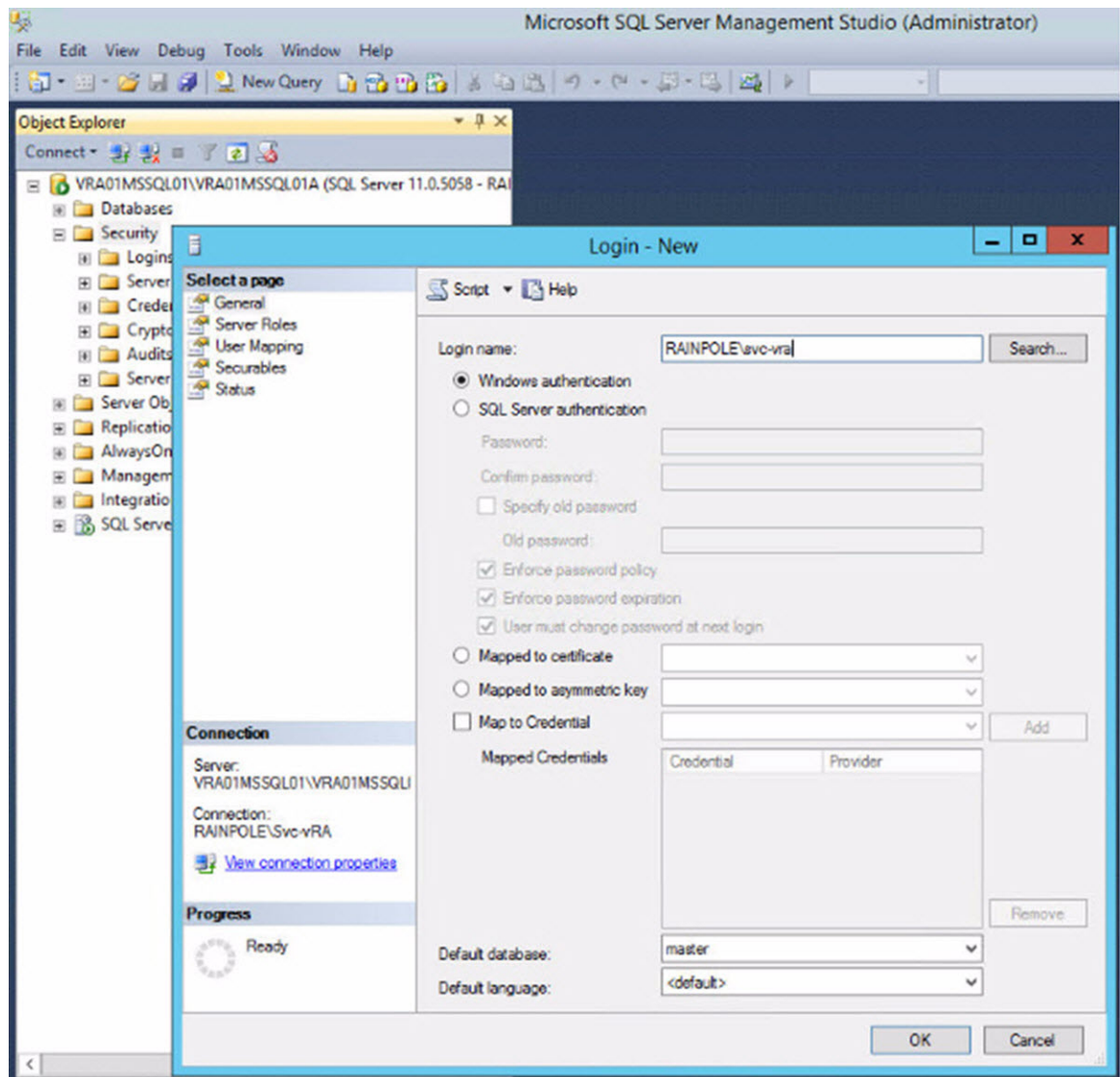
NOTE During the SQL Server installation, the Database Engine configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user was not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name **sa** in the **User name** text box, and the password **sa_password** in the **Password** text box.

- 4 In Object Explorer, expand the server instance **VRA01MSSQL01**.
- 5 Right-click the **Security** folder, click **New**, and click **Login**.

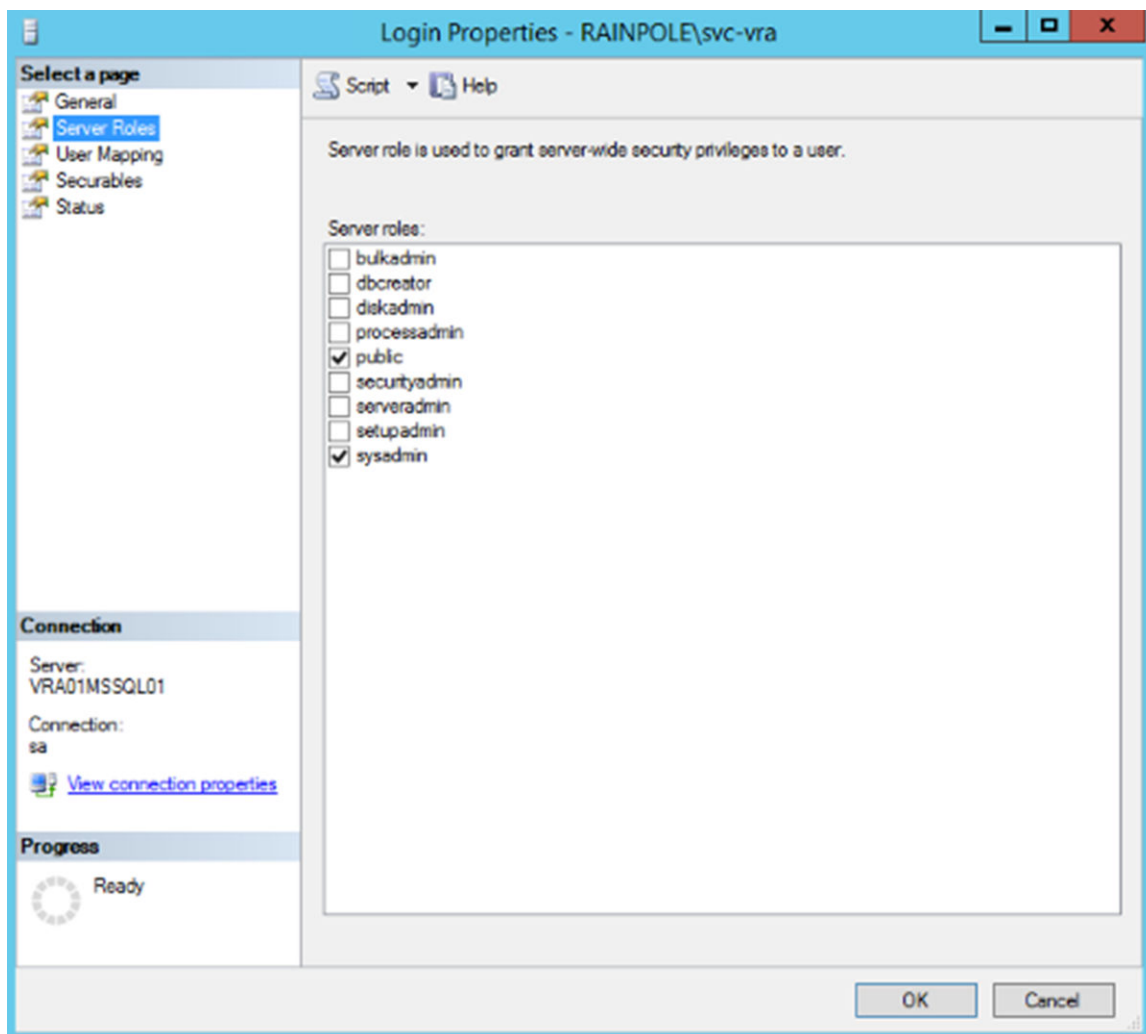


The Login Properties dialog box opens.

- 6 Select the General page of the Login Properties dialog box.
- 7 From the Object Explorer Details pane, select the General page, and enter **Rainpole\Svc-vRA** in the **Login name** text box.



- 8 In the Object Explorer Details pane, select the Server Role page.
- 9 In the Server roles list item field select the **sysadmin** check box, and click **OK**.



Configure Network Access for Distributed Transaction Coordinator for Consolidated SDDC

You configure network access and security between vRealize Automation and your Microsoft SQL Server database using Microsoft Distributed Transaction Coordinator (MSDTC). MSDTC coordinates transactions that update two or more transaction-protected resources, such as databases, message queues, files systems, and so on. These transaction-protected resources may be on a single computer or distributed across many networked computers.

Procedure

- 1 Log in to the VRA01MSSQL01.rainpole.local by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to the virtual machine VRA01MSSQL01.rainpole.local.
 - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

- 2 From the **Start** menu, click **Run**, type **comexp.msc** in the **Open** text box, and click **OK**.

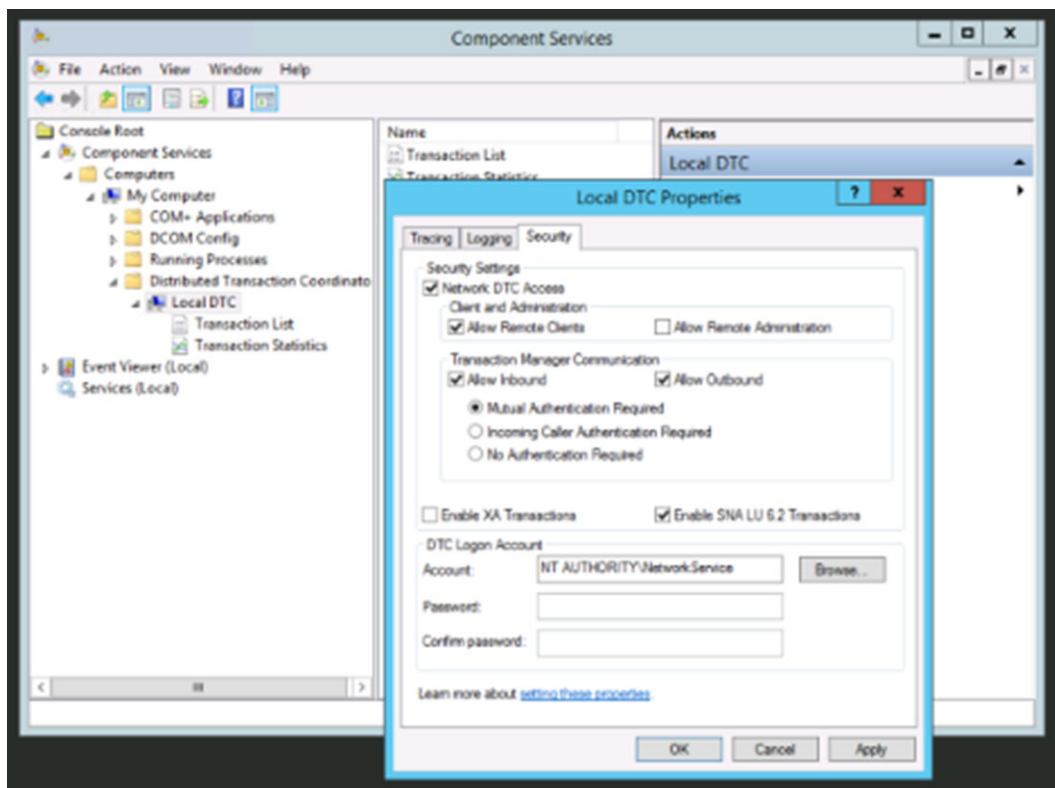
The Component Services manager displays. Component Services lets you manage Component Object Model (COM+) applications.

- 3 Using the navigation tree in the left-side pane, expand **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.
- 4 Right-click **Local DTC** and click **Properties**.

The **Local DTC Properties** dialog box displays.

- 5 Click the **Security** tab in the Local DTC Properties dialog box.
- 6 On the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Remote Administration	Deselected
Allow Inbound	Selected
Allow Outbound	Selected
Mutual Authentication Required	Selected
Enable XA Transactions	Deselected
Enable SNA LU 6.2 Transactions	Selected
Account	Leave the default setting (NT AUTHORITY\NetworkService)
Password	Leave blank



- 7 Click **Yes** to restart the MSDTC Service.
- 8 Click **OK** to confirm that the MSDTC Service has successfully restarted.
- 9 Close the Component Services manager.

Configure SQL Server and MSDTC Access through Windows Firewall for vRealize Automation for Consolidated SDDC

You can configure Windows Firewall to allow or block specific traffic. For vRealize Automation to function correctly, ensure that network access to Microsoft Distributed Transaction Coordinator (MSDTC) and SQL Server is configured to allow access.

Procedure

- 1 Log in to the `VRA01MSSQL01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.
 - a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<code>windows_administrator_password</code>

- 2 From the **Start** menu, click **Run**, type `WF.msc` in the **Open** text box, and click **OK**.
The Windows Firewall with Advanced Security dialog box appears. You use Windows Firewall with Advanced Security to configure firewall properties for each network profile.
- 3 Allow Access for Microsoft SQL Server on TCP Port 1433.
 - a In the navigation pane right-click **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.
The New Inbound Rule Wizard appears.
 - b On the Rule Type page of the New Inbound Rule Wizard, select the **Port** radio button, and click **Next**.
 - c On the Protocol and Ports page, select **TCP**, enter **1433** in the **Specific local ports** text box, and click **Next**.
 - d On the Action page, select **Allow the connection** and click **Next**.
 - e On the Profile page, select the **Domain**, **Private**, and **Public** profiles and click **Next**.
 - f On the Name page, enter a **Name** and **Description** for this rule and click **Finish**.
- 4 Allow access for Microsoft Distributed Transaction Coordinator.
 - a In the navigation pane, right-click **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.
 - b On the Rule Type page, click **Predefined**, click **Distributed Transaction Coordinator**, and click **Next**.
 - c On the Predefined Rules page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.
 - d On the Action page, select **Allow the connection**, and click **Finish**.
- 5 Exit the Windows Firewall with Advanced Security wizard.

Configure Service Account Privileges for Consolidated SDDC

For you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account `svc-vra@rainpole.local` on both the vCenter Server and the NSX instance.

Configure Service Account Privileges on the vCenter Server for Consolidated SDDC

Configure administrator privileges for the `svc-vra` and `svc-vro` users on the vCenter Server for your management and workload consolidation deployment.

If you add more vCenter Server instances in the future, perform this procedure on those instances as well.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 2 In the Navigator pane, select **Global Inventory Lists > vCenter Servers**.
- 3 Right-click the `sfo01w01vc01.sfo01.rainpole.local` instance and select **Add Permission**.
- 4 In the Add Permission dialog box, click the **Add** button.
The Select Users/Groups dialog box appears.
- 5 Select **RAINPOLE** from the **Domain** drop-down menu, and in the **Show Users First** text box enter **svc** to filter user and group names.
- 6 Select **svc-vra** and **svc-vro** from the **User/Group** list, click the **Add** button and click **OK**.
- 7 In the Add Permission dialog box, select **Administrator** from the **Assigned Role** drop-down menu and click **OK**.

The `svc-vra` and `svc-vro` users now have **Administrator** privilege on the vCenter Server for Workload and Management Consolidation.

Configure the Service Account Privilege on the NSX Instance for Consolidated SDDC

Configure Enterprise Administrator privileges for the `svc-vra@rainpole.local` service account.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 2 In the Navigator pane, select **Networking & Security > NSX Managers**.
- 3 Double-click the NSX Manager **172.16.11.66**.
- 4 Click **Manage**, click **Users**, and click the **Add** icon. The Assign Role wizard appears.
- 5 On the Identify User page, select the **Specify a vCenter User** radio button, enter **svc-vra@rainpole.local** in the **User** text box, and click **Next**.

The screenshot shows the 'Assign Role' wizard window. On the left, a sidebar contains two steps: '1 Identify User' (highlighted in blue) and '2 Select Roles'. The main area is titled 'Identify User' and contains the instruction 'Select a vCenter user or group to assign role.' Below this, there are two radio buttons. The first, 'Specify a vCenter user', is selected. Next to it is a text box containing 'svc-vra@rainpole.local'. Below the text box, a note states: 'User can log on with the credentials maintained at vCenter. (ex: test@vsphere.local or test@domain.com)'. The second radio button, 'Specify a vCenter group', is unselected. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 6 On the Select Roles page, select the **Enterprise Administrator** radio button, and click **Finish**.

The screenshot shows the 'Assign Role' wizard window at the 'Select Roles' step. The sidebar on the left now shows both steps with green checkmarks: '1 Identify User' and '2 Select Roles' (highlighted in blue). The main area is titled 'Select Roles' and contains the instruction 'Select NSX role for user.' Below this, there are four radio buttons. The first three are 'Auditor', 'Security Administrator', and 'NSX Administrator', all of which are unselected. The fourth, 'Enterprise Administrator', is selected. Below the radio buttons, a 'Description:' label is followed by the text: 'Users in this role can perform all tasks related to deployment and configuration of NSX products and administration of this NSX Manager instance.' At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

The **rainpole\svc-vra** user is now configured as an Enterprise Administrator for the NSX instance and appears in the lists of users and roles.

vRealize Automation Installation for Consolidated SDDC

A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

After installation, you can customize the installation environment and configure one or more tenants which sets up access to self-service provisioning and lifecycle management of cloud services. By using the secure portal Web interface, administrators, developers, or business users can request IT services and manage specific cloud and IT resources based on their roles and privileges. Users can request infrastructure, applications, desktops, and IT service through a common service catalog.

Load Balancing the Cloud Management Platform for Consolidated SDDC

You configure load balancing for all services and components related to vRealize Automation and vRealize Orchestrator by using an NSX Edge load balancer.

You must configure the load balancer before you deploy the vRealize Automation appliance. This is because you need the virtual IP (VIP) addresses to deploy the vRealize Automation appliance.

Add Virtual IP Addresses to the NSX Load Balancer for Consolidated SDDC

As the first step of configuring load balancing, you add virtual IP Addresses to the edge interfaces.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager and double-click the **sfo01w01lb01** NSX Edge to edit its network settings.
- 5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.
- 6 Select the **OneArmLB** interface and click the **Edit** icon.

- 7 In the Edit NSX Edge Interface dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59

- 8 Click **OK** to save the configuration.

Create Application Profiles for Consolidated SDDC

Create two application profiles to define the behaviors of particular types of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic and makes traffic management tasks easier and more efficient.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager and double-click the **sfo01w01b01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

- 6 Click the **Add** icon and in the New Profile dialog box, enter the following values.

Setting	Value
Name	vRealize-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	None

The screenshot shows the 'New Profile' dialog box with the following configuration:

- Name:** vRealize-https
- Type:** HTTPS
- ☒ **Enable SSL Passthrough**
- HTTP Redirect URL:** (empty)
- Persistence:** None
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- ☐ **Insert X-Forwarded-For HTTP header**
- ☐ **Enable Pool Side SSL**
- Virtual Server Certificate...** (selected tab)
- Service Certificates** (selected sub-tab)
- ☐ **Configure Service Certificate**
- Cipher:** Default
- Client Authentication:** ignore

The certificate list shows the following entries:

Common Name	Issuer	Validity
VSM_SOLUTION_1277i	VSM_SOLUTION_1277i	Mon May 1 2017 - Wed Apr 2 2018
VSM_SOLUTION_695b	VSM_SOLUTION_695b	Mon May 1 2017 - Wed Apr 2 2018
VSM_SOLUTION_1277i	VSM_SOLUTION_1277i	Mon May 1 2017 - Wed Apr 2 2018
VSM_SOLUTION_695b	VSM_SOLUTION_695b	Mon May 1 2017 - Wed Apr 2 2018
sfo01w01psc01.sfo01.n	CA	Fri Apr 28 2017 - Fri Apr 2 2018

- 7 Click **OK** to save the configuration.
- 8 Repeat the same steps to create the following application profile.

Setting	Value
Name	vRealize-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800

Create Service Monitoring for Consolidated SDDC

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager and double-click the **sfo01w01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.
- 6 Click the **Add** icon and in the New Service Monitor dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	vra-svr-443-monitor	vra-iws-443-monitor	vra-ims-443-monitor	vra-vro-8283-monitor
Name	vra-svr-443-monitor	vra-iws-443-monitor	vra-ims-443-monitor	vra-vro-8283-monitor
Interval	3	3	3	3
Timeout	10	10	10	10
Max Retries	3	3	3	3
Type	HTTPS	HTTPS	HTTPS	HTTPS
Expected	204			
Method	GET	GET	GET	GET
URL	/vcac/services/api/health	/wapi/api/status/web	/VMPSProvision	/vco-controlcenter/docs
Receive		REGISTERED	ProvisionService	

New Service Monitor

Name: * vra-svr-443-monitor

Interval: 3 (seconds)

Timeout: 10 (seconds)

Max Retries: 3

Type: HTTPS

Expected: 204

Method: GET

URL: /vcac/services/api/health

Send:

Receive:

Extension:

OK Cancel

- 7 Repeat [Step 6](#) to create a service monitor for each component.

Upon completion, verify that you have successfully entered the monitor names and their respective configuration values.

Create Server Pools for Consolidated SDDC

A server pool consists of back-end server members. After you create a server pool, you associate a service monitor with the pool to manage and share the back-end servers flexibly and efficiently.

The following considerations explain the design of the server pools configuration.

- The configuration uses NONE as health monitor for all server pools. Until vRealize Automation is fully installed and started, the health monitor marks pool members as offline. Health monitors indicate the status of pool members correctly, only after vRealize Automaton is fully installed and initialized.
- Future configurations should disable any added pool member of 3 vRealize Automation VIPs (vra-svr-443, vra-iaas-web-443, vra-iaas-mgr-443). During the installation or power cycle of vRealize Automation, the service inside the second node might not be installed or initialized yet. In this period of time, if the load balancer passes a request to the second node, the request fails. If the second pool member is not disabled, you can experience random failures during vRealize Automation installation, and service initialization or registration failure during a vRealize Automation power cycle.

Perform the procedure multiple times to configure four different server pools.

Table 3-3. Server Pools for the Cloud Management Platform

Pool Name	Monitors	Members				Monitor Port
		Enable Member	Member Name	IP addresses	Port	
vra-svr-443	vra-svr-443-monitor	Yes	vra01svr01a	192.16.8.11.51	443	443
vra-iws-443	vra-iws-443-monitor	Yes	vra01iws01a	192.16.8.11.54	443	443
vra-ims-443	vra-ims-443-monitor	Yes	vra01ims01a	192.16.8.11.57	443	443
vra-svr-8444	vra-svr-443-monitor	Yes	vra01svr01a	192.16.8.11.51	8444	443
vra-vro-8283	vra-vro-8283-monitor	Yes	vra01svr01a	192.16.8.11.51	8283	8283

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

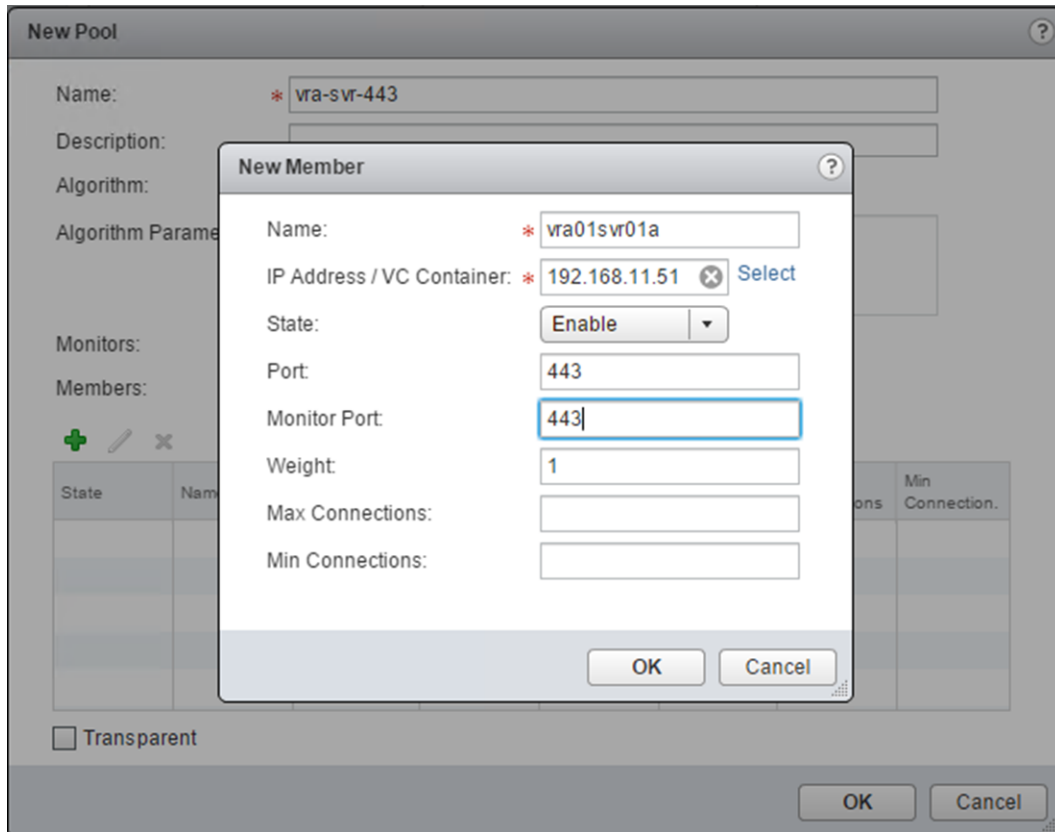
- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager and double-click the **sfo01w01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.
- 6 Click the **Add** icon and in the New Pool dialog box, and enter the following values.

Setting	Value
Name	vra-svr-443
Algorithm	ROUND-ROBIN
Monitors	vra-svr-443-monitor

- 7 Click the **Add** icon to add the first pool member.

- 8 In the **New Member** dialog box, enter the following values and click **OK**.

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51
State	Enable
Port	443
Monitor Port	443
Weight	1



- 9 Repeat the procedure to create the remaining server pools and members.

Create Virtual Servers for Consolidated SDDC

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click **Networking & Security**.
- 3 In the Navigator, click **NSX Edges**.
- 4 From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager and double-click the **sfo01w01lb01** NSX Edge to manage its network settings.
- 5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.
- 6 Click the **Add** icon, and in the New Virtual Server dialog box, configure the values for the virtual server you are adding and click **OK**.

Setting	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Enable Virtual server	Selected	Selected	Selected	Selected	Selected
Application Profile	vRealize-https-persist	vRealize-https-persist	vRealize-https	vRealize-https-persist	vRealize-https-persist
Name	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Description	vRealize Automation Appliance UI	vRealize Automation IaaS Web UI	vRealize Automation IaaS Manager	vRealize Automation Remote Console Proxy	vRealize Orchestrator Control Center
IP Address	192.168.11.53	192.168.11.56	192.168.11.59	192.168.11.53	192.168.11.53
Protocol	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS

Setting	vra-svr-443	vra-iws-443	vra-ims-443	vra-svr-8444	vra-vro-8283
Port	443	443	443	8444	8283
Default Pool	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-svr-8444	vra-vro-8283

New Virtual Server

General | Advanced

☒ Enable Virtual Server

☐ Enable Acceleration

Application Profile: * vRealize-https-persist

Name: * vra-svr-443

Description: vRealize Automation Appliance UI

IP Address: * 192.168.11.53 Select IP Address

Protocol: HTTPS

Port / Port Range: * 443

Default Pool: vra-svr-443

Connection Limit:

Connection Rate Limit: (CPS)

OK Cancel

- Repeat [Step 6](#) to create a virtual server for each component. Upon completion, verify that you have successfully entered the virtual server names and their respective configuration values.

Deploy the vRealize Automation Appliance for Consolidated SDDC

The vRealize Automation appliance is a pre-configured virtual appliance that contains the vRealize Automation server.

The server includes the vRealize Automation appliance product console, which provides a single portal for self-service provisioning and management of cloud services, authoring, administration, and governance.

During deployment of the virtual appliance, a PostgreSQL appliance database is created automatically on the first vRealize Automation appliance. A replica database can be installed on a second vRealize Automation appliance to create a high-availability environment.

Setting	Values for Host A
Name	vra01svr01a.rainpole.local
Select a folder or datacenter	sfo01-w01fd-vra
Network	Mgmt-xRegion01-VXLAN (192.168.11.x)

Setting	Values for Host A
Cluster	sfo01-w01-consolidated01
Virtual Disk Format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	sfo01-w01-vsan01
Enable SSH service in the appliance	Selected
Hostname	vra01svr01a.rainpole.local
Initial Root Password	<i>vra_appA_root_password</i>
Default gateway	192.168.11.1
Domain Name	rainpole.local
Domain Name Servers	172.16.11.4,172.16.11.5
Domain Search Path	rainpole.local,sfo01.rainpole.local
Network 1 IP Address	192.168.11.51
Network 1 Netmask	255.255.255.0

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the Navigator pane, select **Global Inventory Lists > vCenter Servers**.
- 3 Right-click the **sfo01w01vc01.sfo01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, browse to the location of the vRealize Automation Virtual Machine Template file on your file system, and click **Next**.
- 5 On the Select name and folder page, enter the following information, and click **Next**.

Setting	Value
Name	vra01svr01a.rainpole.local
Select a folder or datacenter	sfo01-w01fd-vra

- 6 On the Select a Resource page, select **sfo01-w01-consolidated01 > sfo01-w01rp-sddc-mgmt** and click **Next**.
- 7 On the Review details page, click **Next**.
- 8 On the Accept license agreements page, click **Accept**, and then click **Next**.
- 9 On the Select storage page, select the datastore.
 - a Select **Thin Provision** from the **Select virtual disk format** drop-down menu.
 - b Select **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.
 - c From the datastore table, select the **sfo01-w01-vsan01** vSAN datastore and click **Next**.

- 10 On the Select Networks page, select the distributed port group that ends with `Mgmt-xRegion01-VXLAN` from the **Destination Network** drop-down menu and click **Next**.
- 11 On the Customize template page, configure the following values and click **Next**.

Setting	Value
Enable SSH service in the appliance	Selected
Hostname	<code>vra01svr01a.rainpole.local</code>
Initial Root Password	<code>vra_appA_root_password</code>
Default gateway	<code>192.168.11.1</code>
Domain Name	<code>rainpole.local</code>
Domain Name Servers	<code>172.16.11.4,172.16.11.5</code>
Domain Search Path	<code>rainpole.local,sfo01.rainpole.local</code>
Network 1 IP Address	<code>192.168.11.51</code>
Network 1 Netmask	<code>255.255.255.0</code>

- 12 On the Ready to complete page, review the configuration settings you specified and click **Finish**.
- 13 Click vCenter server `sfo01w01vc01.sfo01.rainpole.local`. Select **VMs** tab. Type `vra01svr01` in the search text box.
- 14 Select virtual machine `vra01svr01a.rainpole.local` and click **Power On** icon.

Wait until the vRealize Automation appliance virtual machine is completely powered on. This may take several minutes.
- 15 From the Virtual Machine Console, verify that `vra01svr01a.rainpole.local` uses the configuration settings you specified.

Deploy Windows Virtual Machines for vRealize Automation for Consolidated SDDC

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration.

Create vSphere Image Customization Specifications for Consolidated SDDC

Create vSphere image customization specifications to use with your vRealize Automation IaaS Server deployments. The customization specification you create customizes the guest operating systems of the virtual machines that host the vRealize Automation IaaS Web Server and IaaS Manager Services.

Customization specifications are XML files that contain guest operating system settings for virtual machines. You create customization specifications with the Guest Customization wizard, and manage specifications using the Customization Specification Manager. vCenter Server saves the customized configuration parameters in the vCenter Server database. 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. When you apply an image customization specification to the guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

Create a Customization Specification File for IaaS Servers for Consolidated SDDC

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Servers deployment.

You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the Guest Customization wizard. The vSphere Image Customization template sysprep answer file stores a number of customization settings such as computer name, licensing information, and workgroup or domain settings.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From Home page, under **Operations and Policies**, click **Customization Specification Manager**.
- 3 Select **sfo01w01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.
- 4 Click the **New** icon.

The Guest Customization wizard opens.

- 5 On the Specify Properties page, configure the following values, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-template

- 6 On the Set Registration Information page, configure the following values, and click **Next**.

Setting	Value
Name	Rainpole
Organization	Rainpole IT

- 7 On the Set Computer Name page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.
- 8 On the Enter Windows License page, configure the following values, and click **Next**.

If you are using Microsoft License Server, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	<i>volume_license_key</i>
Include Server License Information	Selected
Server License Mode	Per seat

- 9 On the Set Administrator Password page, configure the following values, and click **Next**.

Setting	Value
Password	<i>local_administrator_pwd</i>
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

- 10 On the Time Zone page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop-down menu, and click **Next**.
- 11 On the Run Once page, type **net localgroup administrators rainpole\svc-vra /add** in the text box and click **Add**. This command will add service account rainpole\svc-vra into virtual machine's local administrators group. Click **Next**.
- 12 On the Configure Network page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Edit Network** dialog box opens.

- 13 In the Edit Network dialog box, on the IPv4 page, configure the following values and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	192.168.11.1

- 14 On the DNS page, provide DNS servers and search suffixes.

- a Specify the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.16.11.5

- b Enter **rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- c Enter **sfo01.rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- d Click **OK** to save settings and close the Edit Network dialog box, and click **Next**.
- 15 On the Set Workgroup or Domain page, enter credentials that have administrative privileges in the domain, and click **Next**.

Setting	Value
Windows Server Domain	rainpole.local
Username	ad_admin_acct@rainpole.local
Password	<i>ad_admin_password</i>

- 16 On the Set Operating System Options page, select the **Generate New Security ID (SID)** check box, and click **Next**.

- 17 On the Ready to complete page, review the configuration settings that you entered, and click **Finish**.

The customization specification you created is listed in the Customization Specification Manager, and can be used to customize virtual machine guest operating systems.

Create Windows Virtual Machines for vRealize Automation for Consolidated SDDC

An installation of vRealize Automation for the management and workload consolidation deployment requires only two Windows virtual machines to act as IaaS components. Additional virtual machines can be introduced to supplement the installation with high availability or to more evenly distribute IaaS components.

To facilitate cloning, this design uses the vra7-template image customization specification template and the windows-2012r2-64 VM template. Repeat this procedure twice, using the information in the following table.

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
vra01iws01a.rainpole.local	vra01iws01a	sfo01-w01fd-vra	192.168.11.54	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01ims01a.rainpole.local	vra01ims01a	sfo01-w01fd-vra	192.168.11.57	2	8 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN

Prerequisites

- Verify that you have created the Windows 2012 R2 VM template windows2012r2-template.
- SHA512 is disabled in Windows for TLS 1.2 by default. If SHA512 certificates will be used for vRealize Automation, you need to install the windows update in Microsoft KB2973337.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the Navigator pane, select **Global Inventory Lists > vCenter Servers**. Click the **sfo01w01vc01.sfo01.rainpole.local** instance.
- 3 Click **VM Templates in Folders**, and from the VM Templates in Folders pane, right-click the IaaS windows template **windows2012r2-template** and select **New VM from this Template**.

- 4 On the Select a name and folder page, enter the following information and click **Next**. of the Deploy From Template wizard, specify a name and location for the virtual machine.

Setting	Value
Enter a name for the virtual machine	vra01iws01a.rainpole.local
Select a location for the virtual machine	sfo01-w01fd-vra

- 5 On the Select a compute resource page, select **sfo01-w01rp-sddc-mgmt** resource pool and click **Next**.
- 6 On the Select storage page, select the datastore on which to create the virtual machine's disks.
- Select **vSAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.
 - Select the **sfo01-w01-vsan01** vSAN datastore from the datastore table and click **Next**.
- 7 On the Select Clone options page, select the **Customize the operating system** check box, and click **Next**.
- 8 On the Customize guest OS page, select the **vra7-template** from the table, and click **Next**.
- 9 On the User Settings page, enter the following values, and click **Next**.

Setting	Value
NetBIOS name	vra01iws01a
IPv4 address	192.168.11.54
IPv4 subnet mask	255.255.255.0

The screenshot shows the 'win2k12r2_template - Deploy From Template' wizard. The left sidebar indicates the current step is '1f User Settings'. The main area is titled 'User Settings' and contains the following fields:

- Computer Name:** vra01iws01a (with a note: 'The name cannot exceed 63 characters.')
- Network Adapter 1 Settings:**
 - IPv4 address:** 192.168.11.54
 - IPv4 subnet mask:** 255.255.255.0

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 10 On the Ready to Complete page, review your settings and click **Finish**.
- When the deployment of the virtual machine completes, you can customize the virtual machine.
- 11 In the Navigator, select **VMs and Templates**.
- 12 Right-click the **vra01iws01a.rainpole.local** virtual machine and select **Edit Settings**.

- 13 Click **Virtual Hardware** and configure the settings for **CPU**, **Memory**, and the **Network adapter 1**.
 - a Select **2** from the **CPU** drop-down menu.
 - b Set the **Memory** settings to **4096 MB**.
 - c Expand **Network adapter 1** and select **vxxw-dvs-xxxx-Mgmt-xRegion01-VXLAN** from the drop-down menu and click **OK**.

- 14 Right-click the virtual machine **vra01iws01a.rainpole.local**, and select **Power > Power on**.

- 15 From the Virtual Machine Console, verify that vra01iws01a.rainpole.local re-boots, and uses the configuration settings that you specified.

After the Windows customization process completes, a clean desktop appears.

- 16 Log in to the Windows operating system and perform final verification and customization.
 - a Verify that the IP address, computer name, and domain are correct.
 - b Verify that you have added the vRealize Automation service account svc-vra@rainpole.local to the Local Administrators Group.

NOTE You may notice that the virtual machine failed to execute all the steps in the customization specification. When this occurs:

- Delete the virtual machine and its customization specification.
- Retry creating the Windows virtual machines for the IaaS components by creating a new customization specification and provisioning a virtual machine using the newly recreated customization specification.

For information on creating a new customization specification, see [“Create a Customization Specification File for IaaS Servers for Consolidated SDDC,”](#) on page 110. For information on creating Windows virtual machines for the IaaS components, see the current topic, [“Create Windows Virtual Machines for vRealize Automation for Consolidated SDDC,”](#) on page 112.

- 17 Repeat this procedure to deploy and configure the remaining virtual machine.

Install vRealize Automation Management Agent on Windows IaaS VMs for Consolidated SDDC

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

Perform this procedure twice to install the Management Agent on all Windows IaaS virtual machines listed below:

- vra01iws01a.rainpole.local
- vra01ims01a.rainpole.local

Procedure

- 1 Log in to the **vra01iws01.rainpole.local** virtual machine console using the vRealize Automation service account.

Setting	Value
Username	rainpole\svc-vra
Password	svc-vra_password

- 2 Download the vRealize Management Agent.
 - a Open a Web browser and go to **https://vra01svr01a.rainpole.local:5480/installer**.
 - b Download the Management Agent Installer .msi package.
- 3 Install the vRealize Management Agent.
 - a Start the vCAC-IaaSManagementAgent-Setup.msi installer.
 - b On the Welcome page, click **Next** to start the install process.
 - c On the EULA page, select the **I accept the terms of this agreement** check box and click **Next**.
 - d On the Destination Folder page, click **Next** to install in the default path.
 - e On the Management Site Service page, enter the following settings and click **Load**.

Setting	Value
vRA appliance address	https://vra01svr01a.rainpole.local:5480
Root username	root
Password	<i>vra_appA_root_password</i>
 - f Select the **I confirm the fingerprint matches the Management Site Service SSL certificate** check box, and click **Next**.
- 4 On the Management Agent Account Configuration page, enter the following credentials and click **Next**.

Setting	Value
Username	rainpole\svc-vra
Password	<i>svc-vra_password</i>
- 5 On the Ready to Install page, click **Install**.
- 6 Repeat the procedure to install the Management Agent on the remaining Windows IaaS virtual machines.

Install the vRealize Automation Environment for Consolidated SDDC

You use the Installation wizard to deploy a distributed installation with load balancers for high availability and failover.

Once you start the wizard you must complete it. If you cancel the wizard, you must redeploy the appliance to run the wizard again.

Procedure

- 1 Log in to the first vRealize Automation appliance.
 - a Open a Web browser and go to **https://vra01svr01a.rainpole.local:5480/**.
 - b Log in using the following credentials.

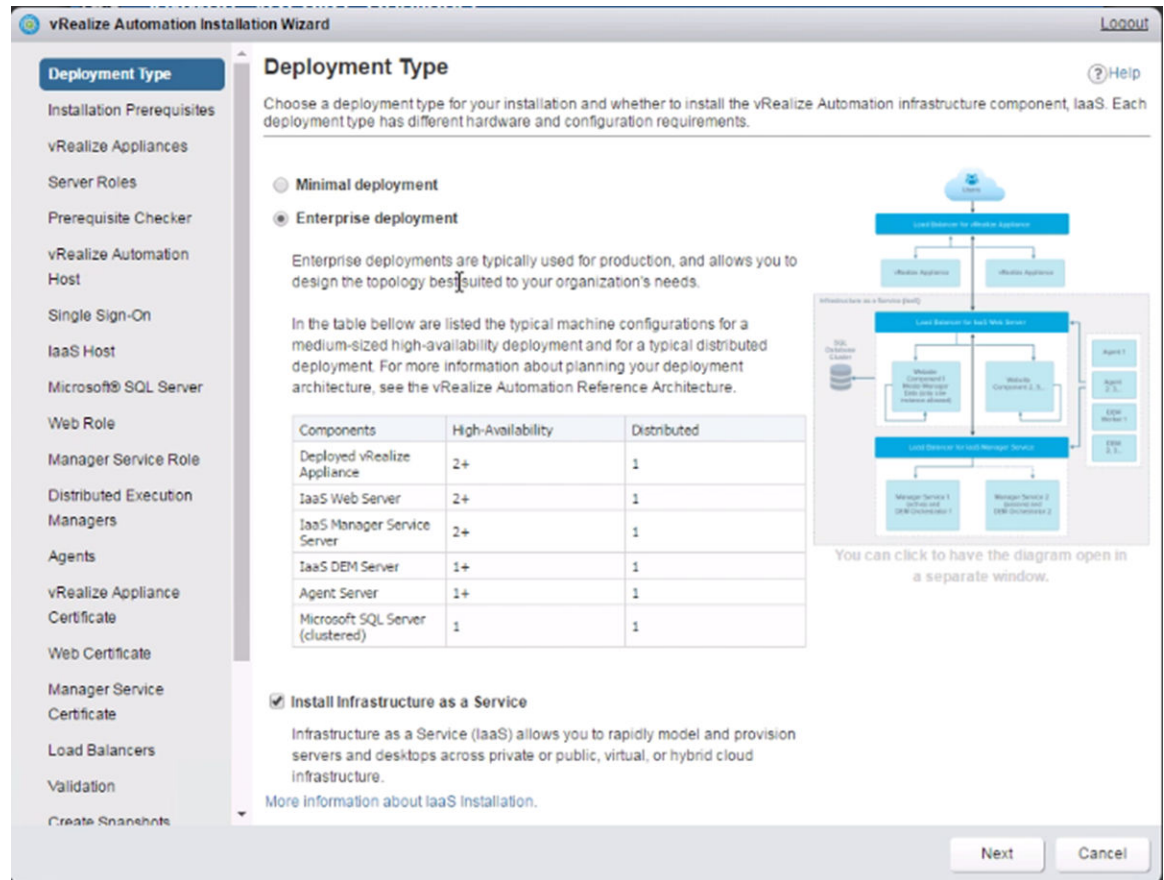
Setting	Value
User name	root
Password	<i>vra_appA_root_password</i>

The vRealize Automation Installation wizard appears.

- 2 On the Welcome to the vRealize Automation Installation Wizard page, click **Next**.
- 3 On the End User License Agreement page, accept the terms of the agreement and click **Next**.

- 4 On the Deployment Type page, specify the following settings and click **Next**.

Setting	Value
Enterprise deployment	Selected
Install Infrastructure as a Service	Selected



- 5 On the Installation Prerequisites page, specify the following time server settings. Click **Change Time Settings**, and click **Next**.

Setting	Value
Virtual Appliance Time Sync. Mode	Use Time Server
Time Server	ntp.sfo01.rainpole.local

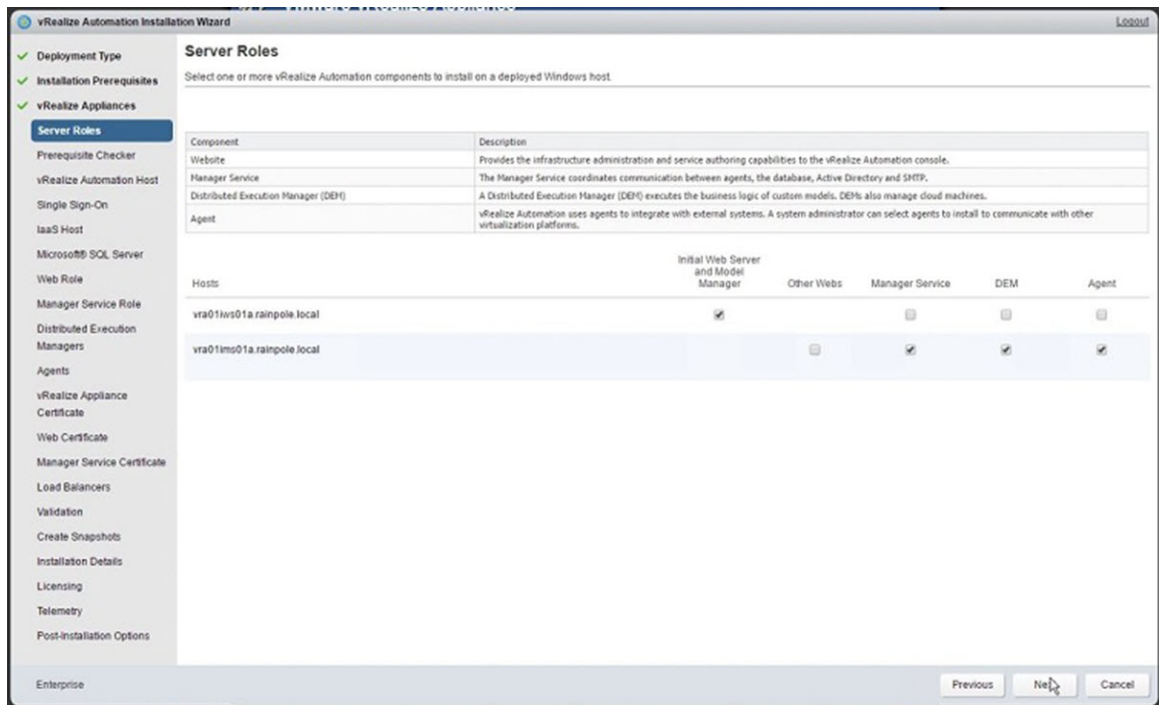
- 6 On the Discovered Hosts page, verify that all Windows IaaS virtual machines are listed and that the time offset is within the -1 / 0 / 1 values and click **Next**.

NOTE The Time Offset column shows the time delta between the vRealize Automation appliance and the Windows IaaS VMs. Time synchronization is critical. If there are values outside of the acceptable values, remediate those before you proceed.

- 7 On the vRealize Appliances page, click **Next**.

- 8 On the Server Roles page, select the respective check boxes for each server based on their role and click **Next**.

Hosts	Role
vra01iws01a.rainpole.local	Initial Web Server and Model Manager
vra01ims01a.rainpole.local	Manager Service, DEM, Agent

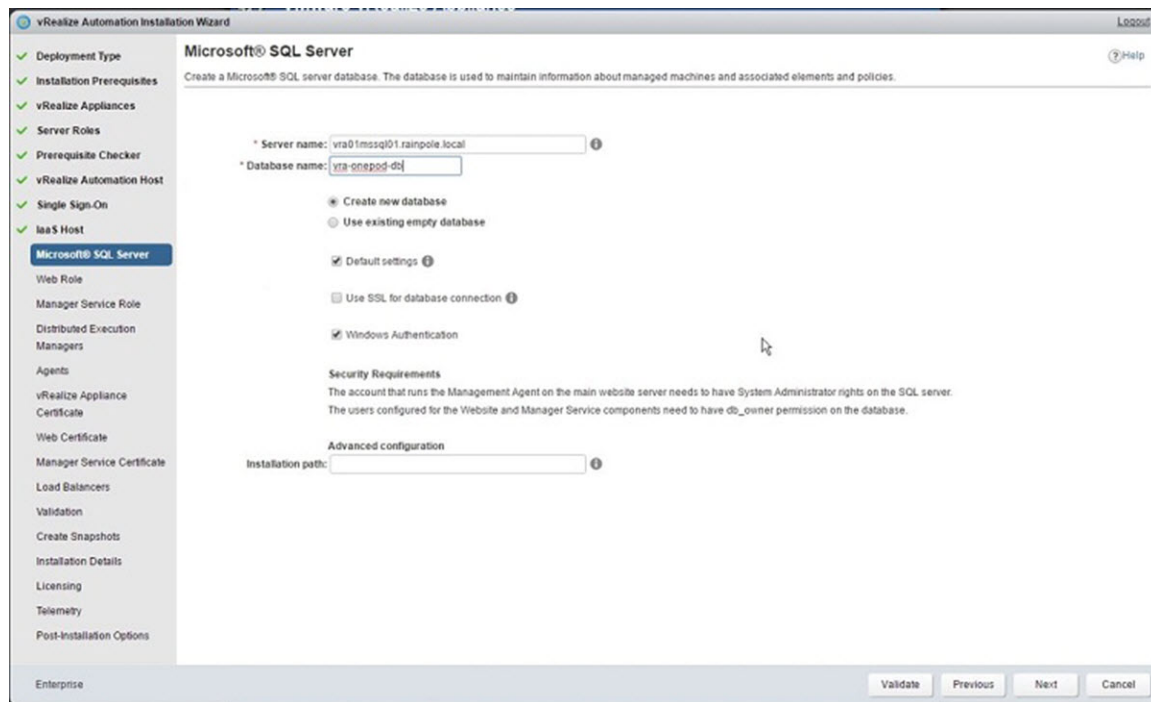


- 9 On the Prerequisite Checker page, verify that the Windows servers for IaaS components are correctly configured.
- Click **Run** and wait for the prerequisite checker to complete.
 - If warnings appear, click **Fix**.
 - Verify that the status of all IaaS components changes to **OK** and click **Next**.
- 10 On the vRealize Automation Host page, enter **vra01svr01.rainpole.local** in the **vRealize Address** text box and click **Next**.
- 11 On the Single Sign-On page, enter and confirm *vra_administrator_password* for the default tenant account administrator@vsphere.local, and click **Next**.
- 12 On the IaaS Host page, configure the following values and click **Next**.

Setting	Value
IaaS Web Address	vra01iws01.rainpole.local
Manager Service Address	vra01ims01.rainpole.local
Security Passphrase	sql_db_pass
Confirm Passphrase	sql_db_pass

- 13 On the Microsoft SQL Server page, configure the following values, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
Server Name	vra01mssql01.rainpole.local
Database Name	vra-onepod-db
Create new database	Selected
Default Settings	Selected
Use SSL for database connection	Deselected
Windows Authentication	Selected



- 14 On the Web Role page, configure the following values for the IaaS servers, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
Website Name	Default Web Site
Port	443
vra01iws01a.rainpole.local Username	rainpole.local\svc-vra
vra01iws01a.rainpole.local Password	svc-vra_password

- 15 On the Manager Service Role page, configure the following values for the IaaS Web servers, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
Active	Selected
IaaS Host Name	vra01ims01a.rainpole.local

Setting	Value
Username	rainpole.local\svc-vra
Password	<i>svc-vra_password</i>

- 16 On the Distributed Execution Managers page, click the **Add** icon as needed, specify the following settings, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
IaaS Host Name	vra01ims01a.rainpole.local
Instance Name	DEM1
Username	rainpole.local\svc-vra
Password	<i>svc-vra_password</i>

- 17 On the Agents page, configure the following values, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
IaaS Host Name	vra01ims01a.sfo01.rainpole.local
Agent Name	VSPHERE
Endpoint	VSPHERE-SFO
Agent Type	vSphere
Username	rainpole.local\svc-vra
Password	<i>svc-vra_password</i>

vRealize Automation Installation Wizard Logout

Agents Help

You can optionally install agents for your deployment. Select a machine to host the agent and the agent type from the drop-down menus and complete the configuration values.

For high-availability mode, you must install two or more instances of the same agent on different servers. Give each instance of the agent the same agent name and the same endpoint name.

IaaS Host Name: vra01ims01a.rainpole.local

Agent Name: VSPHERE

Endpoint: VSPHERE-SFO

Installation Path (Optional): (Optional)

Agent Type: vSphere

Username: rainpole\svc-vra

Password: [masked]

Enterprise Validate Previous **Next** Cancel

- 18 On the next three certificates configuration pages, configure the certificates for all vRealize Automation.

You complete three different certificate configuration pages for the different nodes using the same process and values from the **vra-for-1-pod.key** file for the Private Key and the **vra-for-1-pod.3.pem** file for all certificates stored in the vra folder. For more information on certificate configuration, see "Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components" in the *VMware Validated Design Planning and Preparation (1-Pod)* document.

- a On the vRealize Appliance Certificate page, specify the following settings, click **Save Imported Certificate**, and click **Next**.

Setting	Value
Certificate Action	Import
RSA Private Key	-----BEGIN RSA PRIVATE KEY----- <i>private_key_value</i> -----END RSA PRIVATE KEY-----
Certificate Chain	-----BEGIN CERTIFICATE----- <i>Server_certificate_value</i> -----END CERTIFICATE-----BEGIN CERTIFICATE----- <i>Intermediate_CA_certificate_value</i> -----END CERTIFICATE-----BEGIN CERTIFICATE----- <i>Root_CA_certificate_value</i> -----END CERTIFICATE-----
Passphrase	<i>vra_cert_passphrase</i>

- b Repeat this step on the Web Certificate and the Manager Service Certificate pages of the vRealize Automation Installation Wizard.

vRealize Automation Installation Wizard

Manager Service Certificate

Select a certificate type from the Certificate Action menu.

If you are using a PEM-encoded certificate, select Import Certificate. Select Generate Certificate to create a self-signed certificate; Select Generate already deployed in the certificate store on the IaaS servers.

* Certificate Action

- ☐ Keep Existing
- ☐ Generate Certificate
- ☐ Generate Signing Request
- ☒ Import Certificate
- ☐ Provide Certificate Thumbprint

RSA Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MnXhoannDZ+JFbUhs8Jq/qM59yqJQwVLEPDRNK
a73NajXIEUPpYQ==
-----END RSA PRIVATE KEY-----
```

* Certificate Chain

```
-----BEGIN CERTIFICATE-----
MnXhoannDZ+JFbUhs8Jq/qM59yqJQwVLEPDRNK
a73NajXIEUPpYQ==
-----END RSA PRIVATE KEY-----
```

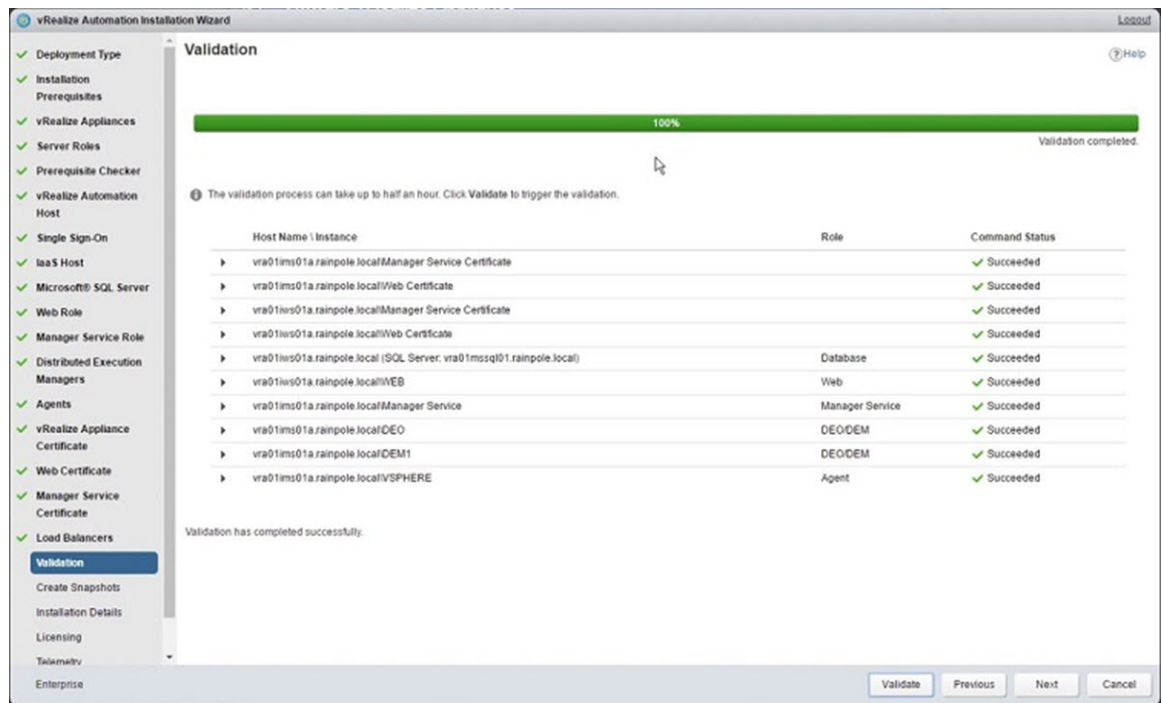
Passphrase

Save Imported Certificate

- 19 On the Load Balancers page, click **Next**.

NOTE You configured load balancing in [“Load Balancing the Cloud Management Platform for Consolidated SDDC,”](#) on page 99.

- 20 On the Validation page, click **Validate**, wait for successful validation, and click **Next**.



- 21 On the Create Snapshots page, do not close the wizard. Navigate to the vSphere Web Client, and create snapshots of all vRealize Automation virtual machines.
 - a In a browser, go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`** to log in to the vSphere Web Client.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password
 - c From the Home page, click **VMs and Templates**.
 - d In the Navigator, expand the **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc01 > sfo01-w01fd-vra** folder.
 - e Right-click the **vra01ms01a.rainpole.local** VM and select **Snapshots > Take Snapshot**.

- f In the Take VM Snapshot dialog box, specify the following settings and click **OK**.

Setting	Value
Name	Prior to vRA IaaS component installation
Snapshot the virtual machine's memory	Deselected

- g Repeat the step to create snapshots of the remaining vRealize Automation VMs.

Virtual Machine	vCenter Folder
vra01svr01a.rainpole.local	sfo01-w01fd-vra
vra01mssql01.rainpole.local	sfo01-w01fd-vra
vra01iws01a.rainpole.local	sfo01-w01fd-vra

After you create snapshots of all virtual machines, return to the vRealize Automation Installation wizard.

- 22 On the Create Snapshots page, click **Next**.
- 23 On the Installation Details page, click **Install**.
- 24 On the Installation Details page, verify that all items complete successfully and click **Next**.
- 25 On the Licensing page, enter your *vRealize_Automation_License_Key*, click **Submit Key**, and click **Next**.
- 26 On the Telemetry page, select **Join the VMware Customer Experience Improvement Program** and click **Next**.
- 27 On the Post-Installation Options page, select **Continue** to proceed without creating initial content and click **Next**.
- 28 Click **Finish** to exit the wizard.

vRealize Automation Default Tenant Configuration for Consolidated SDDC

In shared cloud environments, where multiple companies, divisions or independent groups are using a common infrastructure fabric, it is necessary to set up virtual private clouds where authentication, resources, policy are customized to the needs of each group. Tenants are useful for isolating the users, resources and services of one tenant from those of other tenants.

Create a Local Tenant Administrator for Consolidated SDDC

Join the VMware Identity Manager connectors to the Active Directory domain to support Integrated Windows Authentication. Perform this operation in the default tenant **vsphere.local**.

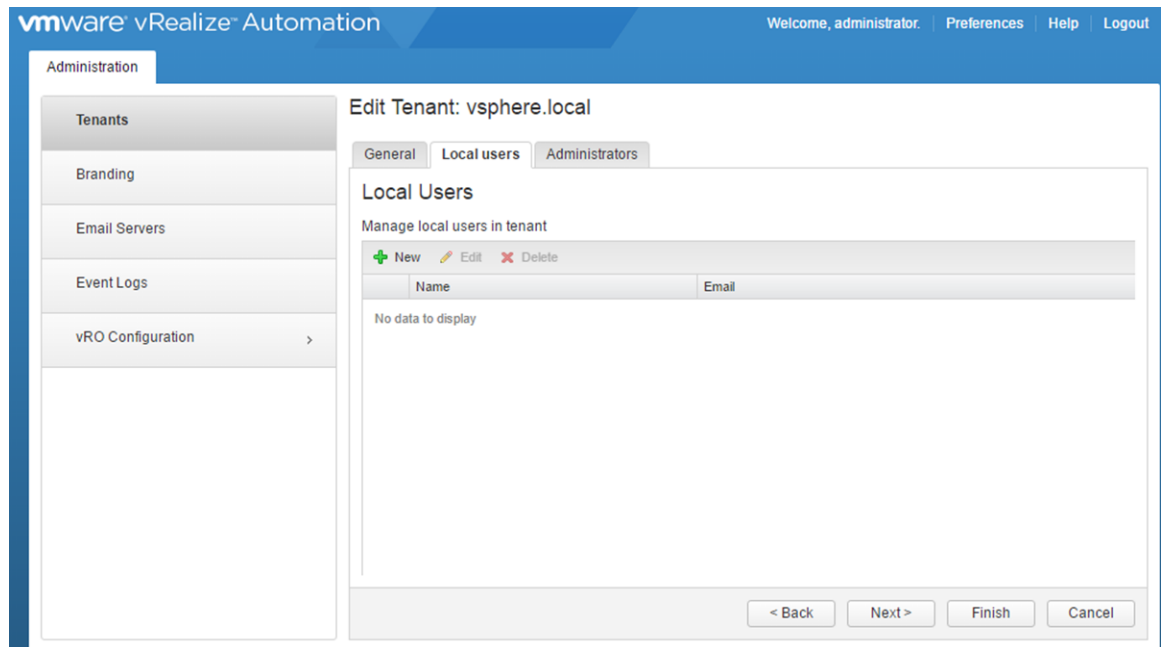
Create a local user for the default tenant in vRealize Automation and assign the Tenant Administrator role to the default tenant.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>

- 2 On the Tenants page, click the default tenant **vsphere.local** to edit its settings.
- 3 Click the **Local users** tab and click **New** to add a local user to the default tenant.



- 4 In the User Details dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalDefaultAdmin
Email	ITAC-LocalDefaultAdmin@vsphere.local
User name	ITAC-LocalDefaultAdmin
Password	<i>itac-localdefaultadmin_password</i>
Confirm password	<i>itac-localdefaultadmin_password</i>

User Details:

* First name:

* Last name:

* Email:

* User name:

* Password:

* Confirm password:

OK Cancel

- 5 On the **Administrators** tab, specify tenant and infrastructure administrators.
 - a In the **Tenant administrators** search text box, enter **ITAC-LocalDefaultAdmin** and press Enter.
 - b In the **IaaS administrators** search text box, enter **ITAC-LocalDefaultAdmin** and press Enter.
 - c Click **Finish**.

vmware vRealize Automation Welcome, administrator. Preferences Help Logout

Administration

Tenants
Branding
Email Servers
Event Logs
vRO Configuration >

Edit Tenant: vsphere.local

General Local users **Administrators**

Tenant administrators
Select users or groups to grant the Tenant administrator role.

Search

Name (1)
ITAC LocalDefaultAdmin (ITAC-LocalID...

IaaS administrators
Select users or groups to grant the IaaS administrator role.

Search

Name (1)
ITAC LocalDefaultAdmin (ITAC-LocalID...

< Back Next > Finish Cancel

- 6 Log out from the vRealize Automation portal.

Join Connectors to an Active Directory Domain for Consolidated SDDC

To use an Active Directory domain for tenant authentication, you must join a VMware Identity Manager connector to vRealize Automation.

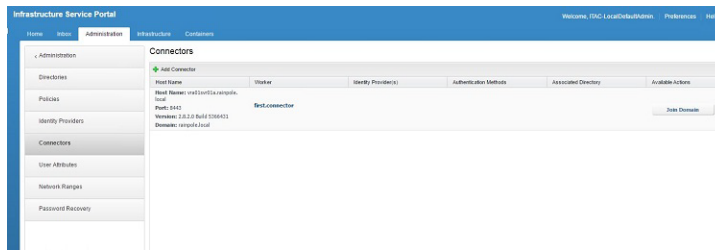
Each vRealize Automation appliance includes a connector that supports user authentication. By default, one connector is typically configured to perform directory synchronization. Perform the procedure by using the ITAC-LocalDefaultAdmin that you configured in the previous procedure.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/vsphere.local**.
 - b Log in using the following credentials.

Setting	Value
User name	ITAC-LocalDefaultAdmin
Password	<i>itac-localdefaultadmin_password</i>

- 2 Navigate to **Administration > Directories Management > Connectors**.
- 3 For the **first.connector**, click **Join Domain**.



- 4 Specify the following settings and click **Join Domain**.

Setting	Value
Domain	<ul style="list-style-type: none"> ■ Select Custom Domain from the drop-down menu. ■ Type rainpole.local in the text field.
Domain User	administrator
Domain Password	<i>domain_admin_password</i>

- 5 Log out from the vRealize Automation portal.

vRealize Automation Tenant Creation for Consolidated SDDC

You create additional vRealize Automation tenants so that users can access the applications and resources that they need to complete their work assignments.

A tenant is a group of users with specific privileges who work within a software instance. Administrators can create additional tenants so that users can log in and complete their work assignments. Administrators can create as many tenants as needed for system operation. Administrators must specify basic configuration such as name, login URL, local users, and administrators. The tenant administrator must also log in and set up an appropriate Active Directory connection and apply custom branding to tenants.

Create the Rainpole Tenant for Consolidated SDDC

The VMware Identity Manager service running in the vRealize Automation appliance provides Single-Sign On (SSO) capability for vRealize Automation users.

VMware Identity Manager is an authentication broker and security token exchange that interacts with the Active Directory to authenticate users. As the system administrator, you configure Identity Manager to provide access to vRealize Automation by the Rainpole tenant. The Rainpole tenant is the tenant through which you manage system-wide configuration, that includes global system defaults for branding, notifications, and monitor system logs.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>

- 2 On the Tenants page, click **New** to configure a new tenant.
- 3 On the **General** tab, enter the following settings for the Rainpole tenant, and click **Submit and Next**.

Setting	Value
Name	Rainpole
URL Name	rainpole
Contact email	administrator@rainpole.local

The screenshot shows the VMware vRealize Automation web interface. The top navigation bar includes 'Administration' and 'New Tenant'. The left sidebar lists various configuration options: Tenants, Branding, Email Servers, Event Logs, and vRO Configuration. The main content area is titled 'New Tenant' and has three tabs: 'General', 'Local users', and 'Administrators'. The 'General' tab is active, displaying the following fields:

- * Name:** Rainpole
- Description:** (empty text area)
- * URL name:** rainpole
- Contact email:** administrator@rainpole.local

At the bottom of the form, there are four buttons: '< Back', 'Submit and Next', 'Finish', and 'Cancel'.

- 4 On the **Local Users** tab, click **New** to add a local user for the tenant.

- 5 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalRainpoleAdmin
Email	ITAC-LocalRainpoleAdmin@rainpole.local
User name	ITAC-LocalRainpoleAdmin
Password	<i>itac-localrainpoleadmin_password</i>
Confirm password	<i>itac-localrainpoleadmin_password</i>

The screenshot shows a dialog box titled "User Details:". Inside the dialog, there are six input fields, each preceded by a red asterisk indicating a required field. The fields are labeled "First name:", "Last name:", "Email:", "User name:", "Password:", and "Confirm password:". The values entered in the first four fields are "ITAC", "LocalRainpoleAdmin", "ITAC-LocalRainpoleAdmin", and "ITAC-LocalRainpoleAdmin" respectively. The "Password:" and "Confirm password:" fields contain seven asterisks. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

- 6 On the **Administrators** tab, specify tenant and infrastructure administrators.
 - a Enter **ITAC-LocalRainpoleAdmin** in the **Tenant administrators** search text box and press **Enter**.
 - b Enter **ITAC-LocalRainpoleAdmin** in the **IaaS administrators** search text box and press **Enter**.
 - c Click **Finish**.

The screenshot shows the 'Edit Tenant: Rainpole' configuration page in the vRealize Automation console. The left sidebar contains navigation links for Administration, Tenants, Branding, Email Servers, Event Logs, and vRO Configuration. The main content area has tabs for General, Local users, and Administrators. Under the Administrators tab, there are two sections: 'Tenant administrators' and 'IaaS administrators'. Each section has a search bar and a table listing selected administrators. In both tables, 'ITAC LocalRainpoleAdmin (ITAC-Local...)' is listed. At the bottom right, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

- 7 Log out of vRealize Automation portal.

Configure Identity Management for the vRealize Automation Tenant for Consolidated SDDC

As part of the tenant creation process, each tenant must be associated with at least one directory service, such as Active Directory. You can add additional directories as needed.

Perform the procedure using the ITAC-LocalRainpoleAdmin user group that you configured earlier in the deployment process.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	ITAC-LocalRainpoleAdmin
Password	<i>itac-localrainpoleadmin_password</i>

- 2 Navigate to **Administration > Directories Management > Directories**.

- 3 Click **Add Directory** and select **Add Active Directory over LDAP/IWA**, specify the following settings and click **Save & Next**.

Setting	Value
Directory Name	rainpole.local
Directory Type	Active Directory (Integrated Windows Authentication)
Sync Connector	vra01svr01a.rainpole.local
Authentication	Yes
Directory Search Attribute	sAMAccountName
Certificates	Deselected
Domain Name	rainpole.local
Domain Admin Username	domain administrator
Domain Admin Password	<i>domain_admin_password</i>
Bind User UPN	svc-vra@rainpole.local
Bind DN Password	<i>svc-vra_password</i>

vmware vRealize Automation Welcome, ITAC-LocalRainpoleAdmin. Preferences Help Logout

Home Inbox **Administration** Infrastructure Containers

< Administration

- Directories**
- Policies
- Identity Providers
- Connectors
- User Attributes
- Network Ranges
- Password Recovery

Add Directory

* Directory Name: rainpole.local

☐ Active Directory over LDAP
☒ Active Directory (Integrated Windows Authentication)

Directory Sync and Authentication

Select the connector that syncs users from Active Directory to the VMware Identity Manager directory.

Sync Connector: vra01svr01a.rainpole.local

Authentication: Do you want this Connector to also perform authentication?
☒ Yes
☐ No

* Directory Search Attribute: sAMAccountName

Enter the account attribute that contains the user name.

Certificates

If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. If there is more than one Root CA certificate, add all the certificates one after another. Make sure each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

☐ This Directory requires all connections to use STARTTLS

Join Domain Details

Enter the name of the Active Directory domain to join and the domain admin user name and password.

* Domain Name: rainpole.local

* Domain Admin Username: administrator

* Domain Admin Password: *****

Bind User Details

Enter the name of the user who can authenticate with the domain. Use the email address format, for example jdoe@mydomain.com.

* Bind User UPN: svc-vra@rainpole.local

* Bind DN Password: *****

Cancel Save & Next

- 4 On the Select the Domains page, select **rainpole.local (RAINPOLE)** and click **Next**.

Select the Domains

If you are adding an Active Directory over LDAP, domains are automatically selected and listed below with a checkmark. If you are adding an Active Directory (Integrated Windows Authentication), select the domains that should be associated with this Active Directory connection.

Domain
<input checked="" type="checkbox"/> rainpole.local (RAINPOLE)
<input type="checkbox"/> lax01.rainpole.local (LAX01)
<input type="checkbox"/> sfo01.rainpole.local (SFO01)

- 5 On the Map User Attributes page, click **Next**.
- 6 On the Select the groups (users) you want to sync page, enter the group DN's to sync.
- Click the **Add** icon to add the distinguished name to the search criteria.
 - In the **Specify the group DN's** text box, enter **dc=rainpole,dc=local** and click **Find Groups**.
 - After the Groups to sync value updates, click **Select**.

Select the groups (users) you want to sync

Enter the Group DN's to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

☒ Sync nested group members

Specify the group DN's	Select All	Groups to sync	
dc=rainpole,dc=local	<input type="checkbox"/>	0 of 62	Select

Group DN	Mapped Groups
----------	---------------

d Select the following groups and click **Save**.

- ug-ITAC-TenantAdmins
- ug-ITAC-TenantArchitects
- ug-SDDC-Admins
- ug-SDDC-Ops
- ug-vROAdmins

<input type="checkbox"/>	Remote Desktop Users	CN=Remote Desktop Users,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	Remote Management Users	CN=Remote Management Users,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	Replicator	CN=Replicator,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	SDDC-Admins	CN=SDDC-Admins,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	SDDC-Ops	CN=SDDC-Ops,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	Schema Admins	CN=Schema Admins,CN=Users,DC=rainpole,DC=local
<input type="checkbox"/>	Server Operators	CN=Server Operators,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	Svc-users	CN=Svc-users,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	TelnetClients	CN=TelnetClients,CN=Users,DC=rainpole,DC=local
<input type="checkbox"/>	Terminal Server License Servers	CN=Terminal Server License Servers,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	Users	CN=Users,CN=Builtin,DC=rainpole,DC=local
<input type="checkbox"/>	WinRMRemoteWMIUsers_	CN=WinRMRemoteWMIUsers_ CN=Users,DC=rainpole,DC=local
<input type="checkbox"/>	Windows Authorization Access Group	CN=Windows Authorization Access Group,CN=Builtin,DC=rainpole,DC=local
<input checked="" type="checkbox"/>	ug-ITAC-TenantAdmins	CN=ug-ITAC-TenantAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input checked="" type="checkbox"/>	ug-ITAC-TenantArchitects	CN=ug-ITAC-TenantArchitects,OU=SDDC-Platform,DC=rainpole,DC=local
<input checked="" type="checkbox"/>	ug-SDDC-Admins	CN=ug-SDDC-Admins,OU=SDDC-Platform,DC=rainpole,DC=local
<input checked="" type="checkbox"/>	ug-SDDC-Ops	CN=ug-SDDC-Ops,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	ug-vCAAdmins	CN=ug-vCAAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	ug-vCenterAdmins	CN=ug-vCenterAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input checked="" type="checkbox"/>	ug-vROAdmins	CN=ug-vROAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	vCAAdmins	CN=vCAAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	vCenterAdmins	CN=vCenterAdmins,OU=SDDC-Platform,DC=rainpole,DC=local
<input type="checkbox"/>	vROAdmins	CN=vROAdmins,OU=SDDC-Platform,DC=rainpole,DC=local

Cancel Save

e Click **Next**.

Select the groups (users) you want to sync

Enter the Group DN's to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

☒ Sync nested group members

Specify the group DN's

dc=rainpole,dc=local

Select All Groups to sync

5 of 62

Select

Group DN

dc=rainpole,dc=local

dc=rainpole,dc=local

dc=rainpole,dc=local

dc=rainpole,dc=local

dc=rainpole,dc=local

dc=rainpole,dc=local

Mapped Groups

CN=ug-ITAC-TenantAdmins,OU=SDDC-Platform,DC=rainpole,DC=local

CN=ug-ITAC-TenantArchitects,OU=SDDC-Platform,DC=rainpole,DC=local

CN=ug-SDDC-Admins,OU=SDDC-Platform,DC=rainpole,DC=local

CN=ug-SDDC-Ops,OU=SDDC-Platform,DC=rainpole,DC=local

CN=ug-vROAdmins,OU=SDDC-Platform,DC=rainpole,DC=local

7 On the Select the Users you would like to sync page, click **Next**.

8 On the Review page, click **Sync Directory**.

Assign Tenant Administrative Roles to Active Directory Users for Consolidated SDDC

After you associate vRealize Automation Directories Management with your Active Directory domain, domain user groups who you assign as tenant and infrastructure administrators can administer the tenant.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>

- 2 On the Tenants page, click the Rainpole tenant to edit its settings.
- 3 Click the **Administrators** tab to assign domain user groups for tenant and infrastructure administrators.
 - a Enter **ug-ITAC-TenantAdmins** in the Tenant administrators search text box and press **Enter**.
 - b Enter **ug-ITAC-TenantAdmins** in the IaaS administrators search text box and press **Enter**.
 - c Click **Finish**.

Edit Tenant: Rainpole

Brand the Tenant Login Pages for Consolidated SDDC

You can apply custom branding on a per-customer basis to the vRealize Automation tenant login pages.

System administrators control the default branding for all tenants. As a tenant administrator, you change the branding of the portal. That includes the logo, the background color, and the information in the header and footer. If the branding for a tenant is changed, a tenant administrator can revert back to the system defaults.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>

- 2 Navigate to **Administration > Branding** and deselect the **Use default** check box.

- 3 On the **Header** tab specify the following settings for the header branding.

Setting	Value
Company Name	Rainpole
Product Name	Infrastructure Service Portal
Background hex color	3989C7
Text hex color	FFFFFF

- 4 Click the **Footer** tab, specify the following settings for the footer branding and click **Finish**.

Setting	Value
Copyright notice	Copyright Rainpole. All Rights Reserved.
Privacy policy link	https://www.rainpole.local
Contact link	https://www.rainpole.local/contact

Branding - System Default

Customize the look and feel of the application including the logo, display color, header, and footer information.

☐ Use default

Header Footer

Copyright notice: Copyright Rainpole. All Rights Reserved.

Privacy policy link: https://www.rainpole.local

Policy link is visible only if you provide the URL.

Contact link: https://www.rainpole.local/contact

Contact link is visible only if you provide the URL.

Copyright Rainpole. All Rights Reserved.

version 7.2.0 (build 4859752) Privacy Policy Contact us

Configure the Default Email Servers for Consolidated SDDC

System administrators configure inbound and outbound email servers to handle email notifications about events involving tenants' machines. System administrators can create only one inbound email server and one outbound email server. These servers are the defaults for all tenants.

If tenant administrators do not override the default email server settings before they enable notifications, vRealize Automation uses the globally configured email server.

Procedure

- 1 Log in to the vRealize Automation portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	vra_administrator_password

- 2 Navigate to **Administration > Email Servers** and click **New**.
- 3 In the **New Email Server** dialog box, select **Email - Inbound** and click **OK**.

- 4 On the **New Inbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Inbound
Security	Deselected
Protocol	IMAP
Server Name	email.rainpole.local
Server Port	143
Folder Name	INBOX
Processed Email	Deselected
User Name	administrator@rainpole.local
Password	<i>vra_administrator_password</i>
Email Address	itac@rainpole.local

New Inbound Email

The screenshot shows the 'New Inbound Email' configuration form. The fields and their values are as follows:

- Name:** Rainpole-Inbound
- Description:** (empty)
- Security:** ☐ Use SSL
- Protocol:** ☒ IMAP ☐ POP3
- Server Name:** email.rainpole.local
- Server Port:** 143
- Folder Name:** INBOX
- User Name:** administrator@rainpole.local
- Password:** (masked with asterisks)
- Email Address:** itac@rainpole.local
- Processed Email:** ☐ Delete From Server
- Accept Self Signed Certificates:** ☐ Yes ☒ No

- 5 On the **Email Servers** page, click **New** to configure the outbound server settings.
- 6 In the **New Email Server** dialog box, select **Email - Outbound** and click **OK**.
- 7 On the **New Outbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Outbound
Server Name	email.rainpole.local
Encryption Method	None
Server Port	25
Authentication	Selected
User Name	administrator@rainpole.local
Password	<i>vra_administrator_password</i>
Sender Address	itac@rainpole.local

New Outbound Email

* Name:	<input type="text" value="Rainpole-Outbound"/>	Description:	<input type="text"/>
* Server Name:	<input type="text" value="email.rainpole.local"/>	Authentication:	<input checked="" type="checkbox"/> Required
* Encryption Method:	<input type="radio"/> Use SSL <input type="radio"/> Use TLS <input checked="" type="radio"/> None	* User Name:	<input type="text" value="administrator@rainpole.local"/>
* Server Port:	<input type="text" value="25"/>	* Password:	<input type="password" value="*****"/>
		* Sender Address:	<input type="text" value="itac@rainpole.local"/>
		Accept Self Signed Certificates:	<input type="radio"/> Yes <input checked="" type="radio"/> No

- 8 Log out of vRealize Automation portal.

Embedded vRealize Orchestrator Configuration for Consolidated SDDC

VMware Embedded vRealize Orchestrator is a platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure as well as other VMware and third-party technologies.

vRealize Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. vRealize Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a REST API.

Configure the Embedded vRealize Orchestrator for Consolidated SDDC

Configure the vRealize Orchestrator services to provide the SDDC foundation orchestration engine.

Configure the Embedded vRealize Orchestrator Virtual Appliance for Consolidated SDDC

You need to configure the vRealize Automation virtual appliance to activate the Embedded vRealize Orchestrator instance.

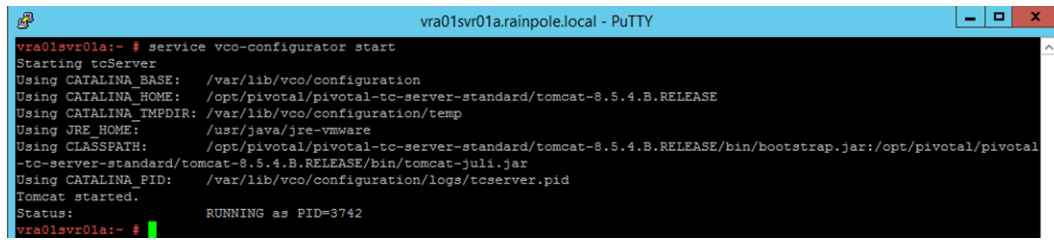
Procedure

- 1 Log in to the vRealize Automation Appliance `vra01svr01a.rainpole.local` to configure the embedded vRealize Orchestrator.
 - a SSH to vRealize Automation Appliance `vra01svr01a.rainpole.local` using the following credentials.

Setting	Value
User name	root
Password	<i>hostA_root_password</i>

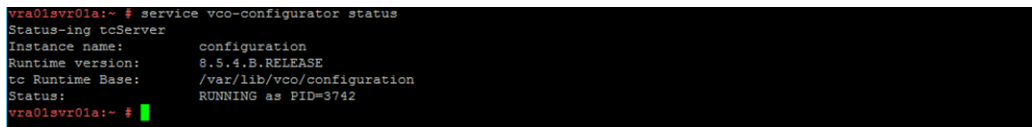
- b Verify the status of `vco-configurator` using the command `service vco-configurator status`.

- 2 Start vco-configurator service using the command **service vco-configurator start**.



```
vra01svr01a:~ # service vco-configurator start
Starting tcServer
Using CATALINA_BASE:   /var/lib/vco/configuration
Using CATALINA_HOME:   /opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE
Using CATALINA_TMPDIR: /var/lib/vco/configuration/temp
Using JRE_HOME:        /usr/java/jre-vmware
Using CLASSPATH:       /opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE/bin/bootstrap.jar:/opt/pivotal/pivotal-tc-server-standard/tomcat-8.5.4.B.RELEASE/bin/tomcat-juli.jar
Using CATALINA_PID:    /var/lib/vco/configuration/logs/tcserver.pid
Tomcat started.
Status:                RUNNING as PID=3742
vra01svr01a:~ #
```

- 3 Verify the status of vco-configurator using the command **service vco-configurator status**.



```
vra01svr01a:~ # service vco-configurator status
Status-ing tcServer
Instance name:      configuration
Runtime version:    8.5.4.B.RELEASE
tc Runtime Base:    /var/lib/vco/configuration
Status:            RUNNING as PID=3742
vra01svr01a:~ #
```

Configure Authentication Provider for vRealize Orchestrator for Consolidated SDDC

Configure the authentication provider for the embedded vRealize Orchestrator.

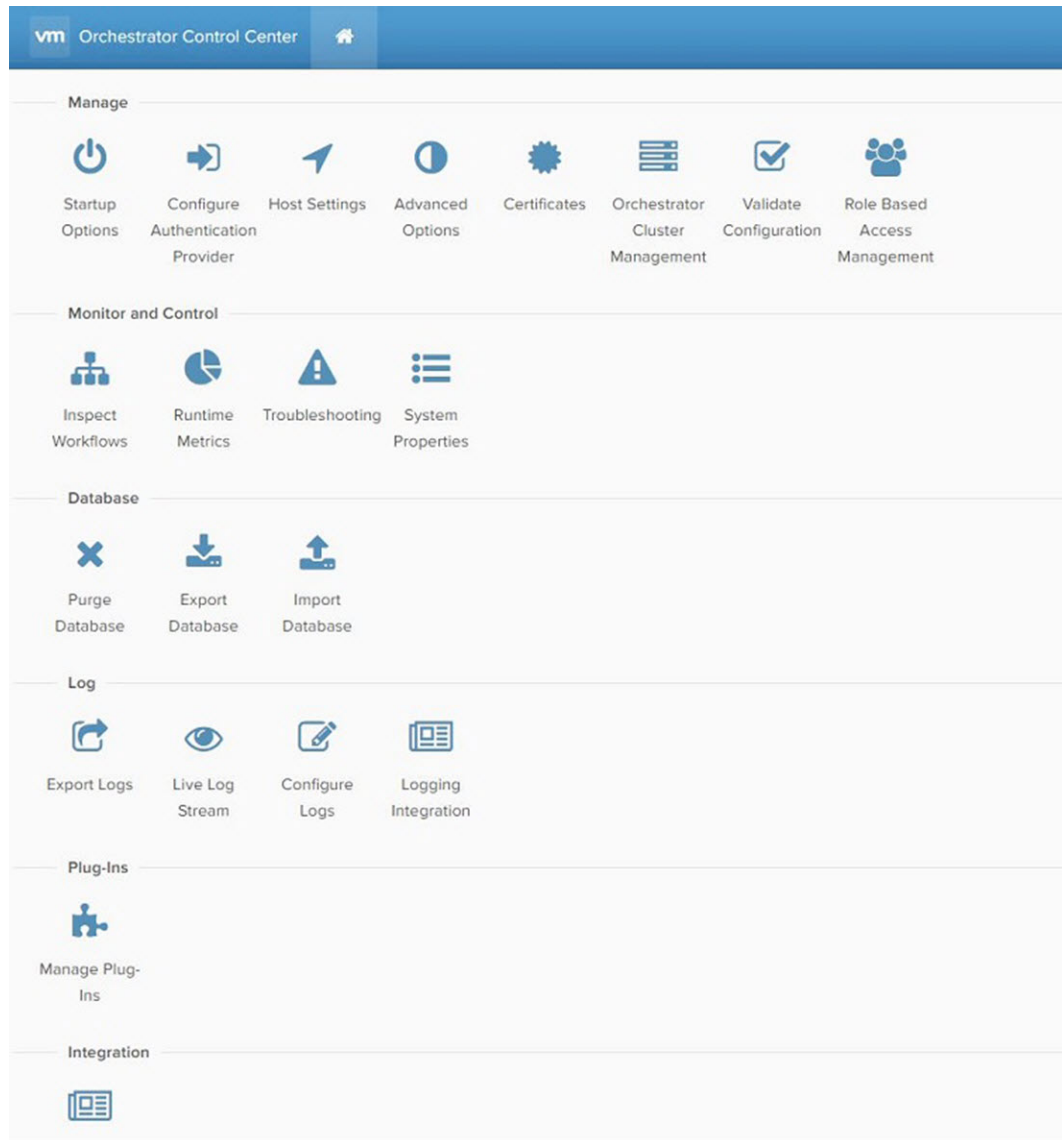
Configure the authentication provider to change the default tenant from vsphere.local to rainpole using the following steps. This enables the usage of Single Sign-On authentication through vRealize Automation.

Procedure

- 1 Log in to the vRealize Orchestrator Control Center.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vsphere_admin_password</i>

- 2 Configure vRealize Automation as a vRealize Orchestrator authentication provider.
 - a On the Home page, under Manage click **Configure Authentication Provider**.



- b In the **Default Tenant** text box, click the **Change** button, enter **rainpole**, and click **Apply**.
 - c In the **Admin group** text box, enter **ug-VR0** and click **Search**.

- d From the drop-down menu, select **rainpole.local\ug-vROAdmins** and click **Save Changes**.

- e At this point, you will be automatically logged out of the control center.
- 3 Verify that you can successfully log in as **svc-vra**.
- a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
- b Log in using the following credentials.

Setting	Value
User name	svc-vra
Password	svc-vra_password

- 4 Log out of control center.
- 5 SSH into the vRealize Automation appliance and run the following commands to restart vRealize Orchestrator services.
- ```
service vco-server restart
service vco-configurator restart
```
- 6 Log back in to control center. as **svc-vra**.
- a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
- b Log in using the following credentials.

| Setting   | Value            |
|-----------|------------------|
| User name | svc-vra          |
| Password  | svc-vra_password |

**NOTE** The log in process may be delayed due to the vRealize Orchestrator services restarting.

## Validate the Configuration for Consolidated SDDC

Verify that vRealize Orchestrator instance embedded in vRealize Automation is configured properly.

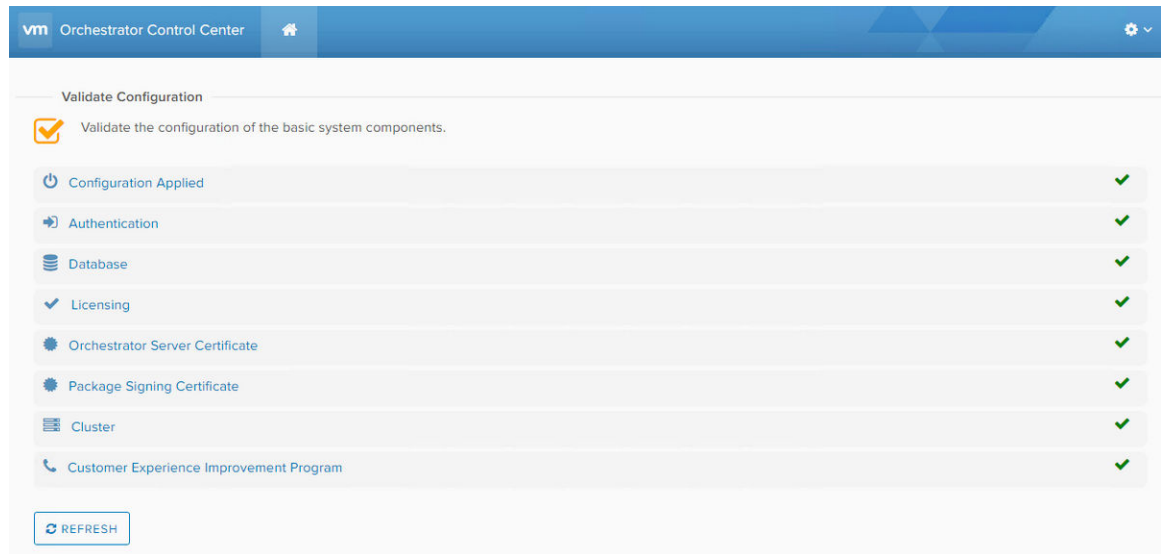
You can verify the configuration of the vRealize Orchestrator instance embedded in vRealize Automation using the Validate Configuration page in the Orchestrator Control Center.

## Procedure

- 1 Log in to the embedded vRealize Orchestrator Control Center.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local:8283/vco-controlcenter**.
  - b Log in using the following credentials.

| Setting   | Value            |
|-----------|------------------|
| User name | svc-vra          |
| Password  | svc-vra_password |

- 2 On the Home page, under Manage, click **Validate Configuration** and verify that all check marks are green.



## Add the vCenter Server Instance to vRealize Orchestrator vRealize for Consolidated SDDC

Add each vCenter Server instance that contributes resources to vRealize Automation and uses the vRealize Orchestrator workflows to allow communication.

## Procedure

- 1 Download and Install the vRealize Orchestrator Client.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local**.
  - b Click **vRealize Orchestrator Client**.
  - c On the VMware vRealize Orchestrator Login page, log in to the Embedded vRealize Orchestrator by using the following hostname and credentials.

| Setting   | Value                         |
|-----------|-------------------------------|
| Host name | vra01svr01.rainpole.local:443 |
| User name | svc-vra                       |
| Password  | svc-vra_password              |

- 2 In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.

- 3 Right-click the **Add a vCenter Server instance** workflow and click **Start Workflow**.
  - a On the Set the vCenter Server Instance page, configure the following settings and click **Next**.

| Setting                                              | Value                             |
|------------------------------------------------------|-----------------------------------|
| IP or hostname of the vCenter Server instance to add | sfo01w01vc01.sfo01.rainpole.local |
| HTTPS port of the vCenter Server instance            | 443                               |
| Location of SDK that you use to connect              | /sdk                              |
| Will you orchestrate this instance                   | Yes                               |
| Do you want to ignore certificate warnings           | Yes                               |

- b On the Set the connection properties page, configure the following settings, and click **Submit**.

| Setting                      | Value                   |
|------------------------------|-------------------------|
| Use a session per user       | No                      |
| vCenter Server user name     | rainpole.local\svc-vro  |
| vCenter Server user password | <i>svc-vro_password</i> |

- 4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vCenter Server** tree control.

The vCenter Server instance you added will be visible in the inventory.

## Integrate vRealize Orchestrator with vRealize Automation for Consolidated SDDC

Configure vRealize Automation to work with vRealize Orchestrator.

### Configure Embedded vRealize Orchestrator Server for Consolidated SDDC

To use vRealize Automation workflows to call vRealize Orchestrator workflows, you must configure vRealize Orchestrator to act as an endpoint.

#### Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

| Setting   | Value                             |
|-----------|-----------------------------------|
| User name | administrator                     |
| Password  | <i>vra_administrator_password</i> |

- 2 Click **Administration > vRO Configuration > Server Configuration**.
- 3 Select the **Use the default Orchestrator server** radio button and click **Test Connection**.
- 4 Once the Successfully connected to the Orchestrator server message appears, click **OK** to complete the configuration.



## Create a vRealize Orchestrator Endpoint for Consolidated SDDC

IaaS administrators are responsible for creating the endpoints that allow vRealize Automation to communicate with your infrastructure. You create a vRealize Orchestrator endpoint for use by Realize Automation to communicate workflows.

### Procedure

- 1 Log in to the Rainpole Infrastructure Service Portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b From the **Select your domain** drop-down menu select **Rainpole.local** and click **Next**
  - c Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Create a new endpoint for vRealize Orchestrator.
  - a Select **Infrastructure > Endpoints > Endpoints**.
  - b Click **New > Orchestration > vRealize Orchestrator**, enter the following values, and click **OK** to complete the process.

| Setting   | Value                                 |
|-----------|---------------------------------------|
| Name      | vra01svr01.rainpole.local             |
| Address   | https://vra01svr01.rainpole.local/vco |
| User name | svc-vra@rainpole.local                |
| Password  | svc-vra_password                      |
| Priority  | 1                                     |

- 3 Start the data collection for the newly created endpoint.
  - a On the Endpoints page, click the newly created vRealize Orchestrator endpoint and click **Actions > Data Collection**.
  - b Click **Start** to begin the vRealize Orchestrator data collection process. Wait several minutes for the data collection process to complete.
  - c Click **Refresh** to verify that the data collection successfully complete.

When a data collection success status message appears, the configuration process is complete.

## Add vRealize Automation Host in vRealize Orchestrator for Consolidated SDDC

To call vRealize Automation Plugin workflows, you configure the vRealize Automation host in vRealize Orchestrator.

### Procedure

- 1 Log in to the vRealize Orchestrator Client.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vco**.
  - b Click **Start Orchestrator Client**.
  - c On the VMware vRealize Orchestrator login page, log in to vRealize Orchestrator using the following hostname and credentials.

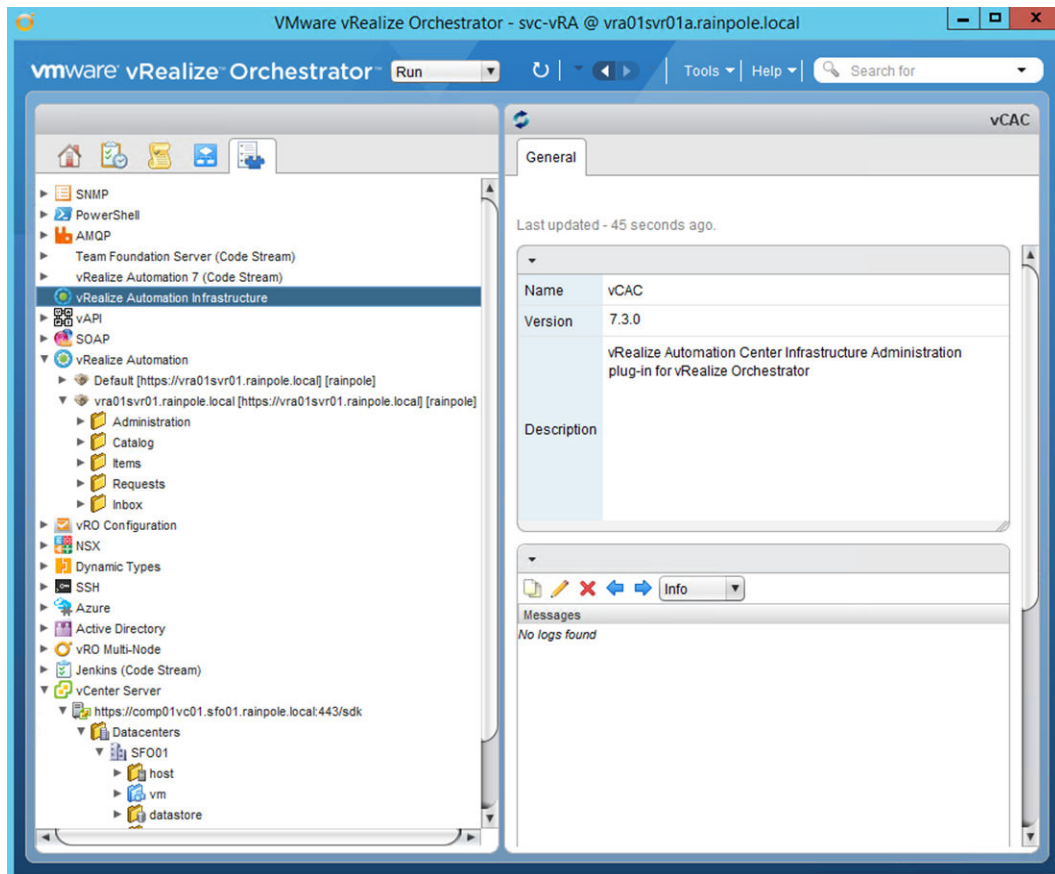
| Setting   | Value                         |
|-----------|-------------------------------|
| Host name | vra01svr01.rainpole.local:443 |
| User name | svc-vra                       |
| Password  | svc-vra_password              |

- 2 In the left pane, click **Workflows**, and navigate to **Library > vRealize Automation > Configuration**.
- 3 Right-click the **Add a vRA host using component registry** workflow and click **Start Workflow**.
  - a On the Common parameters page, configure the following settings, and click **Submit**.

| Setting               | Value                     |
|-----------------------|---------------------------|
| Name of the vCAC host | vra01svr01.rainpole.local |
| Connection timeout    | 30.0                      |
| Operation timeout     | 60.0                      |

- 4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vRealize Automation** tree control.

The vRealize Automation Server instance that you just added is visible in the inventory.



- 5 In the left pane, click **Workflows**, and navigate to **Library > vRealize Automation > Configuration**.

- 6 Right-click the **Add the IaaS host of a vRA host** workflow and click **Start Workflow**.
  - a On the Common parameters page, click the search icon labelled **Not set**. Select **vra01svr01.rainpole.local** [<https://vra01svr01.rainpole.local>] [**rainpole**] for vCAC host and click **Next**.
  - b On the Add an IaaS host page, keep the default settings for Host Properties and click **Next**.

Start Workflow : Add the IaaS host of a vRA host

✓ 1 Common parameters

2 Add an IaaS host

2a Host Properties

2b Proxy settings

3 Host Authentication

3a User Credentials

3b Domain and Workstation

\* Host Name  
IaaS host for vra01svr01.rainpole.local

\* Host URL  
<https://vra01iws01.rainpole.local>

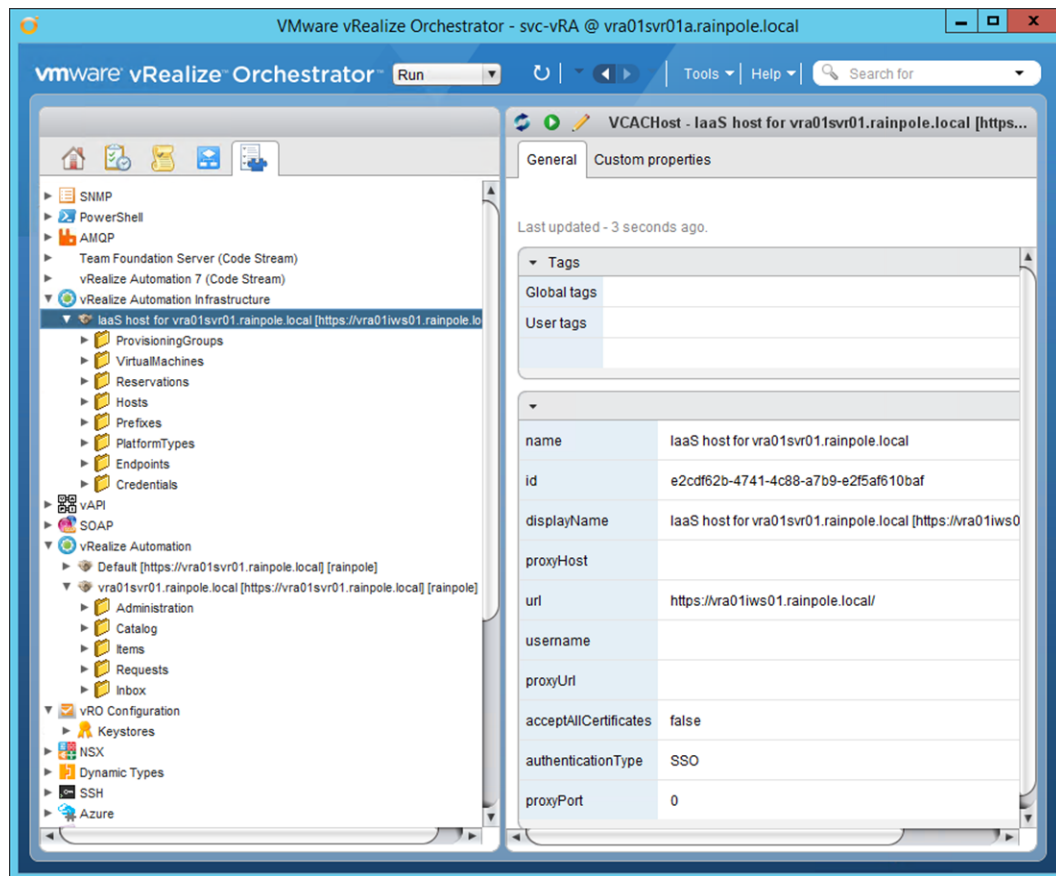
\* Connection timeout  
30

\* Operation timeout  
60

Cancel Back Next Submit

- c On the Add an IaaS host page, keep the default settings for the Proxy Settings and click **Next**.
  - d On the Host Authentication page, select **SSO** for Host's authentication type, and click **Submit**.
- 7 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vRealize Automation Infrastructure** tree control.

The vRealize Automation IaaS Server instance you added is visible in the inventory.



## Install vRealize Business for Consolidated SDDC

vRealize Business is an financial management tool that provides transparency and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

You install vRealize Business, and integrate it with vRealize Automation, to continuously monitor the cost of each individual virtual machine and the costs of their data center.

## Deploy the vRealize Business Virtual Appliances for Consolidated SDDC

VMware vRealize Business allows users to gain greater visibility into the financial aspects of their cloud infrastructure, and lets them optimize and improve these operations.

You deploy two instances of vRealize Business, a server and a data collector. Repeat this procedure twice to deploy the two appliances.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 Click **Hosts and Clusters** and navigate to the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server object.
- 3 Right-click the **sfo01w01vc01.sfo01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, browse to the location of the vRealize Business virtual appliance .ova file on your file system, and click **Next**.
- 5 On the Select name and location page, enter the following information for the respective appliance that you deploy and click **Next**.

| Setting                       | Value for Server            | Value for Data Collector         |
|-------------------------------|-----------------------------|----------------------------------|
| Name                          | vrbc01.sfo01.rainpole.local | sfo01vrbc01.sfo01.rainpole.local |
| Select a datacenter or folder | sfo01-w01fd-vra             | sfo01-w01fd-vraias               |

- 6 On the Select a resource page, select the **sfo01-w01rp-sddc-mgmt** resource pool and click **Next**.
- 7 On the Review details page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the Accept license agreements page, accept the end user license agreements and click **Next**.
- 9 On the Select storage page, select the datastore.
  - a Select **Thin provision** from the **Select virtual disk format** drop-down menu.
  - b Select **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.
  - c From the datastore table, select the **sfo01-w01-vsan01** vSAN datastore and click **Next**.
- 10 On the Select networks page, select the appropriate network from the **Destination** drop-down menu, and click **Next**.

| Setting   | Value for Server               | Value for Data Collector       |
|-----------|--------------------------------|--------------------------------|
| Network 1 | Ends with Mgmt-xRegion01-VXLAN | Ends with Mgmt-RegionA01-VXLAN |

- 11 On the Customize template page, configure the following values and click **Next**.

| Setting                                                 | Values for Server                   | Values for Data Collector           |
|---------------------------------------------------------|-------------------------------------|-------------------------------------|
| Currency                                                | USD                                 | USD                                 |
| Enable SSH service                                      | Selected                            | Selected                            |
| Enable Server                                           | Selected                            | Deselected                          |
| Join the VMware Customer Experience Improvement Program | Selected                            | Selected                            |
| Root user password                                      | <i>vrbc_server_root_password</i>    | <i>vrbc_collector_root_password</i> |
| Default Gateway                                         | 192.168.11.1                        | 192.168.31.1                        |
| Domain Name                                             | vrbc01.sfo01.rainpole.local         | sfo01vrbc01.sfo01.rainpole.local    |
| Domain Name Servers                                     | 172.16.11.4,172.16.11.5             | 172.16.11.5,172.16.11.4             |
| Domain Search Path                                      | rainpole.local,sfo01.rainpole.local | sfo01.rainpole.local                |
| Network 1 IP Address                                    | 192.168.11.66                       | 192.168.31.54                       |
| Network 1 Netmask                                       | 255.255.255.0                       | 255.255.255.0                       |

- 12 On the Ready to complete page, review the configuration settings you specified and

**Deploy OVF Template**

1 Select template  
2 Select name and location  
3 Select a resource  
4 Review details  
5 Accept license agreements  
6 Select storage  
7 Select networks  
**8 Customize template**  
9 Ready to complete

**Customize template**  
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all](#)

**Application** 5 settings

Currency Please select currency.  
USD - US D...

Enable SSH service This will be used as an initial status of the SSH service in the appliance. You can change it later.  
☒

Enable Server This will enable the server components of vRealize Business for Cloud.  
☒

Join the VMware Customer Experience Improvement Program VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information about your organization's use of VMware products and services to help us improve our products and services, to fix problems, and to advise you on how best to deploy and use our products and services. This information does not personally identify any individual. Additional information regarding the data collected through CEIP and how it is used is set forth in the Trust and Assurance Center at <http://www.vmware.com/trust/vmware/>. In VMware's CEIP for this product, you should uncheck the box below. You may join or leave the program at any time.  
☒

Root user password Please enter the password for root user of the virtual appliance.  
Enter password \*\*\*\*\*  
Confirm password \*\*\*\*\*

**Networking Properties** 6 settings

Default Gateway The default gateway address for this VM. Leave blank if DHCP is desired.  
192.168.11.1

Domain Name The domain name of this VM. Leave blank if DHCP is desired.  
vrb01svr01.rainpole.local

Domain Name Servers The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired.  
172.16.11.4, 172.16.11.5

Domain Search Path The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired.  
rainpole.local, sfo01.rainpole.local

Network 1 IP Address The IP address for this interface. Leave blank if DHCP is desired.  
192.168.11.66

Network 1 Netmask The netmask or prefix for this interface. Leave blank if DHCP is desired.  
255.255.255.0

[Back](#) [Next](#) [Finish](#) [Cancel](#)

click **Finish**.

- 13 Change the vRealize Business virtual appliance memory size.
  - a Right-click the virtual machine and select **Edit Settings**. Click **Virtual Hardware**, enter the following value for **Memory**, and click **OK**.

| Setting                             | Value for Server          | Value for Data Collector         |
|-------------------------------------|---------------------------|----------------------------------|
| vRealize Business virtual appliance | vrb01svr01.rainpole.local | sfo01vrbc01.sfo01.rainpole.local |
| Memory                              | 8 GB                      | 2 GB                             |

- 14 Navigate to the new appliance and power on the VM.
- 15 Repeat this procedure to deploy the vRealize Business data collector sfo01vrbc01.sfo01.rainpole.local.

## Configure SSL Certificate for vRealize Business Server for Consolidated SDDC

Import the previously generated certificates for vRealize Business from the vRealize Business appliance management console.

### Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (CertGenVVD). See the *VMware Validated Design Planning and Preparation* documentation.

### Procedure

- 1 Log in to the vRealize Business Server appliance management console.
  - a Open a Web browser and go to **https://vrb01svr01.rainpole.local:5480**.
  - b Log in using the following credentials.

| Setting   | Value                           |
|-----------|---------------------------------|
| User name | root                            |
| Password  | <i>vrb_server_root_password</i> |

- 2 Click the **Administration** tab and click **SSL**.
- 3 On the Replace SSL Certificate page, upload the certificate files that you previously generated for vRealize Business and click **Replace Certificate**.

Use the *vrb.key* file as the **RSA Private Key (.key)** and the *vrb.3.pem* file for the **Certificate(s) (.pem)** entry. These files are in the *vrb* folder that you created during certificate generation.

| Setting                | Value                                                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Choose mode            | Import PEM encoded Certificate                                                                                                                                                                                                                                                    |
| RSA Private Key (.key) | -----BEGIN RSA PRIVATE KEY-----<br><i>private_key_value</i><br>-----END RSA PRIVATE KEY-----                                                                                                                                                                                      |
| Certificate(s) (.pem)  | -----BEGIN CERTIFICATE-----<br><i>Server_certificate_value</i><br>-----END CERTIFICATE-----<br>-----BEGIN CERTIFICATE-----<br><i>Intermediate_CA</i><br>-----END CERTIFICATE-----<br>-----BEGIN CERTIFICATE-----<br><i>Root_CA_certificate_value</i><br>-----END CERTIFICATE----- |
| Private Key Passphrase | <i>vrb_cert_passphrase</i>                                                                                                                                                                                                                                                        |

- 4 Verify that the certificate changed successfully.
 

A message appears that informs you that the SSL certificate was successfully imported .
- 5 Click the **System** tab and click **Reboot** for the changes to take effect.

## Configure NTP for vRealize Business for Consolidated SDDC

Configure the network time protocol (NTP) on both vRealize business appliances from the virtual appliance management interface (VAMI).

Perform the procedure on both vRealize Business server and vRealize Business data collector virtual appliances.



| Host           | VAMI URL                                      |
|----------------|-----------------------------------------------|
| Server         | https://vr01svr01.rainpole.local:5480         |
| Data Collector | https://sfo01vrbc01.sfo01.rainpole.local:5480 |

### Procedure

- 1 Log in to the vRealize Business server appliance management console.
  - a Open a Web browser and go to **https://vr01svr01.rainpole.local:5480**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | root                             |
| Password  | <i>vr01_server_root_password</i> |

- 2 Configure the appliance to use a time server.
  - a Click the **Administration** tab and click **Time Settings**.
  - b On the Time Settings page, enter the following settings and click **Save Settings**.

| Setting         | Value                    |
|-----------------|--------------------------|
| Time Sync. Mode | Use Time Server          |
| Time Server #1  | ntp.sfo01.rainpole.local |

- 3 Repeat the procedure on the vRealize Business data collector virtual appliance sfo01vrbc01.sfo01.rainpole.local.

## Integrate vRealize Business with vRealize Automation for Consolidated SDDC

To prepare vRealize Business for use, you must register the vRealize Business server with vRealize Automation by using the management interface.

### Procedure

- 1 Log in to the vRealize Business server appliance management console.
  - a Open a Web browser and go to **https://vr01svr01.rainpole.local:5480**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | root                             |
| Password  | <i>vr01_server_root_password</i> |

- 2 On the **vRA** tab, enter the following credentials to register with the vRealize Automation server.

| Setting                                  | Value                             |
|------------------------------------------|-----------------------------------|
| Hostname                                 | vra01svr01.rainpole.local         |
| SSO Default Tenant                       | vsphere.local                     |
| SSO Admin User                           | administrator                     |
| SSO Admin Password                       | <i>vra_administrator_password</i> |
| Accept "vRealize Automation" certificate | Deselected                        |

- 3 Click **Register** to connect to vRealize Automation and get its certificate.

A failure message may appear at the top of the page. Wait until the SSO Status changes to The certificate of "vRealize Automation" is not trusted. Please view and accept to register.

- 4 Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.
- 5 Select the **Accept "vRealize Automation" certificate** check box and click **Register**.

SSO Status changes to Connected to vRealize Automation.

## Register the vRealize Business Data Collector with the Server for Consolidated SDDC

After you integrate vRealize Business with vRealize Automation, you connect the two vRealize Business appliances.

Because the tenant is configured in vRealize Automation, you register the vRealize Business data collector appliance with the vRealize Business server using the following procedure.

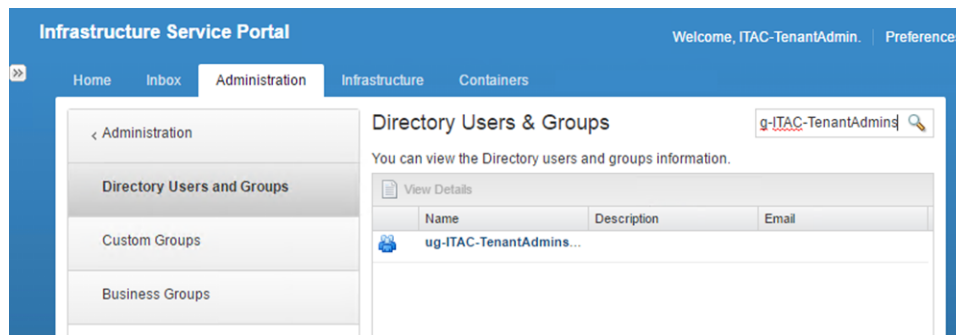
- Grant an additional role to the tenant admin, enter product license key, and generate a one-time key from vRealize Automation.
- Register the data collector with the vRealize Business server.

### Procedure

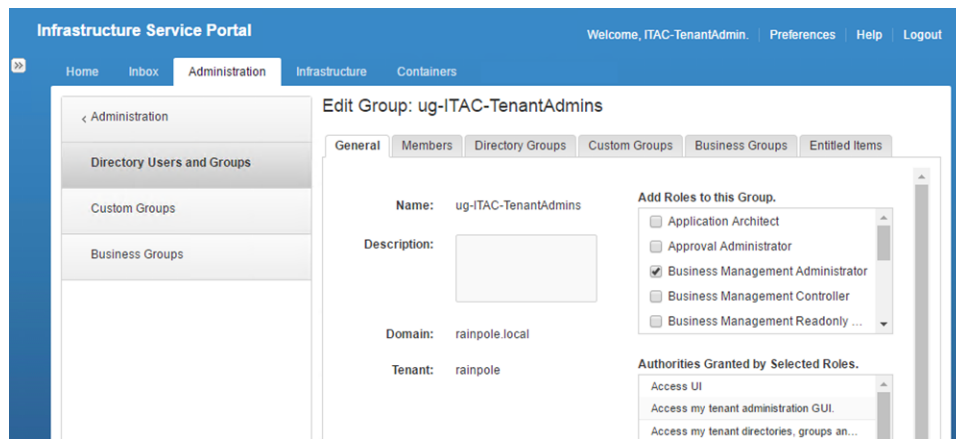
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | Rainpole.local            |

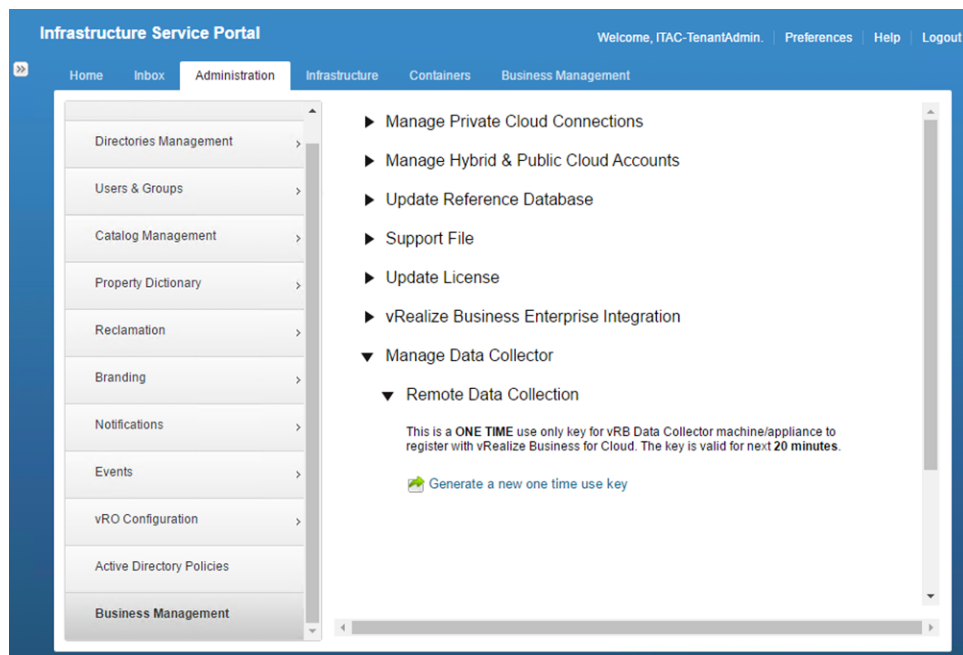
- 2 Navigate to **Administration > Users & Groups > Directory Users & Groups**.
- 3 In the search text box, enter **ug-ITAC-TenantAdmins**.



- 4 Click the **ug-ITAC-TenantAdmins** group to edit its settings.
- 5 On the Edit Group page, in the Add Roles to this Group list, select the **Business Management Administrator** role to add the role and click **Finish**.



- 6 Log out, and log in again by using the same credentials.
- 7 Assign a license to the vRealize Business solution.
  - a Click the **Business Management** tab.
  - b Under License, enter your serial number for vRealize Business and click **Save**.
- 8 Generate a one-time use key for connecting the two vRealize Business appliances.
  - a Navigate to **Administration > Business Management**.
  - b Expand the **Manage Data Collector > Remote Data Collection** section.
  - c Click **Generate a new one time use key**.
  - d Save the one time use key as you need it at a later stage in the implementation sequence.



- 9 Log in to the vRealize Business data collector console.
  - a Open a Web browser and go to **https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

| Setting   | Value                               |
|-----------|-------------------------------------|
| User name | root                                |
| Password  | <i>vrbc_collector_root_password</i> |

- 10 Register the data collector with vRealize Business server.
  - a Expand the **Registration with the vRealize Business Server** section.
  - b Enter the following values and click **Register**.

| Setting                  | Value                              |
|--------------------------|------------------------------------|
| Enter the vRB Server Url | https://vrbc01svr01.rainpole.local |
| Enter the One Time Key   | <i>one_time_use_key</i>            |

After you click **Register**, a warning message informs you that the certificate is not trusted.

### vRealize Business for Cloud Data Collector

---

- ▶ Manage Private Cloud Connections
- ▶ Manage Hybrid & Public Cloud Accounts
- ▼ Registration with vRealize Business Server
 

You can connect your data collector with an existing vRB Server. You can have only one vRB server registered at a time.

Registered vRB URL : vra01bus01.rainpole.local

Register with vRealize Business

---

Enter the vRB Server Url :

The server URL must begin with https://

Enter the One Time Key :

The OTK is found in the One Time Key tab in the vRB Server
- ▶ Support File

- c Click **Install** and click **OK**.

The vRealize Business appliances are now connected.

## Connect vRealize Business with the vCenter Server for Consolidated SDDC

vRealize Business requires communication with the vCenter Server to collect data from the entire cluster. You perform this operation by using the vRealize Business data collector console.

### Procedure

- 1 Log in to the vRealize Business data collector console.
  - a Open a Web browser and go to **https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

| Setting   | Value                               |
|-----------|-------------------------------------|
| User name | root                                |
| Password  | <i>vrbc_collector_root_password</i> |

- 2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click the **Add** icon.
- 3 In the Add vCenter Server Connection dialog box, enter the following settings and click **Save**.

| Setting        | Value                             |
|----------------|-----------------------------------|
| Name           | sfo01w01vc01.sfo01.rainpole.local |
| vCenter Server | sfo01w01vc01.sfo01.rainpole.local |
| Username       | svc-vra@rainpole.local            |
| Password       | <i>svc_vra_password</i>           |

- 4 In the SSL Certificate warning dialog box, click **Install**.
- 5 In the Success dialog box, click **OK**.

## Cloud Management Platform Post-Installation Tasks for Consolidated SDDC

After you deploy vRealize Automation and vRealize Orchestrator, you create anti-affinity rules which enables HA protection for both services, health monitors to check the health status of individual servers, and remove the snapshots created during the vRealize Automation installation.

### Create VM Groups to Define the Startup Order of the Cloud Management Platform for Consolidated SDDC

VM Groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order.

### Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                         |
|-----------|-------------------------------|
| User name | administrator@vsphere.local   |
| Password  | <i>vsphere_admin_password</i> |

- 2 In the Navigator, select **Host and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.
- 3 Create a VM Group for the vRealize Automation IaaS Database.
  - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
  - b On the Configure page, click **VM/Host Groups**.
  - c On the VM/Host Groups page, click the **Add** button.
  - d In the Create VM/Host Group dialog, enter **vRealize Automation IaaS Database** in the **Name** field, select **VM Group** from the **Type** drop down, and click the **Add** button.
  - e In the Add VM/Host Group Member dialog, select **vra01mssql01.rainpole.local** and click **OK**.
  - f Click **OK** to save the VM/Host Group.
- 4 Repeat step 3 to create the following VM/Host Groups.

| VM/Host Group Name                     | VM/Host Group Member             |
|----------------------------------------|----------------------------------|
| vRealize Automation Virtual Appliances | vra01svr01a.rainpole.local       |
| vRealize Automation IaaS Web Servers   | vra01iws01a.rainpole.local       |
| vRealize Automation IaaS Managers      | vra01ims01a.rainpole.local       |
| vRealize Business Servers              | vrb01svr01.rainpole.local        |
| vRealize Business Remote Collectors    | sfo01vrbc01.sfo01.rainpole.local |

- 5 Create a rule to power on the vRealize Automation Database before the vRealize Automation Virtual Appliances.
  - a Select the **sfo01-w01-consolidated01** cluster and click the **Configure** tab.
  - b On the Configure page, click **VM/Host Rules**.
  - c On the VM/Host Rules page, click the **Add** button.
  - d In the Create VM/Host Rule dialog, enter **SDDC Cloud Management Platform 01** in the **Name** field, ensure that the **Enable Rule** check box is selected, select **Virtual Machines to Virtual Machines** from the **Type** drop down.
  - e Select **vRealize Automation IaaS Database** for the **First restart VMs in VM group** drop down list.
  - f Select **vRealize Automation Virtual Appliances** for the **Then restart VMs in VM group** drop down list.
  - g Click **OK** to save the rule.
- 6 Repeat step 5 to create the following VM/Host Rules to ensure the correct restart order for your Cloud Management Platform.

| VM/Host Rule Name                 | First restart VMs in VM group          | Then restart VMs in VM group         |
|-----------------------------------|----------------------------------------|--------------------------------------|
| SDDC Cloud Management Platform 02 | vRealize Automation Virtual Appliances | vRealize Automation IaaS Web Servers |
| SDDC Cloud Management Platform 03 | vRealize Automation IaaS Web Servers   | vRealize Automation IaaS Managers    |
| SDDC Cloud Management Platform 04 | vRealize Automation IaaS Managers      | vRealize Business Servers            |
| SDDC Cloud Management Platform 05 | vRealize Business Servers              | vRealize Business Remote Collectors  |

## Clean Up the vRealize Automation VM Snapshots for Consolidated SDDC

You made snapshots of each vRealize Automation virtual machine during the vRealize Automation installation process. After you successfully complete the installation, you can delete these snapshots.

Repeat this procedure to remove all of the vRealize Automation virtual machine snapshots you created during the implementation. The virtual machine names and their respective folders are listed in the following table.

| Virtual Machines            | vCenter Folder  |
|-----------------------------|-----------------|
| vra01svr01a.rainpole.local  | sfo01-w01fd-vra |
| vra01mssql01.rainpole.local | sfo01-w01fd-vra |
| vra01iws01a.rainpole.local  | sfo01-w01fd-vra |
| vra01ims01a.rainpole.local  | sfo01-w01fd-vra |

### Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 From the Home page, click **VMs and Templates**.
- 3 In the Navigator, expand the **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > sfo01-w01fd-vra** folder.
- 4 Right-click the **vra01svr01a.rainpole.local** virtual machine and select **Snapshots > Manage Snapshots**.
- 5 Select the **Prior to vRA IaaS Component Installation** snapshot and click **Delete** icon.
- 6 Repeat this procedure to remove all of the remaining vRealize Automation virtual machine snapshots.

## Tenant Content Creation for Consolidated SDDC

In order to provision virtual machines in the vCenter, the tenant must be configured to utilize compute resources within the vCenter Server.

### Create Logical Switches for Business Groups for Consolidated SDDC

For each vCenter Server compute instance, you create three logical switches for each business group which simulate networks for the web, database, and application tiers.

You repeat this procedure six times to create six logical switches. The "Logical Switch Names and Descriptions" table lists the logical switch names, and the business group and tier to which you assign each switch.

**Table 3-4.** Logical Switch Names and Descriptions

| Logical Switch Name  | Description                                                   |
|----------------------|---------------------------------------------------------------|
| Production-Web-VXLAN | Logical switch for Web tier of Production Business Group      |
| Production-DB-VXLAN  | Logical switch for Database tier of Production Business Group |

**Table 3-4.** Logical Switch Names and Descriptions (Continued)

| Logical Switch Name   | Description                                                       |
|-----------------------|-------------------------------------------------------------------|
| Production-App-VXLAN  | Logical switch for Application tier of Production Business Group  |
| Development-Web-VXLAN | Logical switch for Web tier of Development Business Group         |
| Development-DB-VXLAN  | Logical switch for Database tier of Development Business Group    |
| Development-App-VXLAN | Logical switch for Application tier of Development Business Group |

**Procedure**

- 1 Log into the vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 Create a logical switch.
  - a Click **Networking & Security**.
  - b In the Navigator, select **Logical Switches**.
  - c From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager.
  - d Click the **New Logical Switch** icon.

The New Logical Switch dialog box appears.

  - e In the New Logical Switch dialog box, enter the following settings, and click **OK**.

| Setting             | Value                                                    |
|---------------------|----------------------------------------------------------|
| Name                | Production-Web-VXLAN                                     |
| Description         | Logical switch for Web tier of Production Business Group |
| Transport Zone      | SFO01W01 Universal Transport Zone                        |
| Replication Mode    | Hybrid                                                   |
| Enable IP Discovery | Selected                                                 |
| Enable MAC Learning | Deselected                                               |

The screenshot shows the 'New Logical Switch' dialog box with the following settings:

- Name:** Production-Web-VXLAN
- Description:** Logical switch for Web tier of Production Business Group
- Transport Zone:** SFO01W01 Universal Transport Zone
- Replication mode:** Hybrid (selected)
- Enable IP Discovery:** ☒
- Enable MAC Learning:** ☒

- 3 Repeat this procedure to create the remaining logical switches.



## Configure User Roles in vRealize Automation for Consolidated SDDC

Roles are sets of privileges that you associate with users to determine what tasks they can perform. Based on their responsibilities, individuals might have one or more roles associated with their user account. All user roles are assigned within the context of a specific tenant. However, some roles in the default tenant can manage system-wide configuration settings that apply to multiple tenants.

This procedure steps you through assigning roles to the `ug-ITAC-TenantAdmins` and `ug-ITAC-TenantArchitects` users and groups.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
  - b Log in using the following credentials.

| Setting   | Value                                   |
|-----------|-----------------------------------------|
| User name | ITAC-LocalRainpoleAdmin                 |
| Password  | <i>itac-localrainpoleadmin_password</i> |
| Domain    | vsphere.local                           |
- 2 Click the Administration tab.
- 3 Navigate to **Users & Groups > Directory Users and Groups**.
- 4 Enter **`ug-ITAC-TenantAdmins`** in the search box and press **Enter**.  
 The **`ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)`** group name displays in the Name text box.
- 5 Click the user group name **`ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)`**.
- 6 In the Add Roles to this Group list, select the **Application Architect, Approval Administrator, Container Administrator, Container Architect, Infrastructure Architect, Software Architect, Tenant Administrator, and XaaS Architect** check boxes, and click **Finish**.
- 7 Enter **`ug-ITAC-TenantArchitects`** in the Tenant Administrators search box and press **Enter**.  
 The **`ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local)`** group name displays in the Name text box.
- 8 Click the user group name **`ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local)`**.
- 9 In the Add Roles to this Group list, select the **Application Architect, Container Architect, Infrastructure Architect, Software Architect, XaaS Architect** check box, and click **Finish**.

## Create the Fabric Group for Consolidated SDDC

IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group.

Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric resources to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants. For the consolidated pod, only one fabric group needs to be created.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Select **Infrastructure > Endpoints > Fabric Groups**.
- 3 Click **New Fabric Group**, enter the following settings and click **OK**.

| Setting               | Value                               |
|-----------------------|-------------------------------------|
| Name                  | SFO Fabric Group                    |
| Fabric administrators | ug-ITAC-TenantAdmins@rainpole.local |

---

**NOTE** You have not yet configured a vCenter Endpoint, so no compute resource is currently available for you to select. You will configure the vCenter Endpoint later.

---

- 4 Log out of the vRealize Automation portal.

**Create Machine Prefixes for Consolidated SDDC**

As a fabric administrator, you create machine prefixes that are used to create names for machines provisioned through vRealize Automation. Tenant administrators and business group managers select these machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

Machine prefixes are shared across all tenants. Every business group has a default machine prefix. Every blueprint must have a machine prefix or use the group default prefix. Fabric administrators are responsible for managing machine prefixes. A prefix consists of a base name to be followed by a counter of a specified number of digits. When the digits are all used, vRealize Automation rolls back to the first number.

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Select **Infrastructure > Administration > Machine Prefixes**.

- 3 Click the **New** icon to create a default machine prefix for the Production group using the following settings, and click the **Save** icon.

| Setting          | Value |
|------------------|-------|
| Machine Prefix   | Prod- |
| Number of Digits | 5     |
| Next Number      | 1     |

- 4 Click the **New** icon to create a default machine prefix for the Development group using the following settings, and click the **Save** icon.

| Setting          | Value |
|------------------|-------|
| Machine Prefix   | Dev-  |
| Number of Digits | 5     |
| Next Number      | 1     |

## Create Business Groups for Consolidated SDDC

Tenant administrators create business groups to associate a set of services and resources to a set of users, that often correspond to a line of business, department, or other organizational unit. Users must belong to a business group to request machines.

For this implementation create two business groups, the Production business group and the Development business group.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Navigate to **Administration > Users and Groups > Business Groups**.
- 3 Click the **New** icon.
- 4 On the **General** tab, enter the following values and click **Next**.

| Setting                | Value                           |
|------------------------|---------------------------------|
| Name                   | Production                      |
| Send Manager emails to | ITAC-TenantAdmin@rainpole.local |

- 5 On the **Members** tab, enter **ug-ITAC-TenantAdmins@rainpole.local** in the Group manager role text box, and click **Next**.
- 6 On the **Infrastructure** tab, select **Prod-** from the **Default machine prefix** drop-down menu and click **Finish**.
- 7 Click the **New** icon.

- 8 On the General tab, configure the following values, and click **Next**.

| Setting                | Value                           |
|------------------------|---------------------------------|
| Name                   | Development                     |
| Send Manager emails to | ITAC-TenantAdmin@rainpole.local |

- 9 On the Members tab, enter **ug-ITAC-TenantAdmins@rainpole.local** in the Group manager role text box and click **Next**.
- 10 On the **Infrastructure** tab, select **Dev-** from the **Default machine prefix** drop-down menu, and click **Finish**.

## Create Reservation Policies for Consolidated SDDC

You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

When you request a machine, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine. You can apply a reservation policy to a blueprint to restrict the machines provisioned from that blueprint to a subset of available reservations. A reservation policy is often used to collect resources into groups for different service levels, or to make a specific type of resource easily available for a particular purpose. You can add multiple reservations to a reservation policy, but a reservation can belong to only one policy. You can assign a single reservation policy to more than one blueprint. A blueprint can have only one reservation policy. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Navigate to **Infrastructure > Reservation > Reservation Policies**.
- 3 Click the **New** icon, configure the following settings, and click the **Save** icon.

| Setting     | Value                                                   |
|-------------|---------------------------------------------------------|
| Name        | SFO-Production-Policy                                   |
| Description | Reservation policy for Production Business Group in SFO |

- 4 Click the **New** icon, configure the following settings, and click the **Save** icon.

| Setting     | Value                                                    |
|-------------|----------------------------------------------------------|
| Name        | SFO-Development-Policy                                   |
| Description | Reservation policy for Development Business Group in SFO |

- 5 Click the **New** icon, configure the following settings, and click the **Save** icon.

| Setting     | Value                                               |
|-------------|-----------------------------------------------------|
| Name        | SFO-Edge-Policy                                     |
| Description | Reservation policy for Tenant Edge resources in SFO |

## Create a vSphere Endpoint in vRealize Automation for Consolidated SDDC

To allow vRealize Automation to manage the infrastructure, IaaS administrators create endpoints and configure user credentials for those endpoints. When you create an endpoint for vSphere, vRealize Automation can communicate with the vCenter Server environment and discover compute resources that are managed by vCenter Server, collect data, and provision machines.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Virtual > vSphere (vCenter)**.
- 3 On the General page, configure the vRealize Automation Endpoint with the following settings, and then click on the **Test Connection**.

| Setting   | Value for vSphere                                          |
|-----------|------------------------------------------------------------|
| Name      | VSPHERE-SFO                                                |
| Address   | <code>https://sfo01w01vc01.sfo01.rainpole.local/sdk</code> |
| User Name | <code>rainpole\svc-vra</code>                              |
| Password  | <i>svc-vra_password</i>                                    |

- 4 If a Security Alert window appears, click **OK**.
- 5 Click **OK** to create the Endpoint.

---

**Note** The vSphere Endpoint Name must be identical to the name that you used to install the proxy agent. See [“Install the vRealize Automation Environment for Consolidated SDDC,”](#) on page 115.

---

## Create an NSX Endpoint in vRealize Automation for Consolidated SDDC

When you create an endpoint for NSX, vRealize Automation can communicate with NSX Manager to discover networking resources.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Network and Security > NSX**.
- 3 On the General page, configure the vRealize Automation Endpoint with the following settings and then click on the **Associations** tab.

| Setting   | Value                                      |
|-----------|--------------------------------------------|
| Name      | NSXEndpoint                                |
| Address   | https://sfo01w01nsx01.sfo01.rainpole.local |
| User Name | rainpole\svc-vra                           |
| Password  | svc-vra_password                           |

- 4 On the Associations tab, click **New**, choose **VSPHERE-SFO** from the **Name** drop-down menu, and click **OK**.
- 5 Click **Test Connection**.
- 6 On the Security Alert window, click **OK**.
- 7 Click **OK** to create the Endpoint.

## Add Compute Resources to a Fabric Group for Consolidated SDDC

You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Navigate to **Infrastructure > Endpoints > Fabric Groups**.

- 3 In the **Name** column, hover the mouse pointer over the fabric group name **SFO Fabric Group**, and click **Edit**.
- 4 On the Edit Fabric Group page, select **sfo01-w01-consolidated01** from the Compute resources table, and click **OK**.

**Infrastructure Service Portal**

Home Catalog Items Requests Inbox Design Administration **Infrastructure** Containers

← Infrastructure

Agents

**Fabric Groups**

Endpoints

**Edit Fabric Group**  
Modify the fabric group.

\*Name: SFO Fabric Group

Description:

Fabric administrators: ug-ITAC-TenantAdmins@rainpole.local

Compute resources:

|                                     | Name                     | Endpoint    | Platform Type     |
|-------------------------------------|--------------------------|-------------|-------------------|
| <input checked="" type="checkbox"/> | sfo01-w01-consolidated01 | VSPHERE-SFO | vSphere (vCenter) |

**NOTE** It might take several minutes for vRealize Automation to connect to the vCenter Server system and associated clusters. If you are still not able to see the cluster after sufficient time has passed, try to restart the proxy agent services in the virtual machine vra01ims01a.sfo01.rainpole.local.

- 5 Navigate to **Infrastructure > Compute Resources > Compute Resources**.
- 6 In the Compute Resource column, hover the mouse pointer over the compute cluster **sfo01-w01-consolidated01**, and click **Data Collection**.
- 7 Click on the **Request now** buttons in each field on the page.  
Wait a few seconds for the data collection process to complete.
- 8 Click **Refresh**, and verify that Status for both Inventory and State shows **Succeeded**.

## Create External Network Profiles for Consolidated SDDC

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for those virtual machines. Each network profile is configured for a specific network port group or virtual network to specify IP address and routing configuration for virtual machines provisioned to that network.

Repeat this procedure six times to create the following external network profiles.

- Ext-Net-Profile-Production-App
- Ext-Net-Profile-Production-DB
- Ext-Net-Profile-Production-Web
- Ext-Net-Profile-Development-App
- Ext-Net-Profile-Development-DB
- Ext-Net-Profile-Development-Web

**Procedure**

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Navigate to **Infrastructure > Reservations > Network Profiles**, and click **New > External**.
- 3 On the New Network Profile - External page, specify the network profiles on the **General** tab.
  - a Add the values for the Production Group External Network Profile.

| Setting     | Production Web Value                                               | Production DB Value                                               | Production App Value                                               |
|-------------|--------------------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------|
| Name        | Ext-Net-Profile-Production-Web                                     | Ext-Net-Profile-Production-DB                                     | Ext-Net-Profile-Production-App                                     |
| Description | External Network profile for Web Tier of Production Business Group | External Network profile for DB Tier of Production Business Group | External Network profile for App Tier of Production Business Group |
| Subnet mask | 255.255.255.0                                                      | 255.255.255.0                                                     | 255.255.255.0                                                      |
| Gateway     | 172.11.10.1                                                        | 172.11.11.1                                                       | 172.11.12.1                                                        |

- b Add the values for the Development Group External Network Profile.

| Setting     | Development Web Value                                               | Development DB Value                                               | Development App Value                                               |
|-------------|---------------------------------------------------------------------|--------------------------------------------------------------------|---------------------------------------------------------------------|
| Name        | Ext-Net-Profile-Development-Web                                     | Ext-Net-Profile-Development-DB                                     | Ext-Net-Profile-Development-App                                     |
| Description | External Network profile for Web Tier of Development Business Group | External Network profile for DB Tier of Development Business Group | External Network profile for App Tier of Development Business Group |
| Subnet mask | 255.255.255.0                                                       | 255.255.255.0                                                      | 255.255.255.0                                                       |
| Gateway     | 172.12.10.1                                                         | 172.12.11.1                                                        | 172.12.12.1                                                         |

- 4 Click the **DNS** tab. Enter the following values for the profile you are creating.

| Setting           | Value                |
|-------------------|----------------------|
| Primary DNS       | 172.16.11.5          |
| Secondary DNS     | 172.16.11.4          |
| DNS suffix        | sfo01.rainpole.local |
| DNS search suffix | sfo01.rainpole.local |



- 5 Click the **Network Ranges** tab. Click the **New** button and enter the following values for the profile you are creating.
  - a Enter the following values for Production Business Network Range.

| Setting     | Production Web Value                             | Production DB Value                             | Production App Value                             |
|-------------|--------------------------------------------------|-------------------------------------------------|--------------------------------------------------|
| Name        | Production-Web                                   | Production-DB                                   | Production-App                                   |
| Description | Static IP range for Web Tier of Production Group | Static IP range for DB Tier of Production Group | Static IP range for App Tier of Production Group |
| Start IP    | 172.11.10.20                                     | 172.11.11.20                                    | 172.11.12.20                                     |
| End IP      | 172.11.10.250                                    | 172.11.11.250                                   | 172.11.12.250                                    |

- b Enter the following values for Development Business IP Range.

| Setting     | Development Web Value                             | Development DB Value                             | Development App Value                             |
|-------------|---------------------------------------------------|--------------------------------------------------|---------------------------------------------------|
| Name        | Development-Web                                   | Development-DB                                   | Development-App                                   |
| Description | Static IP range for Web Tier of Development Group | Static IP range for DB Tier of Development Group | Static IP range for App Tier of Development Group |
| Start IP    | 172.12.10.20                                      | 172.12.11.20                                     | 172.12.12.20                                      |
| End IP      | 172.12.10.250                                     | 172.12.11.250                                    | 172.12.12.250                                     |

- c Click **OK** to save the network range.
- 6 Click **OK** to save the network profile.
- 7 Repeat this procedure to create additional external network profiles.

When all of the network profiles have been added, the Network Profiles page displays six profiles.

## Create Reservations for the Cluster for Consolidated SDDC

Before members of a business group can request machines, fabric administrators must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource. For the scenarios, you perform this procedure twice to create reservations for both the Production and Development business groups.

| Group       | Name                    |
|-------------|-------------------------|
| Production  | SFO01-Comp01-Prod-Res01 |
| Development | SFO01-Comp01-Dev-Res01  |

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

- 2 Navigate to **Infrastructure > Reservations > Reservations**, and click **New > vSphere (vCenter)**.

- 3 On the New Reservation - vSphere (vCenter) page, click the **General** tab and configure the following values.

| Setting                 | Production Group Value  | Development Group Value |
|-------------------------|-------------------------|-------------------------|
| Name                    | SFO01-Comp01-Prod-Res01 | SFO01-Comp01-Dev-Res01  |
| Tenant                  | rainpole                | rainpole                |
| Business Group          | Production              | Development             |
| Reservation Policy      | SFO-Production-Policy   | SFO-Development-Policy  |
| Priority                | 100                     | 100                     |
| Enable This Reservation | Selected                | Selected                |

- 4 On the New Reservation - vSphere (vCenter) page, click the **Resources** tab.
  - a Select **sfo01-w01-consolidated01(VSPHERE-SFO)** from the **Compute resource** drop-down menu.
  - b In the This Reservation column of the Memory (GB) table, enter **200**.
  - c In the Storage (GB) table, select the check box for datastore **sfo01-w01-vsan01**, and enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
  - d Select **sfo01-w01rp-user-vm** from the **Resource pool** drop-down menu.
- 5 On the New Reservation - vSphere (vCenter) page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the Network Paths list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.
  - a Configure the Production Business Group with the following values.

| Production Network Path            | Production Group Network Profile |
|------------------------------------|----------------------------------|
| vxw-dvs-xxxxx-Production-Web-VXLAN | Ext-Net-Profile-Production-Web   |
| vxw-dvs-xxxxx-Production-DB-VXLAN  | Ext-Net-Profile-Production-DB    |
| vxw-dvs-xxxxx-Production-App-VXLAN | Ext-Net-Profile-Production-App   |

- b Configure the Development Business Group with the following values.

| Development Network Path            | Development Group Network Profile |
|-------------------------------------|-----------------------------------|
| vxw-dvs-xxxxx-Development-Web-VXLAN | Ext-Net-Profile-Development-Web   |
| vxw-dvs-xxxxx-Development-DB-VXLAN  | Ext-Net-Profile-Development-DB    |
| vxw-dvs-xxxxx-Development-App-VXLAN | Ext-Net-Profile-Development-App   |

- 7 Click **OK** to save the reservation.
- 8 Repeat this procedure to create the reservation for the development group.

## Create Reservations for the User Edge Resources for Consolidated SDDC

Before members of a business group can request virtual machines, fabric administrators must allocate resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

Perform this procedure twice to create Edge reservations for both the Production and Development business groups.

| Group       | Name                    |
|-------------|-------------------------|
| Production  | SFO01-Edge01-Prod-Res01 |
| Development | SFO01-Edge01-Dev-Res01  |

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Navigate to **Infrastructure > Reservations > Reservations**, and click **New > vSphere (vCenter)**.
- 3 On the New Reservation - vSphere (vCenter) page, click the **General** tab, and configure the following values for your business group.

| Setting                 | Production Group Value  | Development Group Value |
|-------------------------|-------------------------|-------------------------|
| Name                    | SFO01-Edge01-Prod-Res01 | SFO01-Edge01-Dev-Res01  |
| Tenant                  | rainpole                | rainpole                |
| Business Group          | Production              | Development             |
| Reservation Policy      | SFO-Edge-Policy         | SFO-Edge-Policy         |
| Priority                | 100                     | 100                     |
| Enable This Reservation | Selected                | Selected                |

- 4 On the New Reservation - vSphere (vCenter) page, click the **Resources** tab.
  - a Select **sfo01-w01-consolidated01(VSPHERE-SFO)** from the **Compute resource** drop-down menu.
  - b Enter **200** in the This Reservation column of the Memory (GB) table.
  - c In the Storage (GB) table, select the check box for datastore **sfo01-w-01-vsan01**, enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
  - d Select **sfo01-w01rp-user-edge** from the **Resource pool** drop-down menu.
- 5 On the New Reservation - vSphere (vCenter) page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the Network Paths list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

| Production Port Group              | Production Network Profile     |
|------------------------------------|--------------------------------|
| vxw-dvs-xxxxx-Production-Web-VXLAN | Ext-Net-Profile-Production-Web |
| vxw-dvs-xxxxx-Production-DB-VXLAN  | Ext-Net-Profile-Production-DB  |
| vxw-dvs-xxxxx-Production-App-VXLAN | Ext-Net-Profile-Production-App |

Development Business Group

| Development Port Group              | Development Network Profile     |
|-------------------------------------|---------------------------------|
| vxw-dvs-xxxxx-Development-Web-VXLAN | Ext-Net-Profile-Development-Web |
| vxw-dvs-xxxxx-Development-DB-VXLAN  | Ext-Net-Profile-Development-DB  |
| vxw-dvs-xxxxx-Development-App-VXLAN | Ext-Net-Profile-Development-App |

- 7 Click **OK** to save the reservation.
- 8 Repeat the procedure to create a Edge reservation for the Development Business Group.

## Create Blueprint Customization Specifications for Consolidated SDDC

Create two customization specifications, one for Linux and one for Windows, for use by the virtual machines you will deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

You will later use the customization specifications you create when you create blueprints for use with vRealize Automation.

### Create a Linux Customization Specification for Consolidated SDDC

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.
- 3 Select the vCenter Server **sfo01w01vc01.sfo01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.  
The New VM Guest Customization Spec wizard appears.
- 5 On the Specify Properties page, select **Linux** from the **Target VM Operating System** drop-down menu, enter **itac-linux-custom-spec** for the **Customization Spec Name**, and click **Next**.
- 6 On the Set Computer Name page, select **Use the virtual machine name**, enter **sfo01.rainpole.local** in the **Domain Name** text box and click **Next**.
- 7 On the Time Zone page, specify the time zone as shown in the table below for the virtual machine, and click **Next**.

| Setting               | Value       |
|-----------------------|-------------|
| Area                  | America     |
| Location              | Los Angeles |
| Hardware Clock Set To | Local Time  |

- 8 On the Configure Network page, click **Next**.
- 9 On the Enter DNS and domain settings page, leave the default settings, and click **Next**.
- 10 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

## Create a Microsoft Windows Customization Specification for Consolidated SDDC

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.
- 3 Select the vCenter Server **sfo01w01vc01.sfo01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.  
The New VM Guest Customization wizard appears.
- 5 On the Specify Properties page, select **Windows** from the **Target VM Operating System** drop-down menu, enter **itac-windows-joindomain-custom-spec** for the **Customization Spec Name**, and click **Next**.
- 6 On the Set Registration Information page, enter **Rainpole** for the virtual machine owner's **Name** and **Organization**, and click **Next**.
- 7 On the Set Computer Name page, select **Use the virtual machine name**, and click **Next**.  
The operating system uses this name to identify itself on the network.
- 8 On the Enter Windows License page, provide licensing information for the Windows operating system, enter the **volume\_license\_key**, and click **Next**.
- 9 Specify the administrator password for use with the virtual machine, and click **Next**.
- 10 On the Time Zone page, select **(GMT-08:00) Pacific Time(US & Canada)**, and click **Next**.
- 11 On the Run Once page, click **Next**.
- 12 On the Configure Network page, click **Next**.
- 13 On the Set Workgroup or Domain page, select **Windows Server Domain**, configure the following settings, and click **Next**.

| Setting   | Value                              |
|-----------|------------------------------------|
| Domain    | sfo01.rainpole.local               |
| User name | ad_admin_acct@sfo01.rainpole.local |
| Password  | ad_admin_pwd                       |

- 14 On the Set Operating System Options page, select **Generate New Security ID (SID)**, and click **Next**.

- 15 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

## Create VM Templates for Blueprints in Consolidated SDDC

You create virtual machine templates that will be used while creating blueprints.

The table below lists the templates that need to be created.

| VM Template Name          | Guest OS                             |
|---------------------------|--------------------------------------|
| redhat6-enterprise-64     | Red Hat Enterprise Server 6 (64-bit) |
| windows-2012r2-64         | Windows Server 2012 R2 (64-bit)      |
| windows-2012r2-64-sql2012 | Windows Server 2012 R2 (64-bit)      |

## Configure Single Machine Blueprints for Consolidated SDDC

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

### Create a Service Catalog for Consolidated SDDC

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

#### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Navigate to the **Administration** tab, click **Catalog Management > Services**, and click **New**.

The New Service page appears.

- 3 In the New Service page, configure the following settings and click **OK**.

| Setting     | Value                   |
|-------------|-------------------------|
| Name        | SFO Service Catalog     |
| Description | Default setting (blank) |
| Status      | Active                  |
| Icon        | Default setting (blank) |
| Status      | Default setting (blank) |
| Hours       | Default setting (blank) |
| Owner       | Default setting (blank) |

| Setting       | Value                   |
|---------------|-------------------------|
| Support Team  | Default setting (blank) |
| Change Window | Default setting (blank) |

## Create a Single Machine Blueprint for Consolidated SDDC

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create the following six blueprints.

| Blueprint Name                                 | VM Template                                                  | Customization Spec                  | Reservation Policy     |
|------------------------------------------------|--------------------------------------------------------------|-------------------------------------|------------------------|
| Windows Server 2012 R2 - SFO Prod              | windows-2012r2-64<br>(sfo01w01vc01.sfo01.rainpole.local)     | itac-windows-joindomain-custom-spec | SFO-Production-Policy  |
| Windows Server 2012 R2 - SFO Dev               | windows-2012r2-64<br>(sfo01w01vc01.sfo01.rainpole.local)     | itac-windows-joindomain-custom-spec | SFO-Development-Policy |
| Windows Server 2012 R2 With SQL2012 - SFO Prod | windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local) | itac-windows-joindomain-custom-spec | SFO-Production-Policy  |
| Windows Server 2012 R2 With SQL2012 - SFO Dev  | windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local) | itac-windows-joindomain-custom-spec | SFO-Development-Policy |
| Redhat Enterprise Linux 6 - SFO Prod           | redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)     | itac-linux-custom-spec              | SFO-Production-Policy  |
| Redhat Enterprise Linux 6 - SFO Dev            | redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)     | itac-linux-custom-spec              | SFO-Development-Policy |

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                            |
|-----------|----------------------------------|
| User name | itac-tenantadmin                 |
| Password  | <i>itac-tenantadmin_password</i> |
| Domain    | rainpole.local                   |

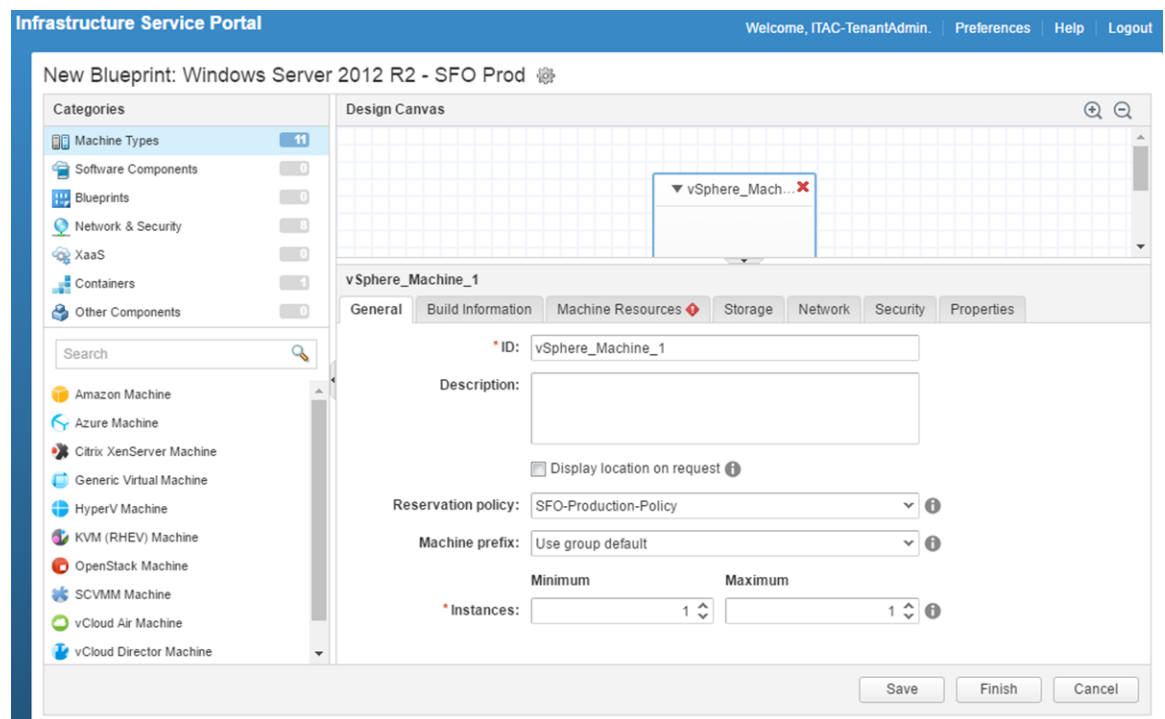
- 2 Navigate to **Design > Blueprints**.
- 3 Click **New**.
- 4 In the New Blueprint dialog box, configure the following settings on the **General** tab. Click **OK**.

| Setting        | Value                             |
|----------------|-----------------------------------|
| Name           | Windows Server 2012 R2 - SFO Prod |
| Archive (days) | 15                                |

| Setting          | Value                   |
|------------------|-------------------------|
| Deployment limit | Default setting (blank) |
| Minimum          | 30                      |
| Maximum          | 270                     |

- 5 Select and drag the **vSphere Machine** icon to Design Canvas.
- 6 Click the **General** tab, configure the following settings, and click **Save**.

| Setting                     | Default                             |
|-----------------------------|-------------------------------------|
| ID                          | Default setting (vSphere_Machine_1) |
| Description                 | Default setting (blank)             |
| Display location on request | Deselected                          |
| Reservation policy          | SFO-Production-Policy               |
| Machine prefix              | Use group default                   |
| Minimum                     | Default setting (blank)             |
| Maximum                     | Default setting (blank)             |



- 7 Click the **Build Information** tab, configure the following settings, and click **Save**.

| Setting               | Value         |
|-----------------------|---------------|
| Blueprint type        | Server        |
| Action                | Clone         |
| Provisioning workflow | CloneWorkflow |



| Setting            | Value                               |
|--------------------|-------------------------------------|
| Clone from         | windows-2012r2-64 template          |
| Customization spec | itac-windows-joindomain-custom-spec |

**NOTE** If the value of the **Clone from** setting does not list **windows-2012r2-64 template**, you must perform a data collection on the **sfo01-w01-comp01** Compute Resource.

- 8 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

| Setting      | Minimum                 | Maximum              |
|--------------|-------------------------|----------------------|
| CPU          | 2                       | 4                    |
| Memory (MB): | 4096                    | 16384                |
| Storage      | Default setting (blank) | Default setting (60) |

- 9 Click the **Network** tab.

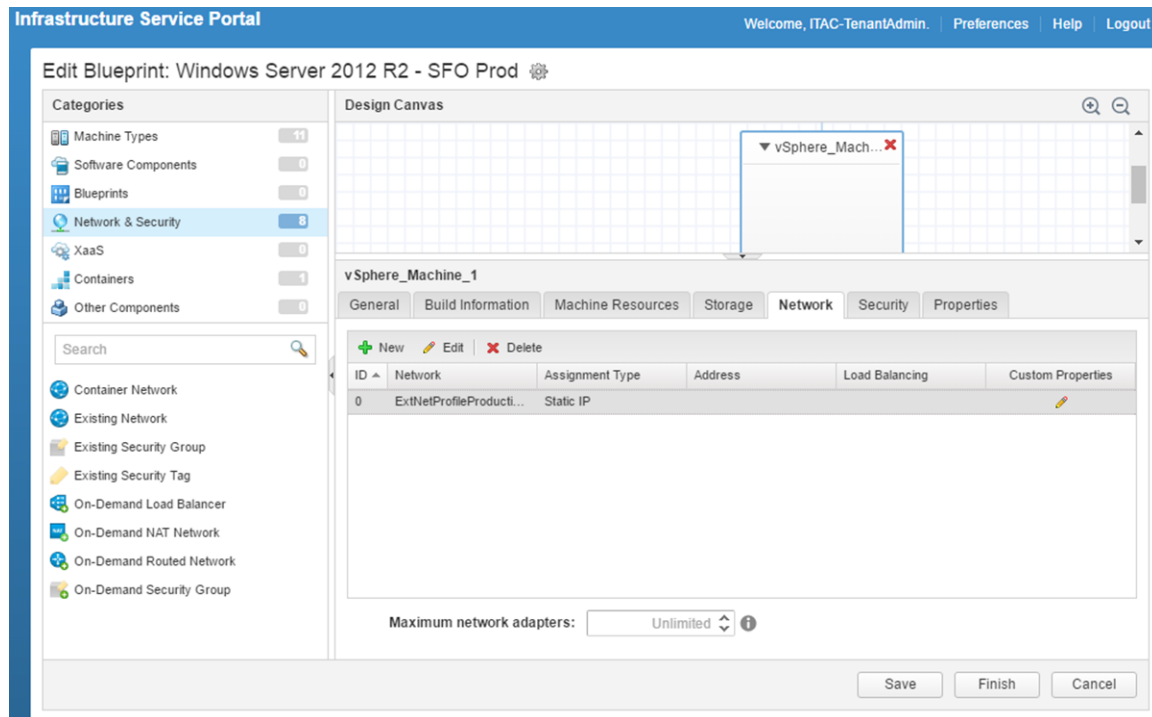
- Select **Network & Security** in the Categories section to display the list of available network and security components.
- Select the **Existing Network** component and drag it onto the design canvas.
- Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

| Blueprint Name                                 | Existing network                |
|------------------------------------------------|---------------------------------|
| Windows Server 2012 R2 - SFO Prod              | Ext-Net-Profile-Production-Web  |
| Windows Server 2012 R2 - SFO Dev               | Ext-Net-Profile-Development-Web |
| Windows Server 2012 R2 With SQL2012 - SFO Prod | Ext-Net-Profile-Production-DB   |
| Windows Server 2012 R2 With SQL2012 - SFO Dev  | Ext-Net-Profile-Development-DB  |
| Redhat Enterprise Linux 6 - SFO Prod           | Ext-Net-Profile-Production-App  |
| Redhat Enterprise Linux 6 - SFO Dev            | Ext-Net-Profile-Development-App |

- Click **Save**.
- Select **vSphere\_Machine** properties from the design canvas.

- f Select the **Network** tab, click **New**, and configure the following settings. Click **OK**.

| Network                         | Assignment Type | Address                 |
|---------------------------------|-----------------|-------------------------|
| Ext-Net-Profile-Production-Web  | Static IP       | Default setting (blank) |
| Ext-Net-Profile-Development-Web | Static IP       | Default setting (blank) |
| Ext-Net-Profile-Production-DB   | Static IP       | Default setting (blank) |
| Ext-Net-Profile-Development-DB  | Static IP       | Default setting (blank) |
| Ext-Net-Profile-Production-App  | Static IP       | Default setting (blank) |
| Ext-Net-Profile-Development-App | Static IP       | Default setting (blank) |



- g Click **Finish** to save the blueprint.
- 10 Select the blueprint **Windows Server 2012 R2 - SFO Prod** and click **Publish**.
- 11 Repeat this procedure to create additional blueprints.

## Create Entitlements for Business Groups for Consolidated SDDC

You add a service, catalog item, or action to an entitlement, allowing the users and groups identified in the entitlement to request provisionable items in the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, users cannot use the blueprint.

Perform this procedure twice to create entitlements for both the Production and Development business groups.

| Entitlement Name          | Status | Business Group | User & Groups        |
|---------------------------|--------|----------------|----------------------|
| Prod-SingleVM-Entitlement | Active | Production     | ug-ITAC-TenantAdmins |
| Dev-SingleVM-Entitlement  | Active | Development    | ug-ITAC-TenantAdmins |

## Procedure

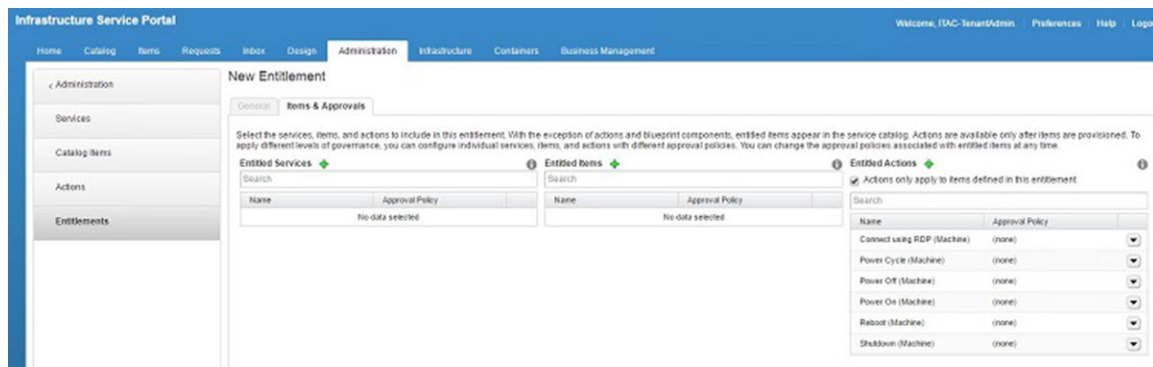
- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Click the **Administration** tab, and click **Catalog Management > Entitlements**.
- 3 Click **New**.  
The New Entitlement page appears.
- 4 On the New Entitlement page, select the **General** tab, configure the following values, and click **Next**.

| Setting              | Production Value          | Development Value        |
|----------------------|---------------------------|--------------------------|
| Name                 | Prod-SingleVM-Entitlement | Dev-SingleVM-Entitlement |
| Description          | Default setting (blank)   | Default setting (blank)  |
| Expiration Date      | Default setting (blank)   | Default setting (blank)  |
| Status               | Active                    | Active                   |
| Business Group       | Production                | Development              |
| All Users and Groups | Unselected                | Unselected               |
| Users & Groups       | ug-ITAC-TenantAdmins      | ug-ITAC-TenantAdmins     |

- 5 Click the **Items & Approvals** tab.
  - a On the Entitlement Actions page, click the **Add Action** icon and add the following actions.
    - Connect using RDP (Machine)
    - Power Cycle (Machine)
    - Power Off (Machine)
    - Power On (Machine)
    - Reboot (Machine)
    - Shutdown (Machine)



- b Click **Finish**.
- 6 Repeat this procedure to create an entitlement for the Development business group.  
Use the same Entitled Actions as for the Production business group.

## Configure Entitlements for Blueprints for Consolidated SDDC

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the blueprints with their entitlement.

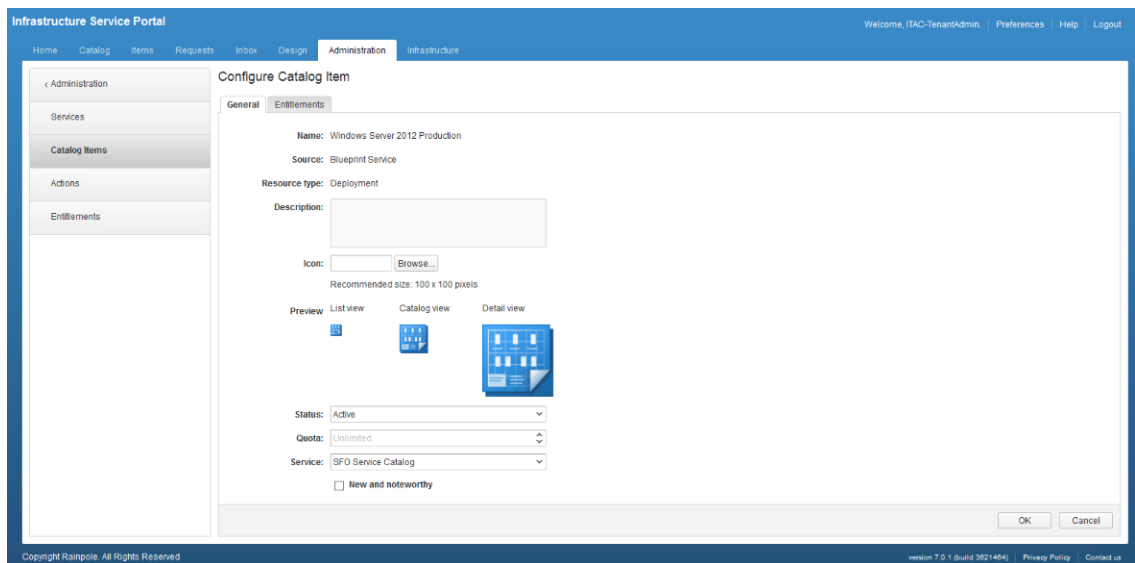
| Blueprint Name                                 | Service Catalog     | Add to Entitlement        |
|------------------------------------------------|---------------------|---------------------------|
| Windows Server 2012 R2 - SFO Prod              | SFO Service Catalog | Prod-SingleVM-Entitlement |
| Windows Server 2012 R2 - SFO Dev               | SFO Service Catalog | Dev-SingleVM-Entitlement  |
| Windows Server 2012 R2 With SQL2012 - SFO Prod | SFO Service Catalog | Prod-SingleVM-Entitlement |
| Windows Server 2012 R2 With SQL2012 - SFO Dev  | SFO Service Catalog | Dev-SingleVM-Entitlement  |
| Redhat Enterprise Linux 6 - SFO Prod           | SFO Service Catalog | Prod-SingleVM-Entitlement |
| Redhat Enterprise Linux 6 - SFO Dev            | SFO Service Catalog | Dev-SingleVM-Entitlement  |

## Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | rainpole.local            |

- 2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.
- 3 On the Catalog Items pane, select the **Windows Server 2012 R2 - SFO Prod** blueprint in the **Catalog Items** list and click **Configure**.
- 4 On the **General** tab of the **Configure Catalog Item** dialog box, select **SFO Service Catalog** from the **Service** drop-down menu, and click **OK**.



- 5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.
  - a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.  
The Edit Entitlement pane appears.
  - b Select the **Items & Approvals** tab and add the **Windows Server 2012 R2 - SFO Prod** blueprint to the **Entitled Items** list. Click **OK**.
  - c Click **Finish**.

- 6 Select the **Catalog** tab and verify that the blueprints are listed in the Service Catalog.



- 7 Repeat this procedure to associate all of the blueprints with their entitlements.

## Test the Deployment of a Single Machine Blueprint for Consolidated SDDC

Test your environment and confirm the successful provisioning of virtual machines using the blueprints that have been created.

### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

| Setting   | Value                     |
|-----------|---------------------------|
| User name | itac-tenantadmin          |
| Password  | itac-tenantadmin_password |
| Domain    | Rainpole.local            |

- 2 Select the **Catalog** tab, and click **SFO Service Catalog** from the catalog of available services.
- 3 Click the **Request** button for the **Windows Server 2012 R2 - SFO Prod** blueprint.
- 4 Click **Submit**.
- 5 Verify the request finishes successfully.
  - a Select the **Requests** tab.
  - b Select the request you submitted and wait several minutes for the request to complete.  
Click the **Refresh** icon every few minutes until a Successful message appears under Status.
  - c Click **View Details**.
  - d Under Status Details, verify that the virtual machine successfully provisioned.
- 6 Verify the virtual machine provisions in the consolidated cluster.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local**.
  - b Log in as the vCenter Server administrator using the following credentials.
 

| Setting   | Value                         |
|-----------|-------------------------------|
| User name | administrator@vsphere.local   |
| Password  | <i>vcenter_admin_password</i> |
  - c Select **Home > VMs and Templates**.
  - d In the Navigator panel, expand the vCenter Server cluster **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01-consolidated01 > sfo01-w01-user-vm**, and verify the existence of the virtual machine.





# Operations Implementation for Consolidated SDDC

# 4

Deploy vRealize Operations Manager, vRealize Log Insight and Update Manager Download Service in the consolidated cluster to add monitoring capabilities to your SDDC.

- [vRealize Operations Manager Implementation for Consolidated SDDC](#) on page 181  
Deploy the vRealize Operations Manager analytics cluster with a single node to monitor the resources in your SDDC. Deploy also the remote collector group with a single node to collect data from the management components in the consolidated SDDC.
- [vRealize Log Insight Implementation for Consolidated SDDC](#) on page 216  
Deploy vRealize Log Insight in a single-node configuration consisting of a single master node with an integrated load balancer.
- [vSphere Update Manager Download Service Implementation for Consolidated SDDC](#) on page 253  
Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository for consolidated SDDC.

## vRealize Operations Manager Implementation for Consolidated SDDC

Deploy the vRealize Operations Manager analytics cluster with a single node to monitor the resources in your SDDC. Deploy also the remote collector group with a single node to collect data from the management components in the consolidated SDDC.

### Procedure

- 1 [Deploy vRealize Operations Manager for Consolidated SDDC](#) on page 182  
Start the deployment of vRealize Operations Manager in the consolidated cluster by deploying the nodes of the analytics cluster and the remote collector group.
- 2 [Configure the Load Balancer for vRealize Operations Manager for Consolidated SDDC](#) on page 191  
Configure load balancing for the analytics cluster on the dedicated sfo01w01lb01 NSX Edge services gateway. The remote collector group does not require load balancing.
- 3 [Add an Authentication Source for the Active Directory for Consolidated SDDC](#) on page 195  
Connect vRealize Operations Manager to the Active Directory of the Consolidated SDDC for central user management and access control.
- 4 [Configure User Access in vSphere for Integration with vRealize Operations Manager for Consolidated SDDC](#) on page 196  
Configure operations service accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the consolidated cluster.

- 5 [Add vCenter Adapter Instance to vRealize Operations Manager for Consolidated SDDC](#) on page 198  
After you deploy the analytics cluster and the remote collector node of vRealize Operations Manager and start vRealize Operations Manager, add vCenter Adapter for the Consolidated vCenter Server.
- 6 [Connect vRealize Operations Manager to the NSX Manager for Consolidated SDDC](#) on page 199  
Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the vSphere cluster and view the vSphere hosts in the NSX transport zones. You can also access end to end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.
- 7 [Connect vRealize Operations Manager to vRealize Automation for Consolidated SDDC](#) on page 205  
Configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.
- 8 [Connect vRealize Operations Manager with vRealize Business for Consolidated SDDC](#) on page 210  
Configure the vRealize Operations Manager Management Pack for vRealize Business to view your infrastructure performance, cost information, and also troubleshooting tips. You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.
- 9 [Enable Storage Device Monitoring in vRealize Operations Manager for Consolidated SDDC](#) on page 212  
Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology, and to monitor the capacity and problems on storage components.
- 10 [Enable vSAN Monitoring in vRealize Operations Manager for Consolidated SDDC](#) on page 214  
Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology and to monitor capacity and problems.
- 11 [Configure E-Mail Alerts in vRealize Operations Manager for Consolidated SDDC](#) on page 216  
You configure e-mail notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

## Deploy vRealize Operations Manager for Consolidated SDDC

Start the deployment of vRealize Operations Manager in the consolidated cluster by deploying the nodes of the analytics cluster and the remote collector group.

### Procedure

- 1 [Prerequisites for Deploying vRealize Operations Manager for Consolidated SDDC](#) on page 183  
Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment.
- 2 [Deploy the Virtual Appliance for the Analytics Cluster for Consolidated SDDC](#) on page 185  
Use the vSphere Web Client to deploy the vRealize Operations Manager node as a virtual appliance in the consolidated cluster.
- 3 [Configure the Analytics Cluster Node for Consolidated SDDC](#) on page 186  
After you deploy the virtual appliance for the master node of the vRealize Operations Manager analytics cluster, enable its administration role in the cluster.
- 4 [Deploy the Remote Collector Virtual Appliance for Consolidated SDDC](#) on page 187  
After you deploy the master node in analytics cluster, use the vSphere Web Client to deploy the virtual appliance for the remote collector for the Consolidated SDDC. You deploy a remote collector to forward data from the vCenter Server instance to the analytics cluster .

- 5 [Connect the Remote Collector Node to the Analytics Cluster for Consolidated SDDC](#) on page 189  
After you deploy the virtual appliance for the remote collector node, configure the settings of the remote collector and connect it to the analytics cluster.
- 6 [Start vRealize Operations Manager for Consolidated SDDC](#) on page 190  
After you deploy the virtual appliances for the analytics cluster node and for the remote collector node, start the analytics cluster.
- 7 [Assign a License to vRealize Operations Manager for Consolidated SDDC](#) on page 190  
After you deploy and start vRealize Operations Manager, you assign a valid license.
- 8 [Group Remote Collector Nodes for Consolidated SDDC](#) on page 191  
After you start vRealize Operations Manager and assign it a license, join the remote collector node into a collector group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

## Prerequisites for Deploying vRealize Operations Manager for Consolidated SDDC

Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment.

### IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the application virtual networks are available for the consolidated SDDC deployment.

For the analytics cluster application virtual network, allocate one static IP address and FQDN for the master node and one for the load balancer, and map the host name to the IP address. For the remote collector group, allocate one static IP address and FQDN.

**Table 4-1.** Application Virtual Network Names for vRealize Operations Manager

| vRealize Operations Manager Component | Application Virtual Network |
|---------------------------------------|-----------------------------|
| Analytics Cluster                     | Mgmt-xRegion01-VXLAN        |
| Remote Collector Group                | Mgmt-RegionA01-VXLAN        |

**Table 4-2.** IP Addresses and Host Names for the Analytics Cluster

| Role                               | IP Address                                                         | FQDN                                                                                     |
|------------------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| External load balancer VIP address | 192.168.11.35                                                      | vrops01svr01.rainpole.local                                                              |
| Master node                        | 192.168.11.31                                                      | vrops01svr01a.rainpole.local                                                             |
| Default gateway                    | 192.168.11.1                                                       | -                                                                                        |
| DNS server                         | 172.16.11.4                                                        | -                                                                                        |
| Subnet mask                        | 255.255.255.0                                                      | -                                                                                        |
| NTP servers                        | <div> <div>■ 172.16.11.251</div> <div>■ 172.16.11.252</div> </div> | <div> <div>0.ntp.sfo01.rainpole.local</div> <div>1.ntp.sfo01.rainpole.local</div> </div> |

**Table 4-3.** IP Addresses and Host Names for the Remote Collector Group

| Role                  | IP Address    | FQDN                                |
|-----------------------|---------------|-------------------------------------|
| Remote collector node | 192.168.31.31 | sfo01vropsc01a.sfo01.rainpole.local |
| Default gateway       | 192.168.31.1  | -                                   |
| DNS server            | 172.16.11.5   | -                                   |

**Table 4-3.** IP Addresses and Host Names for the Remote Collector Group (Continued)

| Role        | IP Address      | FQDN                         |
|-------------|-----------------|------------------------------|
| Subnet mask | 255.255.255.0   | -                            |
| NTP servers | ■ 172.16.11.251 | ■ 0.ntp.sfo01.rainpole.local |
|             | ■ 172.16.11.252 | ■ 1.ntp.sfo01.rainpole.local |

**Deployment Prerequisites**

Verify that your environment satisfies the following prerequisites to deploy vRealize Operations Manager.

**Table 4-4.** Deployment Prerequisites for vRealize Operations Manager

| Prerequisite            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage requirements    | <ul style="list-style-type: none"> <li>■ Virtual disk provisioning. <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per analytics cluster node. <ul style="list-style-type: none"> <li>■ Initial storage per node: 274GB</li> <li>■ Additional storage for monitoring data per node: none</li> </ul> </li> <li>■ Required storage per remote collector group node. <ul style="list-style-type: none"> <li>■ Initial storage per node: 274GB</li> </ul> </li> </ul>                                                                                                             |
| Software Features       | <ul style="list-style-type: none"> <li>■ Verify that vCenter Server is operational.</li> <li>■ Verify that the vSphere cluster has DRS and HA enabled.</li> <li>■ Verify that the NSX Manager is operational.</li> <li>■ Verify that the application virtual networks are available.</li> <li>■ Verify that the Load Balancer service is enabled on the NSX Edge services gateway.</li> <li>■ Verify that vRealize Automation is operational.</li> <li>■ Verify that vRealize Business for Cloud is operational.</li> <li>■ Verify that Postman REST API application is installed in your Chrome browser.</li> </ul> |
| Installation Package    | <ul style="list-style-type: none"> <li>■ Download the .ova file of the vRealize Operations Manager virtual appliance on the machine where you use the vSphere Web Client.</li> <li>■ Download the .pak file for the vRealize Operations Manager Management Pack for NSX for vSphere from VMware Solutions Exchange.</li> <li>■ Download the .pak file for the vRealize Operations Manager Management Pack for Storage Devices from VMware Solutions Exchange.</li> </ul>                                                                                                                                             |
| License                 | <ul style="list-style-type: none"> <li>■ Verify that you have obtained a license that covers the use of vRealize Operations Manager.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Active Directory        | <ul style="list-style-type: none"> <li>■ Verify that you have a parent Active Directory with the SDDC user roles configured for the rainpole.local domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Certification Authority | <ul style="list-style-type: none"> <li>■ Configure the root Active Directory domain controller as a certificate authority for the environment.</li> <li>■ Download the CertGenVVD tool and generate the signed certificate for the analytics cluster. See the <i>VMware Validated Design Planning and Preparation</i> documentation.</li> </ul>                                                                                                                                                                                                                                                                      |
| External Services       | <ul style="list-style-type: none"> <li>■ Verify that you have access to an SMTP server.</li> <li>■ Verify that SNMP is enabled in your network environment to monitor network devices.</li> <li>■ Verify that Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) is enabled on each network device for complete monitoring of your environment.</li> </ul>                                                                                                                                                                                                                                       |

## Deploy the Virtual Appliance for the Analytics Cluster for Consolidated SDDC

Use the vSphere Web Client to deploy the vRealize Operations Manager node as a virtual appliance in the consolidated cluster.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting          | Value                       |
|------------------|-----------------------------|
| <b>User name</b> | administrator@vsphere.local |
| <b>Password</b>  | vsphere_admin_password      |

- 2 Navigate to the sfo01w01vc01.sfo01.rainpole.local vCenter Server object.
- 3 Right-click the **sfo01w01vc01.sfo01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, browse to the location of the vRealize Operations Manager OVA file on your file system, and click **Next**.
- 5 On the Select name and location page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

| Setting               | Value                             |
|-----------------------|-----------------------------------|
| <b>Name</b>           | vrops01svr01a                     |
| <b>vCenter Server</b> | sfo01w01vc01.sfo01.rainpole.local |
| <b>Datacenter</b>     | sfo01-w01dc                       |
| <b>Folder</b>         | sfo01-w01fd-vrops                 |

- 6 On the Select a resource page, select the following values, and click **Next**.

| Setting              | Value                    |
|----------------------|--------------------------|
| <b>Datacenter</b>    | sfo01-w01dc              |
| <b>Cluster</b>       | sfo01-w01-consolidated01 |
| <b>Resource Pool</b> | sfo01-w01rp-sddc-mgmt    |

- 7 On the Review details page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the Accept license agreements page, accept the end user license agreements and click **Next**.
- 9 On the Select configuration page, from the **Configuration** drop-down menu, select the **Medium** deployment configuration of the virtual appliance, and click **Next**.
- 10 On the Select storage page, select the following datastore and configure its settings, and click **Next**.

| Setting                           | Value                       |
|-----------------------------------|-----------------------------|
| <b>Select virtual disk format</b> | Thin provision              |
| <b>VM storage policy</b>          | vSAN Default Storage Policy |
| <b>Datastore</b>                  | sfo01-w01-vsan01            |

- 11 On the Select networks page, select the distributed port group that ends with **Mgmt-xRegion01-VXLAN** on the sfo01-w01-vds01 Distributed Switch, and click **Next**.

- 12 On the Customize template page, set the IPv4 settings and select the time zone for the virtual appliance, and click **Next**.
  - a In the **Networking Properties** section, configure the following IPv4 settings.

| Setting                    | Value         |
|----------------------------|---------------|
| <b>DNS</b>                 | 172.16.11.4   |
| <b>Default gateway</b>     | 192.168.11.1  |
| <b>Static IPv4 address</b> | 192.168.11.31 |
| <b>Subnet mask</b>         | 255.255.255.0 |
| <b>Timezone setting</b>    | Etc/UTC       |

- 13 On the Ready to complete page, verify that the settings for deployment are correct, and click **Finish**.
- 14 Right-click the virtual appliance object and select **Power > Power On**.

During the power-on process, the virtual appliance expands the vRealize Operations Manager data partition as well.

- 15 Change the default empty password for the root user.
  - a In the vSphere Web Client, right-click the analytics virtual appliance and select **Open Console** to open the remote console to the appliance.

| Name                 | Role        |
|----------------------|-------------|
| <b>vrops01svr01a</b> | Master node |

- b Press ALT+F1 to switch to the command prompt.
- c At the command prompt, log in as the **root** user using empty password.
- d At the command prompt, change the default empty password for the root user account with a new **vrops\_root\_password** password.
- e Close the virtual appliance console.

## Configure the Analytics Cluster Node for Consolidated SDDC

After you deploy the virtual appliance for the master node of the vRealize Operations Manager analytics cluster, enable its administration role in the cluster.

### Prerequisites

Generate the PEM file for vRealize Operations Manager by using the CertGenVVD tool and download it to your computer. See the *VMware Validated Design Planning and Preparation* documentation or [VMware Knowledge Base article 2146215](#).

### Procedure

- 1 Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
- 2 On the Get Started page, click **New Installation**.
- 3 On the Getting Started page, review the steps for creating a cluster, and click **Next**.
- 4 On the Set Administrator Password page, type and confirm the password for admin user account, and click **Next**.

- 5 On the Choose Certificate page, click the **Install a certificate** button, click **Browse**, select the certificate chain .pem file that contains the private key and the issuer and certificate files, and click **Next**.

You generate a PEM file `vrops-for-1-pod.2.chain.pem` by using the CertGenVVD tool.

After the setup imports and validates the certificate, notice that the certificate has a common name, `vrops01svr01.rainpole.local`, and a subject alternative name that contains `vrops01svr01a.rainpole.local` for the master node.

- 6 On the Deployment Settings page, configure the following settings, and click **Next**.

| Setting                         | Value                                 |
|---------------------------------|---------------------------------------|
| <b>Cluster Master Node Name</b> | <code>vrops01svr01a</code>            |
| <b>NTP Server Address</b>       | <code>ntp.sfo01.rainpole.local</code> |

- 7 On the Ready To Complete page, click **Finish**.

After the configuration process completes, the vRealize Operations Manager Administration console opens.

- 8 Click **System Status** in the Administration panel to verify that you have a vRealize Operations Manager instance created.

The virtual appliance instance acting as the master node appears in the Nodes in the vRealize Operations Manager Cluster list.

## Deploy the Remote Collector Virtual Appliance for Consolidated SDDC

After you deploy the master node in analytics cluster, use the vSphere Web Client to deploy the virtual appliance for the remote collector for the Consolidated SDDC. You deploy a remote collector to forward data from the vCenter Server instance to the analytics cluster .

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

| Setting          | Value                                    |
|------------------|------------------------------------------|
| <b>User name</b> | <code>administrator@vsphere.local</code> |
| <b>Password</b>  | <code>vsphere_admin_password</code>      |

- 2 Navigate to the `sfo01w01vc01.sfo01.rainpole.local` vCenter Server object.
- 3 Right-click the `sfo01w01vc01.sfo01.rainpole.local` object and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, browse to the location of the vRealize Operations Manager OVA file on your file system, and click **Next**.
- 5 On the Select name and location page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

| Setting               | Value                                          |
|-----------------------|------------------------------------------------|
| <b>Name</b>           | <code>sfo01vropsc01a</code>                    |
| <b>vCenter Server</b> | <code>sfo01w01vc01.sfo01.rainpole.local</code> |
| <b>Data center</b>    | <code>sfo01-w01dc</code>                       |
| <b>Folder</b>         | <code>sfo01-w01fd-vropsrc</code>               |

- 6 On the Select a resource page, select the following values, and click **Next**.

| Setting           | Value                    |
|-------------------|--------------------------|
| <b>Datacenter</b> | sfo01-w01dc              |
| <b>Cluster</b>    | sfo01-w01-consolidated01 |

- 7 On the Review details page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the Accept license agreements page, accept the end user license agreements and click **Next**.
- 9 On the Select configuration page, from the **Configuration** drop-down menu, select the **Remote Collector (Standard)** deployment configuration of the virtual appliance, and click **Next**.
- 10 On the Select storage page, select the datastore indicated in the table below, and click **Next**.

| Setting                           | Value                       |
|-----------------------------------|-----------------------------|
| <b>Select virtual disk format</b> | Thin provision              |
| <b>VM Storage Policy</b>          | vSAN Default Storage Policy |
| <b>Datastore table</b>            | sfo01-w01-vsan01            |

- 11 On the Select networks page, select the distributed port group that ends with **Mgmt-RegionA01-VXLAN** on the sfo01-w01-vds01 Distributed Switch and click **Next**.
- 12 On the Customize template page, set the IPv4 settings and select the time zone for the virtual appliance and click **Next**.
- a In the Networking Properties section, configure the following IPv4 settings.

| Option                     | Description   |
|----------------------------|---------------|
| <b>DNS server</b>          | 172.16.11.5   |
| <b>Default gateway</b>     | 192.168.31.1  |
| <b>Static IPv4 address</b> | 192.168.31.31 |
| <b>Subnet mask</b>         | 255.255.255.0 |

- b From the **Timezone setting** drop-down menu, select the **Etc/UTC** time zone.
- 13 On the Ready to complete page, verify that the settings for deployment are correct, and click **Finish**.
- 14 After the virtual appliance is deployed, right-click the virtual appliance object and select **Power > Power On**.
- 15 Change the default empty password for the root user.
- a In the vSphere Web Client, right-click the remote collector virtual appliance and select **Open Console** to open the remote console to the appliance.

| Name                 | Role             |
|----------------------|------------------|
| <b>sfo01vrosc01a</b> | Remote collector |

- b Press ALT+F1 to switch to the command prompt.
- c At the command prompt, log in as the **root** user using empty password.
- d At the command prompt, change the default empty password for the root user account with a new **vrosc\_root\_password** password.
- e Close the virtual appliance console.



## Connect the Remote Collector Node to the Analytics Cluster for Consolidated SDDC

After you deploy the virtual appliance for the remote collector node, configure the settings of the remote collector and connect it to the analytics cluster.

### Procedure

- 1 Open a Web browser, and go to the initial setup user interface of the remote collector node virtual appliance.

| Remote Collector Node | URL for Setup Interface                     |
|-----------------------|---------------------------------------------|
| Remote collector      | https://sfo01vropsc01a.sfo01.rainpole.local |

- 2 On the Get Started page, click **Expand an Existing Installation**.
- 3 On the Getting Started page, review the steps for expanding existing cluster, and click **Next**.
- 4 On the Node Settings and Cluster Info page, configure the settings of the remote collector node.
  - a Enter a node name, select a node type, and enter master node address.

| Setting                        | Value                        |
|--------------------------------|------------------------------|
| Node name                      | sfo01vropsc01a               |
| Node type                      | Remote Collector             |
| Master node IP address or FQDN | vrops01svr01a.rainpole.local |

- b Click **Validate** next to the **Master node IP address or FQDN** text box.  
The certificate of the master node appears in the text box.
  - c Validate that the master certificate is correct, and click **Accept this certificate**.
  - d Click **Next**.
- 5 On the Username and Password page, select **Use cluster administrator user name and password**, enter the **vrops\_admin\_password** password for the admin user, and click **Next**.
- 6 On the Ready to Complete page, click **Finish**.

After configuration of the remote collector is complete, the cluster on the System Status page of the administration user interface consists of the following nodes: vrops01svr01a and the remote collector sfo01vropsc01a.

## Start vRealize Operations Manager for Consolidated SDDC

After you deploy the virtual appliances for the analytics cluster node and for the remote collector node, start the analytics cluster.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration interface.
  - a Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | admin                       |
| Password  | <i>vrops_admin_password</i> |

On the System Status page, the cluster status is **Not Started**, and the high availability of the cluster is **Disabled**.

- 2 Click **Start vRealize Operations Manager**.
- 3 In the Confirm First Application Startup dialog box, click **Yes** to confirm the startup of vRealize Operations Manager.

After several minutes the cluster starts. The analytics cluster and remote collector nodes are online. You are logged out from the administrator interface of the master node.

## Assign a License to vRealize Operations Manager for Consolidated SDDC

After you deploy and start vRealize Operations Manager, you assign a valid license.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration interface.
  - a Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | admin                       |
| Password  | <i>vrops_admin_password</i> |

- 2 On the Welcome page of the vRealize Operations Manager Configuration wizard, examine the process overview, and click **Next**.
- 3 On the Accept EULA page, accept the end user license agreement, and click **Next**.
- 4 On the Enter Product License Key page, enter the vRealize Operations Manager product license key.
  - a Select **Product Key** and enter the license key.
  - b Click **Validate License Key**, and click **Next**.
- 5 On the Customer Experience Improvement Program page, to send technical information for product improvement, select **Join the VMware Customer Experience Improvement Program** and click **Next**.
- 6 On the Ready to Complete page, click **Finish**.

The vRealize Operations Manager user interface opens.

## Group Remote Collector Nodes for Consolidated SDDC

After you start vRealize Operations Manager and assign it a license, join the remote collector node into a collector group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

### Procedure

- 1 Log in to vRealize Operations Manager by using the administration interface.
  - a Open a Web browser and go to **https://vrops01svr01a.rainpole.local**.
  - b Log in using the following credentials.

| Setting          | Value                       |
|------------------|-----------------------------|
| <b>User name</b> | admin                       |
| <b>Password</b>  | <i>vrops_admin_password</i> |

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, expand **Management**, click **Collector Groups**, and click **Add**.
- 4 On the Collector Groups page, click **Add**.
- 5 In the Add New Collector Group dialog box, configure the following settings, and click **Save**.

| Setting               | Value                            |
|-----------------------|----------------------------------|
| <b>Name</b>           | sfo01-remote-collectors          |
| <b>Description</b>    | Remote collector group for sfo01 |
| <b>sfo01vropsc01a</b> | Selected                         |

The sfo01-remote-collectors group appears on the Collector Groups page under the Administration view of the user interface.

## Configure the Load Balancer for vRealize Operations Manager for Consolidated SDDC

Configure load balancing for the analytics cluster on the dedicated sfo01w01lb01 NSX Edge services gateway. The remote collector group does not require load balancing.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting          | Value                         |
|------------------|-------------------------------|
| <b>User name</b> | administrator@vsphere.local   |
| <b>Password</b>  | <i>vsphere_admin_password</i> |

- 2 From the **Home** menu, select **Networking & Security**.

The vSphere Web Client displays the NSX Home page.

- 3 On the NSX Home page, click **NSX Edges** and select **172.16.11.66** from the **NSX Manager** drop-down menu at the top of the NSX Edges page.
- 4 On the NSX Edges page, double-click the **sfo01w01lb01** NSX edge.
- 5 Configure the load balancing VIP address for analytics cluster.
  - a On the **Manage** tab, click the **Settings** tab and click **Interfaces**.
  - b Select the **OneArmLB** interface and click the **Edit** icon.
  - c In the Edit NSX Edge Interface dialog box, click the **Edit** icon and in the **Secondary IP Addresses** text box enter the **192.168.11.35** VIP address.
  - d Click **OK** to save the configuration.
- 6 Create an application profile.
  - a On the **Manage** tab for the sfo01w01lb01 device, click the **Load Balancer** tab.
  - b Click **Application Profiles**, and click the **Add** icon.
  - c In the New Profile dialog box, configure the profile using the following configuration settings, and click **OK**.

| Setting                       | Value       |
|-------------------------------|-------------|
| <b>Name</b>                   | vrops-https |
| <b>Type</b>                   | HTTPS       |
| <b>Enable SSL Passthrough</b> | Selected    |
| <b>Persistence</b>            | Source IP   |
| <b>Expires in (Seconds)</b>   | 1800        |
| <b>Client Authentication</b>  | Ignore      |

- 7 Create a service monitoring entry.
  - a On the **Load Balancer** tab for the of the sfo01w01lb01 device, click **Service Monitoring** and click the **Add** icon.
  - b In the New Service Monitor dialog box, configure the health check parameters using the following configuration settings, and click **OK**.

| Setting            | Value                                 |
|--------------------|---------------------------------------|
| <b>Name</b>        | vrops-443-monitor                     |
| <b>Interval</b>    | 3                                     |
| <b>Timeout</b>     | 5                                     |
| <b>Max Retries</b> | 2                                     |
| <b>Type</b>        | HTTPS                                 |
| <b>Method</b>      | GET                                   |
| <b>URL</b>         | /suite-api/api/deployment/node/status |
| <b>Receive</b>     | ONLINE (must be upper case)           |

## 8 Add a server pool.

- a On the **Load Balancer** tab of the sfo01w01lb01 device, select **Pools**, and click the **Add** icon.
- b In the New Pool dialog box, configure the load balancing profile using the following configuration settings.

| Setting          | Value             |
|------------------|-------------------|
| <b>Name</b>      | vrops-svr-443     |
| <b>Algorithm</b> | LEASTCONN         |
| <b>Monitors</b>  | vrops-443-monitor |

- c Under **Members**, click the **Add** icon to add the pool members.
- d In the New Member dialog box, add one member for each node of the analytics cluster and click **OK**.

| Setting                | Value         |
|------------------------|---------------|
| <b>Name</b>            | vrops01svr01a |
| <b>IP Address</b>      | 192.168.11.31 |
| <b>State</b>           | Enable        |
| <b>Port</b>            | 443           |
| <b>Monitor Port</b>    | 443           |
| <b>Weight</b>          | 1             |
| <b>Max Connections</b> | 8             |
| <b>Min Connections</b> | 8             |

- e In the New Pool dialog box, click **OK**.

## 9 Add a virtual server.

- a On the **Load Balancer** tab of the sfo01w01lb01 device, select **Virtual Servers** and click the **Add** icon.
- b In the New Virtual Server dialog box, configure the settings of the virtual server for the analytics cluster and click **OK**.

| Setting                      | Value                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Virtual Server</b> | Selected                                                                                                                                                 |
| <b>Application Profile</b>   | vrops_https                                                                                                                                              |
| <b>Name</b>                  | vrops-svr-443                                                                                                                                            |
| <b>Description</b>           | vRealize Operations Manager Cluster                                                                                                                      |
| <b>IP Address</b>            | 192.168.11.35<br>Click <b>Select IP Address</b> , select <b>OneArmLB</b> from the drop-down menu and select <b>192.168.11.35</b> IP for the virtual NIC. |
| <b>Protocol</b>              | HTTPS                                                                                                                                                    |
| <b>Port</b>                  | 443                                                                                                                                                      |
| <b>Default Pool</b>          | vrops-svr-443                                                                                                                                            |
| <b>Connection Limit</b>      | 0                                                                                                                                                        |
| <b>Connection Rate Limit</b> | 0                                                                                                                                                        |

You can now connect to the analytics cluster using the public Virtual Server IP address over HTTPS at the **https://vrops01svr01.rainpole.local** address.

- 10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS without entering another URL in the browser.

- a On the **Load Balancer** tab of the sfo01w01lb01 device, select **Application Profiles** and click the **Add** icon.
- b In the New Profile dialog box, configure the application profile settings and click **OK**.

| Setting                     | Value                                                          |
|-----------------------------|----------------------------------------------------------------|
| <b>Name</b>                 | vrops-http-redirect                                            |
| <b>Type</b>                 | HTTP                                                           |
| <b>HTTP Redirect URL</b>    | https://vrops01svr01.rainpole.local/vcops-web-ent/login.action |
| <b>Persistence</b>          | Source IP                                                      |
| <b>Expires in (Seconds)</b> | 1800                                                           |

- c On the **Load Balancer** tab of the sfo01w01lb01 device, select **Virtual Servers** and click the **Add** icon.
- d Configure the settings of the virtual server for HTTP redirects.

| Setting                      | Value                 |
|------------------------------|-----------------------|
| <b>Enable Virtual Server</b> | Selected              |
| <b>Application Profile</b>   | vrops-http-redirect   |
| <b>Name</b>                  | vrops-svr-80-redirect |
| <b>IP Address</b>            | 192.168.11.35         |
| <b>Protocol</b>              | HTTP                  |
| <b>Port</b>                  | 80                    |
| <b>Default Pool</b>          | NONE                  |
| <b>Connection Limit</b>      | 0                     |
| <b>Connection Rate Limit</b> | 0                     |

You can connect to the analytics cluster at the public Virtual Server IP address over HTTP at the **http://vrops01svr01.rainpole.local** address.

- 11 Verify the pool configuration by examining the pool statistics that reflect the status of the components behind the load balancer.
  - a Log out and log in again to the vSphere Web Client.
  - b From the **Home** menu, select **Networking & Security**.
  - c On the NSX Home page, click **NSX Edges** and select **172.16.11.66** from the **NSX Manager** drop-down menu at the top of the NSX Edges page.
  - d On the NSX Edges page, double-click the **sfo01w01lb01** NSX edge.
  - e On the **Manage** tab, click the **Load Balancer** tab.
  - f Select **Pools** and click **Show Pool Statistics**.
  - g In the Pool and Member Status dialog box, select the **vrops-svr-443** pool.
  - h Verify that the load balancer pool is up.

## Add an Authentication Source for the Active Directory for Consolidated SDDC

Connect vRealize Operations Manager to the Active Directory of the Consolidated SDDC for central user management and access control.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | admin                       |
| Password  | <i>vrops_admin_password</i> |

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Access** and click **Authentication Sources**.
- 4 On the Authentication Sources page, click the **Add** button.
- 5 In the Add Source for User and Group Import dialog box, enter the settings for the rainpole.local and sfo01.rainpole.local Active Directories, and click **OK**.

| Active Directory Settings                                       | rainpole.local Value      | sfo01.rainpole.local Value    |
|-----------------------------------------------------------------|---------------------------|-------------------------------|
| Source Display Name                                             | RAINPOLE.LOCAL            | SFO01.RAINPOLE.LOCAL          |
| Source Type                                                     | Active Directory          | Active Directory              |
| Integration Mode                                                | Basic                     | Basic                         |
| Domain/Subdomain                                                | RAINPOLE.LOCAL            | SFO01.RAINPOLE.LOCAL          |
| Use SSL/TLS                                                     | Deselected                | Deselected                    |
| User Name                                                       | svc-vrops@rainpole.local  | svc-vrops@rainpole.local      |
| Password                                                        | <i>svc-vrops_password</i> | <i>svc-vrops_password</i>     |
| Settings under the Details section                              |                           |                               |
| Automatically synchronize user membership for configured groups | Selected                  | Selected                      |
| Host                                                            | dc01rpl.rainpole.local    | dc01sfo.sfo01.rainpole.local  |
| Port                                                            | 3268                      | 389                           |
| Base DN                                                         | dc=RAINPOLE,dc=LOCAL      | dc=SFO01,dc=RAINPOLE,dc=LOCAL |
| Common Name                                                     | userPrincipalName         | userPrincipalName             |

- 6 Click the **Test** button to test the connection to the domain controller and in the Info dialog click **OK**.
- 7 In the Add Source for User and Group Import dialog box, click **OK**.

The users and user groups in the two Active Directories rainpole.local and sfo01.rainpole.local are added to vRealize Operations Manager.

## Configure User Access in vSphere for Integration with vRealize Operations Manager for Consolidated SDDC

Configure operations service accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the consolidated cluster.

You associate the `svc-vrops-xxx` service accounts in Active Directory with user roles that have certain privileges and you assign the users to the vCenter Server instance in the inventory.

### Procedure

- 1 [Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for Consolidated SDDC](#) on page 196

In vSphere, create a user role with privileges that are required for collecting data about storage devices and vSAN health in vRealize Operations Manager.

- 2 [Configure User Privileges in vSphere for Integration with vRealize Operations Manager for Consolidated SDDC](#) on page 197

Assign global permissions in consolidated SDDC to the operations service accounts in order to enable vRealize Operations Manager access to monitoring data on the consolidated pod for the region.

### Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for Consolidated SDDC

In vSphere, create a user role with privileges that are required for collecting data about storage devices and vSAN health in vRealize Operations Manager.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

| Setting   | Value                         |
|-----------|-------------------------------|
| User name | administrator@vsphere.local   |
| Password  | <i>vsphere_admin_password</i> |

- 2 On the Home page of the vSphere Web Client, click **Roles** under Administration.
- 3 Create a new role for collecting storage device data.
  - a On the Roles page, click the **Create role action** icon.
  - b In the Create Role dialog box, configure the role using the following configuration settings, and click **OK**.

| Setting   | Value                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role name | MPSD Metrics User                                                                                                                                                                                                                      |
| Privilege | <ul style="list-style-type: none"> <li>■ Host.CIM.CIM interaction</li> <li>■ Host.Configuration.Storage partition configuration</li> <li>■ Profile-driven storage.Profile-driven storage view</li> <li>■ Storage views.View</li> </ul> |

This role inherits the **System.Anonymous**, **System.View**, and **System.Read** privileges.



## Configure User Privileges in vSphere for Integration with vRealize Operations Manager for Consolidated SDDC

Assign global permissions in consolidated SDDC to the operations service accounts in order to enable vRealize Operations Manager access to monitoring data on the consolidated pod for the region.

The svc-vrops-vsphere and svc-vrops-nsx users have read-only access on all objects in vCenter Server. The svc-vrops-mpsd and svc-vrops-vsan users have rights that are specifically required for access to storage device and vSAN information, respectively, in vRealize Operations Manager on all objects in vCenter Server.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password  | vsphere_admin_password      |

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the following users according to their roles.

| User                             | Role              |
|----------------------------------|-------------------|
| svc-vrops-vsphere@rainpole.local | Read-only         |
| svc-vrops-nsx@rainpole.local     | Read-only         |
| svc-vrops-mpsd@rainpole.local    | MPSD Metrics User |
| svc-vrops-vsan@rainpole.local    | MPSD Metrics User |

- a Click **Global Permissions** under **Access Control**.
- b Click **Add permission** in the **Manage** tab .
- c In the Global Permissions Root - Add Permission dialog box, click **Add** to associate a user or a group with a role.
- d In the Select Users/Groups dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc-vrops** and press Enter.
- e From the list of users and groups, select **svc-vrops-vsphere**, click **Add**, and click **OK**.
- f In the Global Permissions Root - Add Permission dialog box, from the **Assigned Role** drop-down menu, select **Read-only**, ensure that **Propagate to children** is selected, and click **OK**.
- g Repeat the steps to assign the Read-only user role to the svc-vrops-nsx user, and the MPSD Metrics User user role to the svc-vrops-mpsd and svc-vrops-vsan users.

## Add vCenter Adapter Instance to vRealize Operations Manager for Consolidated SDDC

After you deploy the analytics cluster and the remote collector node of vRealize Operations Manager and start vRealize Operations Manager, add vCenter Adapter for the Consolidated vCenter Server.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | admin                       |
| Password  | <i>vrops_admin_password</i> |

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the Solutions page, select the **VMware vSphere** solution, and click **Configure**.

The Manage Solution - VMware vSphere dialog box appears.

- 5 Under Instance Settings, enter the settings for connection to the Consolidated vCenter Server.
  - a Enter the display name, description, and FQDN of the Consolidated vCenter Server.

| Setting        | Value for Consolidated vCenter Server |
|----------------|---------------------------------------|
| Display Name   | vCenter Adapter - sfo01w01vc01        |
| Description    | Consolidated vCenter Server           |
| vCenter Server | sfo01w01vc01.sfo01.rainpole.local     |

- b Click the **Add** icon on the right side, configure the credentials for connection to the Consolidated vCenter Server instance, and click **OK**.

| vCenter Server Credentials |                                            |
|----------------------------|--------------------------------------------|
| Attribute                  | Value                                      |
| Credential name            | vCenter Adapter Credentials - sfo01w01vc01 |
| User Name                  | svc-vrops-vsphere@rainpole.local           |
| Password                   | <i>svc-vrops-vsphere-password</i>          |

- c Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in vCenter Server from vRealize Operations Manager.
  - d Click **Test Connection** to validate the connection to the vCenter Server instance.  
The vCenter Server certificate appears.
  - e In the Review and Accept Certificate dialog box, verify the certificate information, and click **Accept**.
  - f Click **OK** in the Info dialog box.
  - g Expand the **Advanced Settings** section of settings.

- h From the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** group.
- i Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server.

| Setting               | Value                         |
|-----------------------|-------------------------------|
| Registration user     | administrator@vsphere.local   |
| Registration password | <i>vsphere_admin_password</i> |

- 6 Click **Define Monitoring Goals**.
- 7 In the Define Monitoring Goals dialog box, under **Enable vSphere Hardening Guide Alerts?**, select **Yes**, leave the default configuration for the other options, and click **Save**.
- 8 Click **OK** in the Success dialog box.
- 9 Click **Save Settings**.
- 10 In the Info dialog box, click **OK**.
- 11 In the Manage Solution - VMware vSphere dialog box, click **Close**.
- 12 On the Solutions page, select **VMware vSphere** from the solution table to view the collection state and collection status of the adapter.

The **Collection State** column for the vCenter Adapters displays **Collecting**, and the **Collection Status** column displays **Data receiving**.

## Connect vRealize Operations Manager to the NSX Manager for Consolidated SDDC

Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the vSphere cluster and view the vSphere hosts in the NSX transport zones. You can also access end to end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.

### Procedure

- 1 [Install the vRealize Operations Manager Management Pack for NSX for vSphere for Consolidated SDDC](#) on page 200  
Install the .pak file for the management pack for NSX for vSphere to add the solution entry and adapter to vRealize Operations Manager.
- 2 [Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Consolidated SDDC](#) on page 200  
Assign the permissions that are required to access monitoring data from the Consolidated NSX Manager in vRealize Operations Manager for the service account svc-vrops-nsx.
- 3 [Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Consolidated SDDC](#) on page 202  
After you install the management pack, configure NSX-vSphere Adapter for the NSX Manager in the consolidated cluster.
- 4 [Add Network Devices Adapter to vRealize Operations Manager for Consolidated SDDC](#) on page 203  
Configure a Network Devices Adapter to monitor the switches and routers in your environment, and view related alerts, metrics and object capacity.

## Install the vRealize Operations Manager Management Pack for NSX for vSphere for Consolidated SDDC

Install the .pak file for the management pack for NSX for vSphere to add the solution entry and adapter to vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

| Setting   | Value                       |
|-----------|-----------------------------|
| User name | admin                       |
| Password  | <i>vrops_admin_password</i> |

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, click the **Add** icon.
- 5 On the Select Solution page from the Add Solution wizard, browse to the .pak file of the vRealize Operations Manager Management Pack for NSX for vSphere and click **Upload**.

After the NSX management pack file has been uploaded, you see details about the management pack.

- 6 After the upload is complete, click **Next**.
- 7 On the End User License Agreement page, accept the license agreement and click **Next**.  
The installation of the management pack starts. You see its progress on the Install page.
- 8 After the installation is complete, click **Finish** on the Install page.

The Management Pack for NSX-vSphere solution appears on the Solutions page of the vRealize Operations Manager user interface.

## Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Consolidated SDDC

Assign the permissions that are required to access monitoring data from the Consolidated NSX Manager in vRealize Operations Manager for the service account svc-vrops-nsx.

### Procedure

- 1 Log in to the NSX Manager by using a Secure Shell (SSH) client.
  - a Open an SSH connection to the NSX Manager virtual machine.

| NSX Manager                              | Host name                          |
|------------------------------------------|------------------------------------|
| NSX Manager for the consolidated cluster | sfo01w01nsx01.sfo01.rainpole.local |

- b Log in using the following credentials.

| Setting   | Value                          |
|-----------|--------------------------------|
| User name | admin                          |
| Password  | <i>sfo01nsx_admin_password</i> |

- 2 Create the local service account `svc-vrops-nsx` on the NSX Manager instance.
  - a Run the following command to switch to Privileged mode of the NSX Manager.  
`enable`
  - b Enter the admin password when prompted and press Enter.
  - c Switch to Configuration mode.  
`configure terminal`
  - d Create the service account `svc-vrops-nsx`.  
`user svc-vrops-nsx password plaintext svc-vrops-nsx_password`
  - e Assign the `svc-vrops-nsx` user access to NSX Manager from the vSphere Web Client.  
`user svc-vrops-nsx privilege web-interface`
  - f Exit Configuration mode  
`exit`
  - g Commit these updates to the NSX Manager.  
`copy running-config startup-config`

- 3 Assign the `security_admin` role to the `svc-vrops-nsx` service account.
  - a Log in to the Windows host that has access to your data center.
  - b In a Chrome Web browser, start the Postman application and log in.
  - c Select **POST** from the drop-down menu that contains the HTTP request methods.
  - d In the URL text box next to the selected method, enter the following URL.

| NSX Manager                     | POST URL                                                                                                        |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Consolidated NSX Manager</b> | <code>https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true</code> |

- e On the Authorization tab, configure the following authorization settings and click **Update Request**.

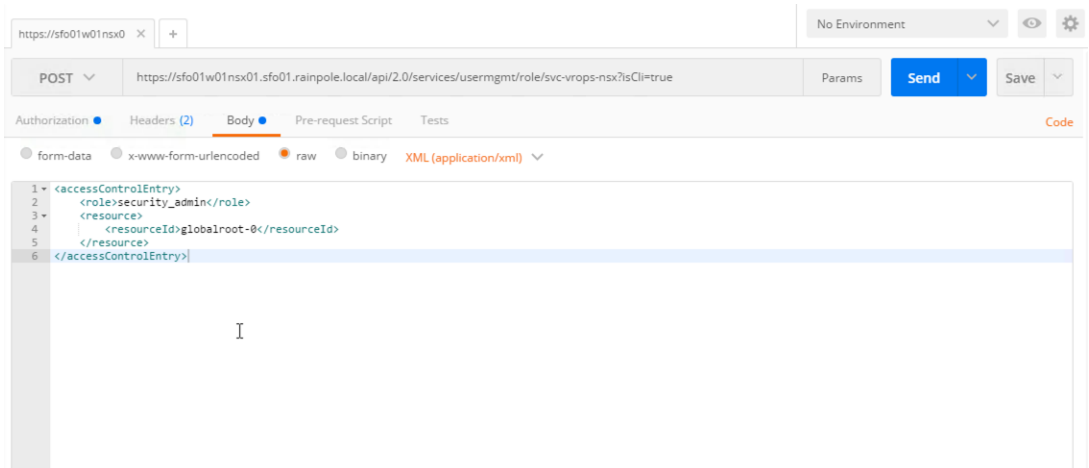
| Setting   | Value                                |
|-----------|--------------------------------------|
| Type      | Basic Auth                           |
| User name | admin                                |
| Password  | <code>sfo01nsx_admin_password</code> |

- f On the Headers tab, enter the following header details.

| Setting | Value           |
|---------|-----------------|
| Key     | Content-Type    |
| Value   | application/xml |

- g On the Body tab, select **raw**, paste the following request body in the **Body** text box, and click **Send**.

```
<accessControlEntry>
 <role>security_admin</role>
 <resource>
 <resourceId>globalroot-0</resourceId>
 </resource>
</accessControlEntry>
```



The Status changes to 204 No Content.

## Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Consolidated SDDC

After you install the management pack, configure NSX-vSphere Adapter for the NSX Manager in the consolidated cluster.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, select **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.

- 5 In the Manage Solution - Management Pack for NSX-vSphere dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

Empty settings for the NSX-vSphere Adapter appear under **Instance Settings** if vRealize Operations Manager does not have NSX-vSphere Adapters configured.

- 6 Under Instance Settings, enter the settings for connection to the NSX Manager in the consolidated cluster.
  - a Enter the display name, the FQDN of NSX Manager, and the FQDN of the vCenter Server instance that is connected to the NSX Manager.

Setting	Value for the NSX Manager in the Consolidated Cluster
Display Name	NSX Adapter - sfo01w01nsx01
Description	Consolidated NSX Manager
NSX Manager Host	sfo01w01nsx01.sfo01.rainpole.local
VC Host	sfo01w01vc01.sfo01.rainpole.local
Enable Log Insight integration if configured	false

- b Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to NSX Manager and vCenter Server, and click **OK**.

Setting	Value for the NSX Manager for the Consolidated Cluster
Credential name	NSX Adapter Credentials - sfo01w01nsx01
NSX Manager User Name	svc-vrops-nsx
NSX Manager Password	<i>svc-vrops-nsx_password</i>
vCenter User Name	svc-vrops-nsx@rainpole.local
vCenter Password	<i>svc-vrops-nsx-password</i>

- c Click **Test Connection** to validate the connection to the Consolidated NSX Manager.  
The NSX Manager certificate appears.
    - d In the Review and Accept Certificate dialog box, verify the certificate information and click **Accept**.
    - e In the Info dialog, click **OK**.
    - f Expand the Advanced Settings pane, select **sfo01-remote-collectors** from the **Collectors/Groups** drop-down menu .
    - g Click **Save Settings**.
    - h In the Info dialog, click **OK**.
- 7 In the Manage Solution - Management Pack for NSX-vSphere dialog box, click **Close**.

The NSX-vSphere Adapter is available on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is Collecting and the **Collection Status** is Data receiving.

## Add Network Devices Adapter to vRealize Operations Manager for Consolidated SDDC

Configure a Network Devices Adapter to monitor the switches and routers in your environment, and view related alerts, metrics and object capacity.

The Network Devices Adapter collects data across all network devices that you want to monitor using vRealize Operations Manager.

## Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, select the **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.
- 5 In Manage Solution - Management Pack for NSX-vSphere dialog box, from the **Adapter Type** table at the top, select **Network Devices Adapter**.
- 6 Under **Instance Settings**, enter the settings for SNMP connection to the network devices for the management cluster.
  - a Enter the display name, SNMP version and credentials.

Setting	Value
Display Name	Network Devices Adapter
Description	Global Network Devices Adapter
SNMP Ports	161
SNMP Version	SNMPv2
SNMPv3 Privacy Protocol	AES
SNMPv3 Authentication Protocol	MD5

- b Click the **Add** icon, and configure the credentials for connecting the Network Devices Adapter to the network devices, and click **OK**.

Credential	Value
Credential Kind	SNMPv1, SNMPv2 Credential
Credential Name	Network Devices Adapter Credentials - sfo01
SNMP Read Community Strings	public

**NOTE** For SNMPv1 and SNMPv2 devices, enter a comma-separated list of community names (default is public).

For SNMPv3 devices, provide SNMPv3 credentials in addition to the settings for SNMPv1 and SNMPv2.

- c Click **Test Connection** to verify the settings, and if the test is successful click the **OK** button.
  - d Expand the **Advanced Settings** section of settings, and verify that the **Collectors/Groups** option is set to **Default collector group**.
  - e Click **Save Settings**.
  - f Click **OK** in the Info dialog box that appears.
- 7 In the Manage Solution - Management Pack for NSX-vSphere dialog box, click **Close**.



The Network Devices Adapter appears on the Solutions page of the vRealize Operations Manager user interface. The adapter is collecting data about the network devices for the local region of the SDDC. The **Collection State** of the adapter is Collecting and the **Collection Status** is Data receiving.

## Connect vRealize Operations Manager to vRealize Automation for Consolidated SDDC

Configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

### Procedure

- 1 [Configure Collection of Metrics from vRealize Automation in vRealize Operations Manager for Consolidated SDDC](#) on page 205  
Connect vRealize Automation to vRealize Operations Manager for collecting statistics about the tenant workloads that are provisioned using vRealize Automation.
- 2 [Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation for Consolidated SDDC](#) on page 208  
Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation in the consolidated SDDC. Such workloads have low use of CPU, memory use, or disk space.

## Configure Collection of Metrics from vRealize Automation in vRealize Operations Manager for Consolidated SDDC

Connect vRealize Automation to vRealize Operations Manager for collecting statistics about the tenant workloads that are provisioned using vRealize Automation.

### Procedure

- 1 [Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager for Consolidated SDDC](#) on page 206  
Assign the permissions that are required to access monitoring data from the vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account. The svc-vrops-vra user has rights that are specifically required for access to vRealize Automation in vRealize Operations Manager.
- 2 [Add vRealize Automation Adapter to vRealize Operations Manager for Consolidated SDDC](#) on page 207  
Configure a vRealize Automation adapter to collect monitoring data from vRealize Automation.

## Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager for Consolidated SDDC

Assign the permissions that are required to access monitoring data from the vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account. The svc-vrops-vra user has rights that are specifically required for access to vRealize Automation in vRealize Operations Manager.

### Procedure

- 1 Log in to the vRealize Automation portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator
Password	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** tab, click the **Rainpole** tenant.
- 3 Click the **Administrators** tab to assign tenant administrator and IaaS administrator roles to the svc-vrops-vra service account.
  - a Enter **svc-vrops-vra** in the **Tenant administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that shows in the search result list to assign the role to the account.
  - b Enter **svc-vrops-vra** in the **IaaS administrators** search text box, click **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that shows in the search result list to assign the role to the account.
  - c Click **Finish**.
- 4 Log out of the vRealize Automation Default tenant portal.
- 5 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	Rainpole.local

- 6 Navigate to **Administration > Users & Groups > Directory Users and Groups** to assign the software architect role to the svc-vrops-vra service account.
  - a Enter **svc-vrops-vra** in the search box, click the **Search** icon and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user.
  - b The setting of the svc-vrops-vra account appear.
  - c On the **General** tab, select **Infrastructure Architect** and **Software Architect** under Add roles to this User, and click **Finish**.

- 7 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.
  - a On the Fabric Groups page, click **SFO Fabric Group**.
  - b On Edit Fabric Group page, enter **svc-vrops-vra** in **Fabric administrators** search text box and click the **Search** icon.
  - c Click **svc-vrops-vra@rainpole.local** in the search result list to assign the fabric administrator role to the account, and click **OK**.

### Add vRealize Automation Adapter to vRealize Operations Manager for Consolidated SDDC

Configure a vRealize Automation adapter to collect monitoring data from vRealize Automation.

#### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the Solutions page, select **VMware vRealize Automation** and click **Configure**.

The Manage Solution - VMware vRealize Automation dialog box appears.

- 5 In the Manage Solution - VMware vRealize Automation dialog box, under **Instance Settings**, enter the settings for connection to vRealize Automation.
  - a Enter the display name, description, and the FQDN of vRealize Automation front-end portal, and turn data collection on for the Rainpole tenant.

Setting	Value
Display Name	vRealize Automation Adapter - vra01svr01 (Rainpole)
Description	vRealize Automation - Rainpole Tenant
vRealize Automation Appliance URL	https://vra01svr01.rainpole.local

- b Click the **Add** icon, configure the credentials for connection to vRealize Automation, and click **OK**.

Credential	Value
Credential name	vRA Adapter Credentials - vra01svr01
SysAdmin Username	administrator@vsphere.local
SysAdmin Password	vra_administrator_password
SuperUser Username	svc-vrops-vra@rainpole.local
SuperUser Password	svc_vrops_vra_password

- c Click **Test Connection** to validate the connection to vRealize Automation.

- d In the Review and Accept Certificate dialog box, verify the vRealize Automation certificate information, and click **Accept**.
- e Click **OK** in the Info dialog box.
- f Expand the Advanced Settings section, and verify the following configuration.

Advanced Setting	Value
Collectors/Groups	Default collector group
Tenants	rainpole
vRA Endpoint Monitoring	Enabled
Auto Discovery	true

- g Click **Save Settings** and click **OK** in the Info box that appears.
- 6 In the Manage Solution - VMware vRealize Automation dialog box, click **Close**.
- The **vRealize Automation Adapter** appears on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation for Consolidated SDDC

Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation in the consolidated SDDC. Such workloads have low use of CPU, memory use, or disk space.

### Procedure

- 1 [Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation for Consolidated SDDC](#) on page 208  
Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in the consolidated SDDC.
- 2 [Add vRealize Operations Manager as a Metrics Provider for vRealize Automation for Consolidated SDDC](#) on page 209  
Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

### Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation for Consolidated SDDC

Configure read-only privileges for the svc-vra-vrops@rainpole.local service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in the consolidated SDDC.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, expand **Access**, and click **Access Control**.
- 4 On the Access Control page, click the **User Accounts** tab and click the **Import Users** icon.
- 5 On the Import Users page, import the svc-vra-vrops@rainpole.local service account.
  - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
  - b Select the **Basic** option for the search query.
  - c In the **Search String** text box, enter **svc-vra-vrops** and click **Search**.  
The search results contain the svc-vra-vrops user account.
  - d Select **svc-vra-vrops@rainpole.local** and click **Next**.
- 6 On the Assign Groups and Permissions page, assign the ReadOnly role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	vCenter Adapter > vCenter Adapter - sfo01w01vc01

### Add vRealize Operations Manager as a Metrics Provider for vRealize Automation for Consolidated SDDC

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

#### Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	Rainpole.local

- 2 Navigate to **Administration > Reclamation > Metrics Provider**.
- 3 On the Metrics Provider page, configure the vRealize Operations Manager settings.
  - a Select **vRealize Operations Manager endpoint**.
  - b Configure the following settings for vRealize Operations Manager.

Setting	Value
URL	https://vrops01svr01.rainpole.local/suite-api/
Username	svc-vra-vrops@rainpole.local
Password	svc-vra-vrops_password

- c Click **Test Connection**, verify that the test connection is successful, and click **Save**.
- d In the certificate warning message box, click **OK**.

The vSphere metrics provider updated successfully message appears.

## Connect vRealize Operations Manager with vRealize Business for Consolidated SDDC

Configure the vRealize Operations Manager Management Pack for vRealize Business to view your infrastructure performance, cost information, and also troubleshooting tips. You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

### Connect vRealize Operations Manager to vRealize Business for Cloud for Consolidated SDDC

Configure a vRealize Business for Cloud adapter to collect monitoring data from vRealize Business for Cloud.

#### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
<b>User name</b>	admin
<b>Password</b>	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 From the solution table on the Solutions page, select **VMware vRealize Business for Cloud** solution and click **Configure**.

The Manage Solution - VMware vRealize Business for Cloud dialog box appears.

- 5 Under Instance Settings, enter the settings for connection to vRealize Business for Cloud.
  - a Enter the display name, description and FQDN of the vRealize Business for Cloud Server.

Setting	Value for vRealize Business for Cloud Server
<b>Display Name</b>	vRealize Business Adapter - vrb01svr01
<b>Description</b>	vRealize Business for Cloud Server
<b>vRealize Business for Cloud server</b>	vrb01svr01.rainpole.local

- b Click **Test Connection** to validate the connection to the vRealize Business server instance.
  - c Click **OK** in the Test Connection Info dialog box.
  - d Expand the **Advanced Settings** section of settings.
  - e From the **Collectors/Groups** drop-down menu, make sure that the **Default collectors group** is selected.
- 6 Click **Save Settings**.
- 7 Click **OK** in the Adapter Instance Information dialog box.

- 8 In the Manage Solution - VMware vRealize Business for Cloud dialog box, click **Close**.

The **vRBC Adapter** appears on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Verify Connectivity to vRealize Business for Cloud for Consolidated SDDC

To verify integration of VMware vRealize Business for Cloud with vRealize Operations Manager, run a Private Cloud Reclamation report from the vRealize Operations Manager operations interface. If the integration is interrupted, re-register the Consolidated vCenter Server with vRealize Business.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vroops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vroops_admin_password

- 2 On the main navigation bar, click **Home**.
- 3 In the left pane of vRealize Operations Manager, click **Business Management**.
- 4 Log in to vRealize Business using the following credentials.

Setting	Value
User name	itac-tenantadmin
Tenant	rainpole
Password	itac-tenantadmin_password

The dashboard of vRealize Business opens on the Business Management page of the vRealize Operations Manager operations interface.

- 5 On the Business Management page, click **Overview** and locate the Private Cloud Reclamation widget on the right.
- 6 If on running the report, the integration message **Cost Savings from Private Cloud reclamation requires integration with vRealize Operations Manager** appears, re-register vRealize Business with the vCenter Server.
  - a Open a Web browser and go to **https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	vrbc_collector_root_password

- c Click **Manage Private Cloud Connections** and select **vCenter Server**.
- d Select the vCenter Server **sfo01w01vc01.sfo01.rainpole.local** and click the **Delete** icon.  
The connection to vCenter Server is removed.
- e Click **Add**.

- f In the Add vCenter Server Connections dialog box, enter the following settings and click **Save**.

Setting	Value
<b>Name</b>	sfo01w01vc01.sfo01.rainpole.local
<b>vCenter Server</b>	sfo01w01vc01.sfo01.rainpole.local
<b>Username</b>	svc-vra@rainpole.local
<b>Password</b>	svc_vra_password

- g In the SSL Certificate dialog box, click **Install**.
- h In the Success dialog box, click **OK**.
- 7 Wait a few minutes for vRealize Business for Cloud to initiate a synchronization, run the report again and verify that it is generated successfully.

## Enable Storage Device Monitoring in vRealize Operations Manager for Consolidated SDDC

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology, and to monitor the capacity and problems on storage components.

### Procedure

- 1 [Install the vRealize Operations Manager Management Pack for Storage Devices for Consolidated SDDC](#) on page 212  
Install the .pak file of the management pack for storage devices to add the management pack as a solution to vRealize Operations Manager.
- 2 [Add Storage Devices Adapter in vRealize Operations Manager for Consolidated SDDC](#) on page 213  
After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices in the SDDC.

## Install the vRealize Operations Manager Management Pack for Storage Devices for Consolidated SDDC

Install the .pak file of the management pack for storage devices to add the management pack as a solution to vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
<b>User name</b>	admin
<b>Password</b>	vrops_admin_password

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, click the **Add** icon.
- 5 On the Select Solution page from the Add Solution wizard, browse to the .pak file of the vRealize Operations Manager Management Pack for Storage Devices and click **Upload**.
- 6 After the upload is complete, click **Next**.



- 7 On the End User License Agreement page, accept the license agreement and click **Next**.  
The installation of the management pack starts. You see its progress on the Install page.
- 8 After the installation is complete, click **Finish** on the Install page.

The Management Pack for Storage Devices solution appears on the Solutions page of the vRealize Operations Manager user interface.

## Add Storage Devices Adapter in vRealize Operations Manager for Consolidated SDDC

After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices in the SDDC.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, select **Management Pack for Storage Devices** from the solution table and click **Configure**.

The Manage Solution - Management Pack for Storage Devices dialog box appears.

- 5 Under Instance Settings, enter the settings for connection to the Consolidated vCenter Server.
  - a Enter the display name, description, and FQDN of the vCenter Server instance.

Setting	Value for the Consolidated vCenter
Display Name	Storage Devices Adapter - sfo01w01vc01
Description	Connection to Consolidated vCenter for Storage Devices
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
SNMP Community Strings	-

- b Click the **Add** icon, configure the credentials for connection to the Consolidated vCenter Server, and click **OK**.

Setting	Value for the Consolidated vCenter
Credential name	Storage Devices Adapter Credentials - sfo01w01vc01
User Name	svc-vrops-mpsd@rainpole.local
Password	<i>svc-vrops-mpsd-password</i>

- c Click **Test Connection** to validate the connection to the Consolidated vCenter Server.
  - d In the Review and Accept Certificate dialog box, verify the vCenter Server certificate information and click **Accept**.

- e Click **OK** in the Info dialog box.
  - f Expand the **Advanced Settings** section of settings, and from the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** collector group.
  - g Click **Save Settings** and click **OK** in the Info dialog box that appears.
- 6 In the Manage Solution - Management Pack for Storage Devices dialog box, click **Close**.

The Storage Devices Adapter appear on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Enable vSAN Monitoring in vRealize Operations Manager for Consolidated SDDC

Configure the vRealize Operations Management Pack for vSAN to view the vSAN topology and to monitor capacity and problems.

### Procedure

- 1 [Turn On the vSAN Performance Service for Consolidated SDDC](#) on page 214  
When you create a vSAN cluster, the performance service is disabled. Turn on the vSAN performance service to monitor the performance of vSAN clusters, hosts, disks, and VMs.
- 2 [Add a vSAN Adapter in vRealize Operations Manager for Consolidated SDDC](#) on page 215  
Configure the vSAN adapter to collect monitoring data about vSAN usage in the Consolidated SDDC.

### Turn On the vSAN Performance Service for Consolidated SDDC

When you create a vSAN cluster, the performance service is disabled. Turn on the vSAN performance service to monitor the performance of vSAN clusters, hosts, disks, and VMs.

When you turn on the performance service, vSAN places a Stats database object in the datastore to collect statistical data. The Stats database is a namespace object in the cluster's vSAN datastore.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Enable the vSAN performance service.
  - a In the Navigator, expand the **sfo01-w01dc** data center object.
  - b Click the **sfo01-w01-consolidated01** cluster object and click the **Configure** tab.
  - c Under vSAN, select **Health and Performance**.
  - d Next to the Performance Service settings, click **Edit**, configure the following settings and click **OK**.

Setting	Value
Turn ON vSAN performance service	Selected
Storage policy	vSAN Default Storage Policy

## Add a vSAN Adapter in vRealize Operations Manager for Consolidated SDDC

Configure the vSAN adapter to collect monitoring data about vSAN usage in the Consolidated SDDC.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
<b>User name</b>	admin
<b>Password</b>	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, select **VMware vSAN** from the solution table and click **Configure**.  
The Manage Solution - VMware vSAN dialog box appears.
- 5 Under Instance Settings, enter the settings for connection to the Consolidated vCenter Server.
  - a Enter the display name, description and FQDN of the vCenter Server instance.

Setting	Value for the Consolidated vCenter
<b>Display Name</b>	vSAN Adapter - sfo01w01vc01
<b>Description</b>	vSAN Adapter for Consolidated vCenter Server
<b>vCenter Server</b>	sfo01w01vc01.sfo01.rainpole.local

- b Click the **Add** icon, configure the credentials for connection to the Consolidated vCenter Server, and click **OK**.

Setting	Value for the Consolidated vCenter
<b>Credential name</b>	vSAN Adapter Credentials - sfo01w01vc01
<b>User Name</b>	svc-vrops-vsan@rainpole.local
<b>Password</b>	<i>svc-vrops-vsan-password</i>

- c Click **Test Connection** to validate the connection to the Consolidated vCenter Server.
  - d In the Review and Accept Certificate dialog box, verify the vCenter Server certificate information and click **Accept**.
  - e Click **OK** in the Info dialog box.
  - f Expand the **Advanced Settings** section of settings.
  - g From the **Collectors/Groups** drop-down menu, select the **sfo01-remote-collectors** collector group.
  - h Make sure **Auto Discovery** is set to **true**.
  - i Click **Save Settings** and click **OK** in the Info dialog box that appears.
- 6 In the Manage Solution - VMware vSAN dialog box, click **Close**.

The vSAN Adapter appears on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure E-Mail Alerts in vRealize Operations Manager for Consolidated SDDC

You configure e-mail notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Management** and click **Outbound Settings**.
- 4 On the Outbound Settings page, click the **Add** icon to create an outbound alert instance.
- 5 In the Add/Edit Outbound Instance dialog box, configure the settings for the Standard Email Plug-in, and click **OK**.

Alert Instance Setting	Value
Plugin Type	Standard Email Plugin
Instance Name	SMTP Alert Mail Relay
Use Secure Connection	Selected
SMTP Host	<i>mailserver.rainpole.local</i>
SMTP Port	25
Secure Connection Type	TLS
Sender Email Address	vrops@rainpole.com
Sender Name	vRealize Operations Admin

- 6 Click **Test** to verify the connection with the SMTP server and click **OK**.
- 7 Click **Save**.

## vRealize Log Insight Implementation for Consolidated SDDC

Deploy vRealize Log Insight in a single-node configuration consisting of a single master node with an integrated load balancer.

### Procedure

- 1 [Deploy vRealize Log Insight for Consolidated SDDC](#) on page 217  
Start the deployment of vRealize Log Insight in the Consolidated SDDC by deploying the master node and enabling the integrated load balancer.
- 2 [Replace the Certificate of vRealize Log Insight for Consolidated SDDC](#) on page 223  
After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight.

- 3 [Connect vRealize Log Insight to the vSphere Environment for Consolidated SDDC](#) on page 224  
Start collecting log information about the ESXi and vCenter Server instances in the Consolidated SDDC.
- 4 [Connect vRealize Log Insight to vRealize Operations Manager for Consolidated SDDC](#) on page 228  
Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications to troubleshoot vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.
- 5 [Connect vRealize Log Insight to the NSX Instances for Consolidated SDDC](#) on page 235  
Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.
- 6 [Connect vRealize Log Insight to vRealize Automation for Consolidated SDDC](#) on page 241  
Connect the vRealize Log Insight to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight user interface.
- 7 [Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Consolidated SDDC](#) on page 250  
Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances in vRealize Log Insight.
- 8 [Configure Log Retention and Archiving for Consolidated SDDC](#) on page 251  
Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

## Deploy vRealize Log Insight for Consolidated SDDC

Start the deployment of vRealize Log Insight in the Consolidated SDDC by deploying the master node and enabling the integrated load balancer.

### Procedure

- 1 [Prerequisites for Deploying vRealize Log Insight for Consolidated SDDC](#) on page 218  
Before you deploy vRealize Log Insight, verify that your environment satisfies the requirements for this deployment.
- 2 [Deploy the Virtual Appliance for the Maser Node of the vRealize Log Insight Cluster for Consolidated SDDC](#) on page 219  
Use the vSphere Web Client to deploy the vRealize Log Insight master node as a virtual appliance in the Consolidated SDDC.
- 3 [Start the vRealize Log Insight Instance for Consolidated SDDC](#) on page 221  
Configure and start the vRealize Log Insight master node.
- 4 [Enable the Integrated Load Balancer of vRealize Log Insight for Consolidated SDDC](#) on page 222  
After you create the vRealize Log Insight cluster, enable the Integrated Load Balancer (ILB) for balancing incoming ingestion traffic of syslog data and for high availability.
- 5 [Join vRealize Log Insight to the Active Directory for Consolidated SDDC](#) on page 222  
To use user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

## Prerequisites for Deploying vRealize Log Insight for Consolidated SDDC

Before you deploy vRealize Log Insight, verify that your environment satisfies the requirements for this deployment.

### IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the vRealize Log Insight are available in the application virtual network for the Consolidated SDDC.

For the application virtual network, allocate a static IP address for the vRealize Log Insight master node and another IP address for the integrated load balancer. Map host names to the IP addresses.

**NOTE** Consolidated SDDC must be routable via the vSphere management network.

**Table 4-5.** IP Addresses and Host Names for the vRealize Log Insight Instance in Consolidated SDDC

Role	IP Address	FQDN
Integrated load balancer VIP address	192.168.31.10	sfo01vrli01.sfo01.rainpole.local
Master node	192.168.31.11	sfo01vrli01a.sfo01.rainpole.local
Default gateway	192.168.31.1	-
DNS server	<ul style="list-style-type: none"> <li>■ 172.16.11.5</li> <li>■ 172.16.11.4</li> </ul>	-
Subnet mask	255.255.255.0	-
NTP servers	<ul style="list-style-type: none"> <li>■ 172.16.11.251</li> <li>■ 172.16.11.252</li> </ul>	ntp.sfo01.rainpole.local

### Deployment Prerequisites

Verify that your environment satisfies the following prerequisites to deploying vRealize Log Insight.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> <li>■ Virtual disk provisioning. <ul style="list-style-type: none"> <li>■ Thin</li> </ul> </li> <li>■ Required storage per node <ul style="list-style-type: none"> <li>■ Initial storage for node deployment: 510 GB</li> </ul> </li> </ul>
Software Features	<ul style="list-style-type: none"> <li>■ Verify that vCenter Server is operational.</li> <li>■ Verify that the vSphere cluster has DRS and HA enabled.</li> <li>■ Verify that the Consolidated NSX Manager is operational.</li> <li>■ Verify that vRealize Operations Manager is operational.</li> <li>■ Verify that the application virtual networks for the single-node vRealize Log Insight cluster are available.</li> <li>■ Verify that vRealize Automation is operational.</li> <li>■ Verify that vRealize Business for Cloud is operational.</li> <li>■ Verify that Postman REST API application is installed in your Chrome browser.</li> <li>■ Verify the following NFS datastore requirements: <ul style="list-style-type: none"> <li>■ Create an NFS share of 250 GB for the consolidated pod and export it as /V2D_VRLI_Consolidated_250GB.</li> <li>■ Verify that the NFS server supports NFS v3.</li> <li>■ Verify that the NFS partition allows read and write operations for guest accounts.</li> <li>■ Verify that the mount does not require authentication.</li> <li>■ Verify that the NFS share is directly accessible to vRealize Log Insight.</li> <li>■ If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).</li> </ul> </li> </ul>

Prerequisite	Value
Installation Package	Download the .ova file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.
License	Obtain a license that covers the use of vRealize Log Insight.
Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the <code>rainpole.local</code> domain.
Certification Authority	Configure the Active Directory domain controller as a certificate authority for the environment.
E-mail account	Provide an email account to send vRealize Log Insight notifications from.

■

## Deploy the Virtual Appliance for the Master Node of the vRealize Log Insight Cluster for Consolidated SDDC

Use the vSphere Web Client to deploy the vRealize Log Insight master node as a virtual appliance in the Consolidated SDDC.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 Navigate to the `sfo01w01vc01.sfo01.rainpole.local` vCenter Server object.
- 3 Right-click **`sfo01w01vc01.sfo01.rainpole.local`** and select **Deploy OVF Template**.
- 4 On the Select template page, select **Local file**, click **Browse**, browse to the location of the vRealize Log Insight .ova file on your local file system, and click **Next**.
- 5 On the Select name and location page, make the following selections, and click **Next**.
  - a Enter a name for the node according to its role.

Name	Role
<b>sfo01vrli01a</b>	Master node

- b Select the inventory folder for the virtual appliance.

Setting	Value
<b>vCenter Server</b>	sfo01w01vc01.sfo01.rainpole.local
<b>Data center</b>	sfo01-w01dc
<b>Folder</b>	sfo01-w01fd-vrli

- 6 On the Select a resource page, select the following values, and click **Next**.

Setting	Value
Data center	sfo01-w01dc
Cluster	sfo01-w01-consolidated01
Resource Pool	sfo01-w01rp-sddc-mgmt

- 7 On the Review details page, examine the virtual appliance details, such as product, version, download size, and disk size, and click **Next**.
- 8 On the Accept license agreements page, accept the end user license agreements and click **Next**.
- 9 On the Select configuration page, from the **Configuration** drop-down menu, select the **Small** deployment configuration, and click **Next**.
- 10 On the Select storage page, select the datastore information.
- From **Select virtual disk format** drop-down menu, select **Thin provision**.
  - From the **VM storage policy** drop-down menu, select **vSAN Default Storage Policy**.
  - From the Datastores table, select the **sfo01-w01-vsan01** datastore and click **Next**.
- 11 On the Select networks page, select the distributed port group on the distributed switch that ends with Mgmt-RegionA01-VXLAN, and click **Next**.
- 12 On the Customize template page, set networking settings and the root user credentials for the virtual appliance.
- In the Networking Properties section, configure the following networking settings.

Property	Value
<b>DNS</b>	172.16.11.5,172.16.11.4
<b>DNS domain</b>	sfo01.rainpole.local
<b>DNS searchpath</b>	sfo01.rainpole.local,rainpole.local
<b>Default gateway</b>	192.168.31.1
<b>Hostname</b>	sfo01vrli01a.sfo01.rainpole.local
<b>Network 1 IP Address</b>	192.168.31.11
<b>Network 1 Netmask</b>	255.255.255.0

- In the Other Properties section, enter and confirm a password for the root user.  
The password must contain at least 8 characters, and must include:
    - One uppercase character
    - One lowercase character
    - One digit
    - One special character
 Use this password when you log in to the console of the vRealize Log Insight virtual appliance.
  - Click **Next**.
- 13 On the Ready to complete page, review the configuration data and click **Finish**.  
The deployment of the virtual appliance starts.
- 14 After the deployment, right-click the virtual appliance object **sfo01vrli01a** and select **Power > Power On**.



## Start the vRealize Log Insight Instance for Consolidated SDDC

Configure and start the vRealize Log Insight master node.

### Procedure

- 1 Open a Web browser and go to **https://sfo01vrli01a.sfo01.rainpole.local**.  
The initial configuration wizard opens.
- 2 On the Setup page, click **Next**.
- 3 On the Choose Deployment Type page, click **Start New Deployment**.
- 4 After the deployment is launched, on the Admin Credentials page, set the email address and the password of the admin user, and click **Save And Continue**.

The password must be at least 8 characters long, and must contain one uppercase character, one lowercase character, one number, and one special character.

- 5 On the License page, enter the license key, click **Add License**, and click **Save And Continue**.
- 6 On the General Configuration page, enter the following settings and click **Save And Continue**.

Setting	Value
<b>Email System Notifications To</b>	<i>email_address_to_receive_system_notifications</i>
<b>Send HTTP Post System Notifications To</b>	https://sfo01vrli01.sfo01.rainpole.local

- 7 On the Time Configuration page, enter the following settings, click **Test**, and click **Save And Continue**.

Setting	Value
<b>Sync Server Time With</b>	NTP server (recommended)
<b>NTP Servers</b>	ntp.sfo01.rainpole.local

- 8 On the SMTP Configuration page, specify the properties of an SMTP server to enable outgoing alerts and system notification emails, and to test the email notification.
  - a Set the connection setting for the SMTP server that will send the email messages from vRealize Log Insight.

Contact your system administrator for details about the email server.

SMTP Option	Description
<b>SMTP Server</b>	FQDN of the SMTP server
<b>Port</b>	Server port for SMTP requests
<b>SSL (SMTPS)</b>	Sets whether encryption should be enabled for the SMTP transport option connection.
<b>STARTTLS Encryption</b>	Enable or disable the STARTTLS encryption.
<b>Sender</b>	Address that appears as the sender of the email.
<b>Username</b>	User name on the SMTP server
<b>Password</b>	Password for the SMTP server you specified in Username

- b To verify that the SMTP configuration is correct, type a valid email address and click **Send test Email**.

vRealize Log Insight sends a test email to the address that you provided.

- 9 On the Setup Complete page, click **Finish**.  
vRealize Log Insight starts operating in standalone mode.


## Enable the Integrated Load Balancer of vRealize Log Insight for Consolidated SDDC

After you create the vRealize Log Insight cluster, enable the Integrated Load Balancer (ILB) for balancing incoming ingestion traffic of syslog data and for high availability.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01a.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under Management, click **Cluster**.
- 4 Under Integrated Load Balancer, click **New Virtual IP Address**.
- 5 In the New Virtual IP dialog box, enter the following settings and click **Save**.

Setting	Value
IP	192.168.31.10
FQDN	sfo01vrli01.sfo01.rainpole.local


## Join vRealize Log Insight to the Active Directory for Consolidated SDDC

To use user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Configuration**, click Authentication.

- 4 On the **Authentication Configuration** page, click the **Active Directory** tab and configure the following Active Directory settings.

Setting	Value
<b>Enable Active Directory support</b>	Selected
<b>Default Domain</b>	RAINPOLE.LOCAL
<b>Domain Controller(s)</b>	dc01rpl.rainpole.local
<b>Username</b>	svc-vrli
<b>Password</b>	<i>svc-vrli_password</i>
<b>Connection Type</b>	Standard
<b>Require SSL</b>	Yes or No according to the instructions from the IT administrator

- 5 Click **Test Connection** to verify the connection, and click **Save**.


## Replace the Certificate of vRealize Log Insight for Consolidated SDDC

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight.

### Procedure


- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under Configuration, click **SSL**.
- 4 On the SSL Configuration page, click **Choose File** next to **New Certificate File (PEM format)**, browse to the location of the PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	vrli-for-1-pod.2.chain.pem

The certificate is uploaded to vRealize Log Insight.

- 5 Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.  
A warning message that the connection is not trusted appears.
- 6 To review the certificate, click the padlock  in the address bar of the browser, and verify that **Subject Alternative Name** contains the name of the vRealize Log Insight cluster node.
- 7 Import the certificate in your Web browser.

For example, in Google Chrome under the HTTPS/TLS settings click **Manage certificates**, and in the Certificates dialog box import *vrli-chain.pem*.

You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

## Connect vRealize Log Insight to the vSphere Environment for Consolidated SDDC

Start collecting log information about the ESXi and vCenter Server instances in the Consolidated SDDC.

### Procedure

- 1 [Configure User Privileges in vSphere for Integration with vRealize Log Insight for Consolidated SDDC](#) on page 224

Assign global permissions in the Consolidated SDDC to the operations service account svc-vrli in order to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight. The svc-vrli user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

- 2 [Connect vRealize Log Insight to vSphere for Consolidated SDDC](#) on page 226

After you configure the svc-vrli Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instance and ESXi hosts, connect vRealize Log Insight to vSphere.

- 3 [Configure vCenter Server to Forward Log Events to vRealize Log Insight for Consolidated SDDC](#) on page 227

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

- 4 [Update the Host Profile for the Consolidated Cluster with Syslog Settings](#) on page 228

In order to have a consistent logging configuration across all ESXi hosts in the consolidated cluster, update the host profile to accommodate the syslog settings for connection to vRealize Log Insight.

## Configure User Privileges in vSphere for Integration with vRealize Log Insight for Consolidated SDDC

Assign global permissions in the Consolidated SDDC to the operations service account svc-vrli in order to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight. The svc-vrli user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 From the **Home** menu, select **Administration**.
- 3 Under Access Control, click **Roles**.

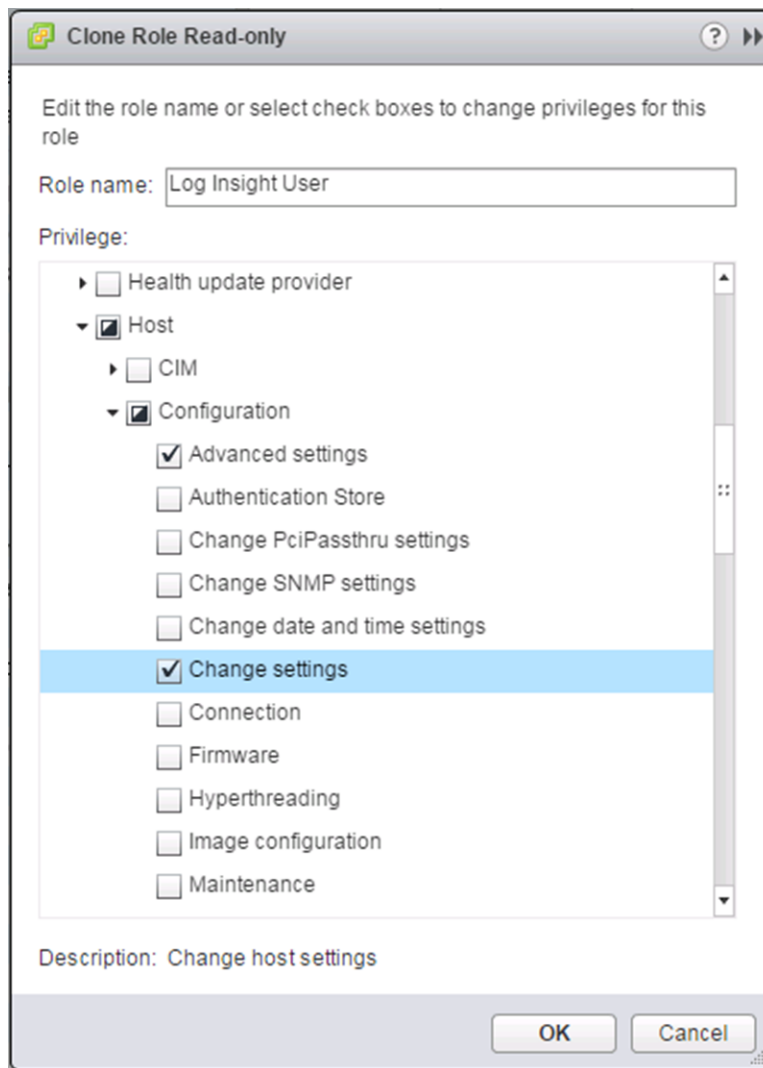
- 4 Create a role for vRealize Log Insight.
  - a Select **Read-only** and click the **Clone role action** icon.

You clone the Read-only role because it includes the **System.Anonymous**, **System.View**, and **System.Read** privileges. vRealize Log Insight requires those privileges for accessing log information related to the vCenter Server instances.

- b In the Clone Role Read-only dialog box, complete the configuration of the role and click **OK**.

Setting	Description
<b>Role name</b>	Log Insight User
<b>Privilege</b>	<ul style="list-style-type: none"> <li>■ Host.Configuration.Advanced settings</li> <li>■ Host.Configuration.Change settings</li> <li>■ Host.Configuration.Network configuration</li> <li>■ Host.Configuration.Security profile and firewall</li> </ul>

These host privileges allow vRealize Log Insight to configure the syslog service on the ESXi hosts.



- 5 Assign global permissions to the **svc-vrli@rainpole.local** service account.
  - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Global Permissions** under Access Control.
  - b On the **Manage** tab, click **Add Permission** icon.
  - c In the Global Permissions Root - Add Permission dialog box, click **Add** to associate a user or a group with a role.
  - d In the Select Users/Groups dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
  - e From the list of users and groups, select the **svc-vrli** user, click **Add**, and click **OK**.
  - f In the Global Permissions Root - Add Permission dialog box, from the **Assigned Role** drop-down menu, select **Log Insight User**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-vrli@rainpole.local user propagate to all linked vCenter Server instances.


## Connect vRealize Log Insight to vSphere for Consolidated SDDC

After you configure the svc-vrli Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instance and ESXi hosts, connect vRealize Log Insight to vSphere.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under Integration, click **vSphere**.
- 4 In the vCenter Servers pane, enter the connection settings for vCenter Server.
  - a Enter the host name, user credentials, and collection options for the vCenter Server instance, and click **Test Connection**.

vCenter Server Option	Value
Hostname	sfo01w01vc01.sfo01.rainpole.local
Username	svc-vrli@rainpole.local
Password	svc-vrli_user_password
Collect vCenter Server events, tasks, and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

- b Click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that you are connected to the correct vCenter Server.
- 5 Click **Save**.  
A progress dialog box appears.

- 6 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instance.

You see the vSphere dashboards under the VMware - vSphere content pack Dashboards category.

## Configure vCenter Server to Forward Log Events to vRealize Log Insight for Consolidated SDDC

You can configure each vCenter Server and Platform Services Controller appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight web interface.

In the Consolidated SDDC, you configure the following vCenter Server and Platform Services Controller instances:

Appliance Type	Virtual Appliance Management Interface URL
vCenter Server instance	<a href="https://sfo01w01vc01.sfo01.rainpole.local:5480">https://sfo01w01vc01.sfo01.rainpole.local:5480</a>
Platform Services Controller instance	<a href="https://sfo01w01psc01.sfo01.rainpole.local:5480">https://sfo01w01psc01.sfo01.rainpole.local:5480</a>

### Procedure

- 1 Redirect the log events from the vCenter Server appliance to vRealize Log Insight.
  - a Open a Web browser and go to **<https://sfo01w01vc01.sfo01.rainpole.local:5480>**.
  - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vc_root_password</i>

- c In the Navigator, click **Syslog Configuration**.
  - d On the Syslog Configuration page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	sf01vrli01.sfo01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- e Repeat the steps for the Platform Services Controller appliance.
- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
  - a Open a Web browser and go to **<https://sfo01vrli01.sfo01.rainpole.local>**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** under **Content Pack Dashboards**.
  - d Verify that the vCenter Server and Platform Services Controller nodes are presented on the All vSphere events by hostname widget of the **General Overview** dashboard.

## Update the Host Profile for the Consolidated Cluster with Syslog Settings

In order to have a consistent logging configuration across all ESXi hosts in the consolidated cluster, update the host profile to accommodate the syslog settings for connection to vRealize Log Insight.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the host profile to the consolidated cluster.
  - a From the vSphere Web Client Home menu, select **Home**.
  - b In the Navigator, click **Policies and Profiles** and click **Host Profiles**.
  - c Right-click **sfo01-w01-consolidated01** and select **Copy Settings from Host**.
  - d Select **sfo01w01esx01.sfo01.rainpole.local** and click **OK**.
- 3 Verify that the syslog host settings have been updated.
  - a On the Host Profiles page in the Navigator, click **sfo01-w01-consolidated01**.
  - b On the **Configure** tab, click **Settings**.
  - c In **Filter** search box, type in **Syslog.global.logHost**.
  - d Select the **Syslog.global.logHost** entry from the list and verify that value of the option is `udp://sfo01vrli01.sfo01.rainpole.local`.
- 4 Verify compliance for the hosts in the consolidated cluster.
  - a From the vSphere Web Client **Home** menu, select **Hosts and Clusters**.
  - b Click the **sfo01-w01-consolidated01** cluster, click the **Monitor** tab, and click **Profile Compliance**.
  - c Click the **Check Compliance Now** button.

Verify All hosts are compliant with the attached profile.

## Connect vRealize Log Insight to vRealize Operations Manager for Consolidated SDDC

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two applications to troubleshoot vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

### Procedure

- 1 [Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight for Consolidated SDDC](#) on page 229  
Configure administrator privileges for the svc-vrli-vrops@rainpole.local service account on vRealize Operations Manager.



- 2 [Enable the vRealize Log Insight Integration with vRealize Operations Manager for Consolidated SDDC](#) on page 230

Connect vRealize Log Insight in the Consolidated SDDC with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.

- 3 [Connect vRealize Operations Manager to vRealize Log Insight for Consolidated SDDC](#) on page 230

- 4 [Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Consolidated SDDC](#) on page 232

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight in Consolidated SDDC.

## Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight for Consolidated SDDC

Configure administrator privileges for the svc-vrli-vrops@rainpole.local service account on vRealize Operations Manager.

### Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left of vRealize Operations Manager, expand **Access** and click **Access Control**.
- 4 On the Access Control page, click the **User Accounts** tab and click the **Import Users** icon.
- 5 On the Import Users page, import the svc-vrli-vrops@rainpole.local service account.
  - a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.
  - b Select the **Basic** option for the search query.
  - c In the **Search String** text box, enter **svc-vrli-vrops** and click **Search**.  
The search result contains the svc-vrli-vrops user account.
  - d Select **svc-vrli-vrops@rainpole.local** user and click **Next**.
- 6 On the Assign Groups and Permissions page, to assign the Administrator role to the svc-vrli-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings, and click **Finish**.

Setting	Value
Select Role	Administrator
Assign this role to the user	Selected
Allow access to all objects in the system	Selected

- 7 When prompted with the warning about allowing access to all objects on the system, click **Yes**.


## Enable the vRealize Log Insight Integration with vRealize Operations Manager for Consolidated SDDC

Connect vRealize Log Insight in the Consolidated SDDC with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under Integration, click **vRealize Operations**.
- 4 On the vRealize Operations Manager page, configure the integration settings for vRealize Operations Manager.

Setting	Value
Hostname	vrops01svr01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	<i>svc-vrli-vrops_password</i>
Enable alerts integration	Selected
Enable launch in context	Selected

- 5 Click **Test Connection** to validate the connection and click **Save**.  
A progress dialog box appears.
- 6 Click **OK** to close the dialog.

## Connect vRealize Operations Manager to vRealize Log Insight for Consolidated SDDC

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment. You can access unstructured log data about any object in your environment by using Launch in Context in vRealize Operations Manager.

## Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
  - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane of vRealize Operations Manager, click **Solutions**.
- 4 On the Solutions page, select **VMware vRealize Log Insight** from the solution table, and click **Configure**.

The Manage Solution - VMware vRealize Log Insight dialog box appears.

- 5 Under Instance Settings, enter the settings for connection to vRealize Log Insight.
  - a Enter the display name, description and the FQDN of the vRealize Log Insight instance.

Setting	Value for vRealize Log Insight
Display Name	Log Insight Adapter - sfo01vrli01
Description	vRealize Log Insight - sfo01
Log Insight server	sfo01vrli01.sfo01.rainpole.local

- b Click **Test Connection** to validate the connection to vRealize Log Insight.
  - c Click **OK** in the Adapter Instance Info box.
  - d Expand the **Advanced Settings** pane and select **sfo01-remote-collectors** from the **Collectors/Groups** drop-down menu.
  - e Click **Save Settings**.
  - f Click **OK** in the Info box about the adapter instance.
- 6 In the Manage Solution - VMware vRealize Log Insight dialog box, click **Close**.

The vRealize Log Insight Adapter is available on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Consolidated SDDC

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight in Consolidated SDDC.

### Procedure

- 1 Enable Secure Shell (SSH) on each node of vRealize Operations Manager in vCenter Server.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Under the sfo01w01vc01.sfo01.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
vrops01svr01a	Master node
sfo01vropsc01a	Remote collector

- d Right-click the appliance node and select **Open Console** to open the remote console to the appliance.
  - e Press ALT+F1 to switch to the command prompt.
  - f Log in using the following credentials.

Setting	Value
User name	root
Password	vrops_root_password

- g Start the SSH service by running the following command.

```
service sshd start
```

- 2 Configure the Log Insight agent in vRealize Operations Manager.
  - a Open an SSH connection to the vRealize Operations Manager appliances using the following settings.

Setting	Value
Hostname	<ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ sfo01vropsc01a.sfo01.rainpole.local</li> </ul>
User name	root
Password	vrops_root_password

- b Edit the liagent.ini file using a text editor such as vi.

```
vi /var/lib/loginsight-agent/liagent.ini
```

- c Locate the [server] section and uncomment the following parameters.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=sfo01vrli01.sfo01.rainpole.local
; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
;
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

- d After the [server] section, add the following block on each vRealize Operations Manager node.

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"<vROPS Node Role Here>",
"vmw_vr_ops_nodename":"<Your vROPS Node Name Here>",
"vmw_vr_ops_hostname":"<Your vROPS Hostname Here>"}
```

- e Modify the following parameters specifically for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_clusterrole	Role of the vRealize Operations Manager node	Set to <b>Master</b> , <b>Replica</b> , <b>Data</b> or <b>Remote Collector</b> according to the role of the node.
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each <Your VROPS Node Name Here> with the following names: <ul style="list-style-type: none"> <li>■ vrops01svr01a</li> <li>■ sfo01vrops01a</li> </ul>
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each <Your VROPS Hostname Here> with the following names: <ul style="list-style-type: none"> <li>■ vrops01svr01a.rainpole.local</li> <li>■ sfo01vrops01a.sfo01.rainpole.local</li> </ul>

Use the following as an example, on the master node you change the [common|filelog] section in order to add context to the logs that are sent to the vRealize Log Insight cluster:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01",
"vmw_vr_ops_clusterrole":"Master", "vmw_vr_ops_nodename":"vrops01svr01a",
"vmw_vr_ops_hostname":"vrops01svr01a.rainpole.local"}
```


- f Press Esc and enter :wq! to save the file.

- g Restart the Log Insight agent on the node by running the following console command.  

```
/etc/init.d/liagentd restart
```
  - h Verify that the Log Insight agent is running.  

```
/etc/init.d/liagentd status
```
  - i Stop the SSH service on the virtual appliance by running the following command.  

```
service sshd stop
```
- 3 Repeat the steps to configure the remaining vRealize Operations Manager appliances.
  - 4 Configure the Linux Agent group for the vRealize Operations Manager components from the vRealize Log Insight Web user interface.
    - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
    - b Log in using the following credentials.
 

Setting	Value
User name	admin
Password	vrli_admin_password
    - c Click the configuration drop-down menu icon  and select **Administration**.
    - d Under Management, click **Agents**.
    - e From the drop-down menu at the top, select **vROps 6.4 or higher - Sample** from the Available Templates section and click **Copy Template** button at the bottom.
    - f In the Copy Agent Group dialog box, enter **vRops6 – Agent Group** in the **Name** text box and click **Copy**.
    - g In the agent filter fields, enter the following values pressing Enter after each host name.
 

Filter	Operator	Values
Hostname	matches	■ vrops01svr01a.rainpole.local
		■ sfo01vropsc01a.sfo01.rainpole.local
    - h Click **Refresh** and verify that all the agents in the filter appear in the Agents list.
    - i Click **Save New Group** button at the bottom of the page.
    - j Click the **Dashboards** tab and select the **VMware - vRops 6.x** dashboard under the **Content Pack Dashboards** on the left.

All VMware - vRops 6 dashboards become available on the home page of vRealize Log Insight. You see Total number of vRops Clusters showing 1 and Total number of vRops nodes over time showing the host names of the vRealize Operations Manager nodes.

## Connect vRealize Log Insight to the NSX Instances for Consolidated SDDC

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

### Procedure

- 1 [Install the vRealize Log Insight Content Pack for NSX for vSphere for Consolidated SDDC](#) on page 235  
Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight.
- 2 [Configure NSX Manager to Forward Log Events to vRealize Log Insight for Consolidated SDDC](#) on page 236  
Configure the NSX Manager for the consolidated cluster to send audit logs and system events to vRealize Log Insight in the Consolidated SDDC.
- 3 [Configure the NSX Controllers to Forward Events to vRealize Log Insight for Consolidated SDDC](#) on page 236  
Configure the NSX Controller instances for the consolidated cluster to forward log information to vRealize Log Insight in Consolidated SDDC by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.
- 4 [Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight for Consolidated SDDC](#) on page 240  
Redirect log information from the edge services gateways, universal distributed logical router and load balancer to vRealize Log Insight in the Consolidated SDDC.


## Install the vRealize Log Insight Content Pack for NSX for vSphere for Consolidated SDDC

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight.

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - NSX-vSphere** content pack and click its icon.
- 5 In the Install Content Pack dialog box, accept the License Agreement and click **Install**.
- 6 In the VMware - NSX-vSphere Setup Instructions dialog box, click **OK**.

After the installation is complete, the VMware - NSX-vSphere content pack appears in the Installed Content Packs list on the left.

## Configure NSX Manager to Forward Log Events to vRealize Log Insight for Consolidated SDDC

Configure the NSX Manager for the consolidated cluster to send audit logs and system events to vRealize Log Insight in the Consolidated SDDC.

### Procedure

- 1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.
  - a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the consolidated cluster	<a href="https://sfo01w01nsx01.sfo01.rainpole.local">https://sfo01w01nsx01.sfo01.rainpole.local</a>

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 On the main page of the appliance user interface, click **Manage Appliance Settings**.
- 3 Under Settings, click **General**, and in the Syslog Server pane, click **Edit**.
- 4 In the Syslog Server dialog box, configure vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	sfo01vrli01.sfo01.rainpole.local
Port	514
Protocol	UDP

## Configure the NSX Controllers to Forward Events to vRealize Log Insight for Consolidated SDDC

Configure the NSX Controller instances for the consolidated cluster to forward log information to vRealize Log Insight in Consolidated SDDC by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

### Procedure

- 1 Log in to the Windows host that has access to your data center.
- 2 In a Chrome Web browser, start the Postman application and log in.



- 3 Specify the request headers for requests to the NSX Manager.
  - a On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	<i>sfo01nsx_admin_password</i>

The Authorization:Basic XXX header appears in the Headers pane.

- b On the **Headers** tab, enter the following header details.

Request Header Attribute	Value
Content-Type	application/xml

The Content-Type:application/xml header appears in the Headers pane.

- 4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.
  - a Select **GET** from the drop-down menu that contains the HTTP request methods.
  - b In the URL text box next to the selected method, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the consolidated cluster	<a href="https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller">https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller</a>

The Postman application sends a query to the NSX Manager about the installed NSX controllers.

- c After the NSX Manager sends a response back, click the **Body** tab in the response pane.

The response body contains a root `<controllers>` XML element that groups the details about the three controllers that form the controller cluster.

- d Within the `<controllers>` element, locate the `<controller>` element for each controller and write down the content of the `id` element.

Controller IDs have the `controller-id` format where *id* represents the sequence number of the controller in the cluster, for example, `controller-2`.

The screenshot shows a web browser window with the address bar displaying `https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller`. The browser is displaying the response body of a GET request. The response is an XML document with the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<controllers>
 <controller>
 <objectTypeName>Controller</objectTypeName>
 <revision>0</revision>
 <name>nsx-controller-w01-01</name>
 <clientHandle></clientHandle>
 <isUniversal>false</isUniversal>
 <universalRevision>0</universalRevision>
 <id>controller-1</id>
 <ipAddress>172.20.31.118</ipAddress>
 <status>RUNNING</status>
 <upgradeStatus>NOT_STARTED</upgradeStatus>
 <version>6.3.49862</version>
 <upgradeAvailable>true</upgradeAvailable>
 <virtualMachineInfo>
 <objectId>vm-61</objectId>
 <objectTypeName>VirtualMachine</objectTypeName>
 <vsmUuid>42238848-7155-14FC-6A2F-E381D54881EA</vsmUuid>
 <nodeId>9eb6f396-a3bc-4a95-a64e-e38a019f3c70</nodeId>
 <revision>12</revision>
 <type>
 <typeName>VirtualMachine</typeName>
 </type>
 <name>NSX_Controller_d5c429e8-192d-4e32-8dfc-e347a2dc3ee1</name>
 <scope>
 <id>resgroup-25</id>
 <objectTypeName>ResourcePool</objectTypeName>
 <name>sfo01-w01rp-sddc-edge</name>
 </scope>
 <clientHandle></clientHandle>
 <extendedAttributes></extendedAttributes>
 <isUniversal>false</isUniversal>
 <universalRevision>0</universalRevision>
 </virtualMachineInfo>
 <hostInfo>
 <objectId>host-22</objectId>
 <objectTypeName>HostSystem</objectTypeName>
 </hostInfo>
 </controller>

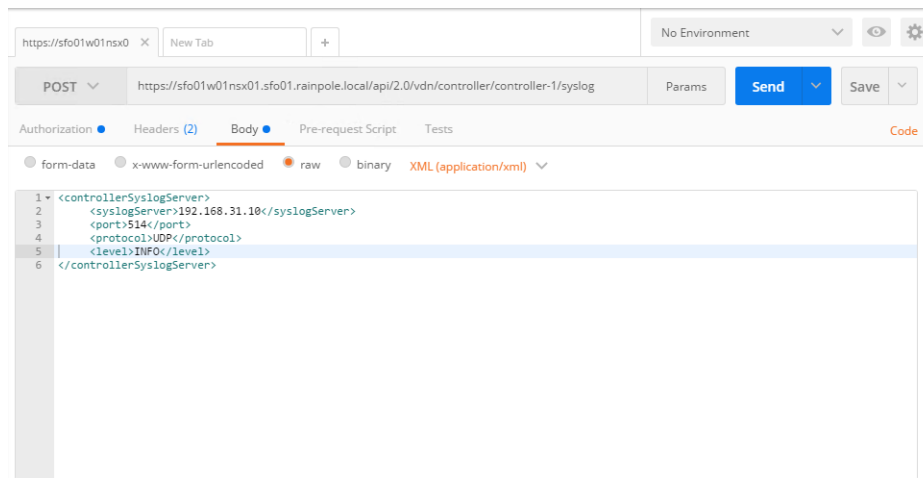
```

- 5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.
  - a In the request pane at the top, select **POST** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the consolidated cluster	NSX Controller 1	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-3/syslog

- b Click the **Body** tab, select **raw**, ensure that the content-type is **XML (application/xml)**, paste the following request body in the **Body** text box, and click **Send**.

```
<controllerSyslogServer>
 <syslogServer>192.168.31.10</syslogServer>
 <port>514</port>
 <protocol>UDP</protocol>
 <level>INFO</level>
</controllerSyslogServer>
```



- c Repeat the steps for the other NSX Controllers.
- 6 Verify the syslog configuration on each NSX Controller.
  - a In the request pane, from the method drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from the previous step, and click the **Send** button.
  - b After the NSX Manager sends a response back, click the **Body** tab in the response pane.  
The response body contains a root <controllerSyslogServer> element which represents the settings for the remote syslog server on the NSX Controller.

- c Verify that the value of the <syslogServer> element is 192.168.31.10.
- d Repeat the steps for the other NSX Controllers to verify the syslog configuration.

The screenshot shows a REST client interface with the following details:

- URL:** `https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog`
- Method:** GET
- Authorization:** Basic Auth
  - Username:** admin
  - Password:** [REDACTED]
- Body:** XML
 

```
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
 <syslogServer>192.168.31.10</syslogServer>
 <port>514</port>
 <protocol>UDP</protocol>
 <level>INFO</level>
</controllerSyslogServer>
```
- Status:** 200 OK, Time: 113 ms

## Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight for Consolidated SDDC

Redirect log information from the edge services gateways, universal distributed logical router and load balancer to vRealize Log Insight in the Consolidated SDDC.

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.
- 3 From the **Networking & Security** menu on the left, click **NSX Edges**.
- 4 On the **NSX Edges** page, select the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	IP Address
Consolidated NSX Manager	172.16.11.66

The edge devices in the scope of the NSX Manager appear.

- 5 Configure the log forwarding on each edge service gateway of the Consolidated NSX Manager instance.
  - a Double-click the edge device to open its user interface.

Traffic	Consolidated NSX Edge Services Gateway
North-South Routing	sfo01w01esg01
North-South Routing	sfo01w01esg02
East-West Routing	sfo01w01udlr01
Load Balancer	sfo01w01lb01

- b On the NSX Edge device page, click the **Manage** tab, click **Settings**, and click **Configuration**.
  - c In the Details pane, click **Change** next to **Syslog servers**.
  - d In the Edit Syslog Servers Configuration dialog box, configure the following settings and click **OK**.

Setting	Value
Syslog Server 1	192.168.31.10
Protocol	udp

- e Click **OK**.
  - f Repeat the steps for the remaining NSX Edge devices of Consolidated NSX Manager instance.

The vRealize Log Insight user interface starts showing log data in the NSX-vSphere-Overview dashboard. The dashboard is under the VMware - NSX-vSphere group of Content Pack Dashboards.

## Connect vRealize Log Insight to vRealize Automation for Consolidated SDDC

Connect the vRealize Log Insight to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight user interface.

### Procedure

- 1 [Install the vRealize Log Insight Content Packs for the Cloud Management Platform for Consolidated SDDC](#) on page 242  
Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.
- 2 [Install and Configure vRealize Log Insight Windows Agents for Consolidated SDDC](#) on page 243  
Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents from the vRealize Log Insight Web interface.
- 3 [Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances for Consolidated SDDC](#) on page 245  
vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on the virtual appliance using the appliance management interface.
- 4 [Configure the vRealize Log Insight Linux Agents on vRealize Business for Consolidated SDDC](#) on page 247  
vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

- 5 [Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight for Consolidated SDDC](#) on page 249

You enable the vRealize Log Insight agent and configure the agent group for the embedded vRealize Orchestrator to start collecting log data in the vRealize Orchestrator dashboards.

## Install the vRealize Log Insight Content Packs for the Cloud Management Platform for Consolidated SDDC

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.


You install the following content packs:

- VMware - vRA 7
- VMware - Orchestrator - 7.0.1+
- Microsoft - SQL Server

### Procedure

- 1 Log in to the vRealize Log Insight user interface.
  - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under Content Pack Marketplace, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.
- 5 In the Install Content Pack dialog box, accept the license agreement and click **Install**.
- 6 In the VMware - vRA 7 Setup Instructions dialog box, click **OK**.
- 7 Repeat the procedure to install the **VMware - Orchestrator - 7.0.1+** and **Microsoft - SQL Server** content packs.

After the installations are complete, the VMware - vRA, VMware - Orchestrator - 7.0.1+ and Microsoft - SQL Server content packs appear in the Installed Content Packs list on the left.

## Install and Configure vRealize Log Insight Windows Agents for Consolidated SDDC

Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents from the vRealize Log Insight Web interface.

### Procedure

- 1 Install the Log Insight Windows Agents on all the vRealize Automation Windows VMs.

- a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

vRealize Automation Component	Host Name or VM Name
IaaS Web Server	vra01iws01a.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local


- b Log in using the following credentials.

Setting	Value
User name	Rainpole\svc-vra
Password	svc-vra-user-password

- c Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.

- d Log in using the following credentials.


Setting	Value
User name	admin
Password	vrli_admin_password

- e Click the configuration drop-down menu icon  and select **Administration**.
- f Under Management, click **Agents**.
- g On the Agents page, click the **Download Log Insight Agent Version xxx** link.
- h In the Download Log Insight Agent Version xxx dialog box, click **Windows MSI (32-bit/64-bit)** and save the .msi file on your computer.
- i Double-click the .msi file to run the installer.
- j In the VMware vRealize Log Insight Agent Setup wizard, accept the license agreement and click **Next**.
- k With the Log Insight host name **sfo01vrli01.sfo01.rainpole.local** shown in the **Host** text box, click **Install**.
- l After the installation is complete, click **Finish**.
- m Repeat the steps for other Windows VMs.

- 2 Configure the Log Insight Windows agent group for the vRealize Automation IaaS components from the vRealize Log Insight user interface.

- a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password


- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under Management, click **Agents**.
- e From the drop-down at the top, select **vRealize Automation 7 - Windows** from the Available Templates section.
- f Click **Copy Template**.
- g In the Copy Agent Group dialog box, enter **vRA7 - Windows Agent Group** in the **Name** text box and click **Copy**.
- h In the agent filter fields, use the following selections.  
Press ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	■ vra01iws01a.rainpole.local ■ vra01ims01a.rainpole.local

- i Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.
  - j Click **Save New Group** at the bottom of the page.
- 3 Configure the Log Insight Windows Agent Group for the Microsoft SQL Server component that is used by vRealize Automation.

- a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under Management, click **Agents**.
- e From the drop down on the top, select **Microsoft - SQL Server** from the Available Templates section.
- f Click **Copy Template**.
- g In the Copy Agent Group dialog box, enter **vRA7 - Microsoft SQL Server Agent Group** in the **Name** text box and click **Copy**.



- h In the agent filter fields, use the following selections.

Press ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01mssql01.rainpole.local

- i Under Agent Configuration, click **Edit**.
- j Locate `directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log` and change it to `directory=C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log`  
In this VMware Validated Design, Microsoft SQL Server 2012 R2 has been installed in the default location on the Windows Server virtual machine.
- k Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.
- l Click **Save New Group** at the bottom of the page.

All VMware - vRA 7 dashboards become available on the vRealize Log Insight Home page.

## Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances for Consolidated SDDC

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on the virtual appliance using the appliance management interface.

### Procedure

- 1 Configure Log Insight agent in the management interface of the vRealize Automation Appliance.

- a Open a Web browser and log in to the following URL.

Setting	Value
URL	<code>https://vra01svr01a.rainpole.local:5480/</code>
User name	<code>root</code>
Password	<code>vra_applianceA_root_password</code>

- b On the **VRA Settings** tab, click the **Logs** tab .
- c Scroll down to the **Log Insight Agent Configuration** section
- d Enter the following values and click **Save Settings**,


Setting	Value
Host	<code>sfo01vrli01.sfo01.rainpole.local</code>
Port	<code>9000</code>
Protocol	<code>CFAPI</code>
SSL Enabled	<code>Unchecked</code>
Reconnect	<code>30</code>
Max Buffer Size	<code>2000</code>

## 2 Configure the Linux agent group on the vRealize Log Insight server.

a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

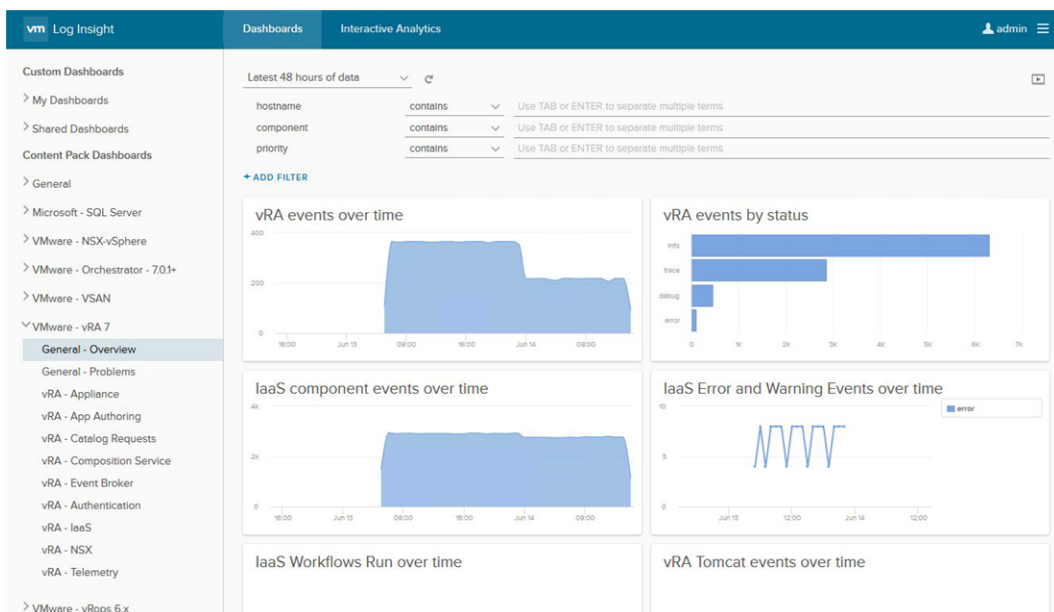
c Click the configuration drop-down menu icon  and select **Administration**.d Under Management, click **Agents**.e From the drop-down menu on the top, select **vRealize Automation 7 - Linux** from the Available Templates section.f Click **Copy Template** at the bottom of the page.g In the Copy Agent Group dialog box, enter **vRA7 - Linux Agent Group** in the name field and click **Copy**.

h In the agent filter fields, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	matches	vra01svr01a.rainpole.local

i Click **Refresh** and verify that all the agents in the filter appear in the Agents list.j Click **Save New Group** at the bottom of the page.k Click the **Dashboard** tab and select the **VMware - VR 7** dashboard from the drop-down menu on the left.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.



## Configure the vRealize Log Insight Linux Agents on vRealize Business for Consolidated SDDC

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

### Procedure

- 1 Enable Secure Shell on both the vRealize Business appliances.

- a Open a Web browser and go to the following URLs,

vRealize Business node	Virtual Appliance Management Interface URL
vRealize Business Server Appliance	<a href="https://vr01svr01.rainpole.local:5480">https://vr01svr01.rainpole.local:5480</a>
vRealize Business Data Collector	<a href="https://sfo01vrbc01.sfo01.rainpole.local:5480">https://sfo01vrbc01.sfo01.rainpole.local:5480</a>

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vr01svr01_root_password</i>

The appliance management interface of the appliance opens.

- c Click the **Administration** tab and click **Administration**.
  - d Under the Actions section, click **Toggle SSH setting**.
  - e Verify that the SSH service status reports **Enabled**.
- 2 Configure the Log Insight agent in on the vRealize Business appliances.

- a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	■ vr01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local
User name	root
Password	<i>vr01svr01_appliance_root_password</i>

- b Edit the `liagent.ini` file using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

- c Add the following information under `[server]` section

```
[server]

hostname=sfo01vrli01.sfo01.rainpole.local

proto = cfapi

port = 9000

ssl = no
```


- d Replace all instances of FQDN\_localhost parameter located after agent\_name with vrb01svr01.rainpole.local.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local
proto=cfcp1
port=9000
ssl=no

; itfm server log
[filelog]ItfmServer
directory=/var/log/vrb/itfm-server
include=*
tags={"appliance": "vrb", "service": "itfm_server", "agent_name": "vrb01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"

; itfm tomcat log
[filelog]ItfmCatalina
directory=/usr/local/tcserver/vfabric-tc-server-standard/itbm-server/logs
include=*
tags={"appliance": "vrb", "service": "itfm_catalina", "agent_name": "vrb01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"

; data collector log
[filelog]DataCollector
directory=/var/log/vrb/data-collector
include=*
tags={"appliance": "vrb", "service": "data_collector", "agent_name": "vrb01svr01.rainpole.local"}
event_marker="(\d{4}-\d{2}-\d{2})\d{2}:\d{2}:\d{2}\.\d{3}\d{2}-[A-Z][a-z]{2}-\d{4}\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"
```

- e Press ESC and enter :wq! to save the file.
- f Start the Log Insight agent.
- ```
/etc/init.d/liagentd start
```
- g Verify that the Log Insight agent is running.
- ```
/etc/init.d/liagentd status
```
- h Turn on auto-run by default for the log insight agent.
- ```
chkconfig liagentd on
```
- i Repeat the steps to configure the vRealize Business Data Collector at vrb01buc01.sfo01.rainpole.local.
- 3 Confirm that the Log Insight agents are working in the vRealize Log Insight Web interface.
- a Open a Web browser and go to **<https://sfo01vrli01.sfo01.rainpole.local>**.
- b Log in using the following credentials.
- | Setting | Value |
|-----------|---------------------|
| User name | admin |
| Password | vrli_admin_password |
- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under Management, click **Agents**.
- e Verify that vrb01svr01.rainpole.local and sfo01vrbc01.sfo01.rainpole.local appear on the page.


Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight for Consolidated SDDC

You enable the vRealize Log Insight agent and configure the agent group for the embedded vRealize Orchestrator to start collecting log data in the vRealize Orchestrator dashboards.

Procedure

- 1 Enable vRealize Log Insight agents for vRealize Orchestrator.
 - a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|---------------------|
| User name | admin |
| Password | vrli_admin_password |

- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under Management, click **Agents**.
- e From the drop-down menu at the top, select **vRealize Orchestrator 7.0.1** from the All Agents section and click **Copy Template**.
- f In the Copy Agent Group dialog box, enter **vr07 - Agent Group** in the name text box and click **Copy**.
- g To set which agents receive the configuration, in the agent filter fields, enter the following values pressing Enter after each host name.

| Filter | Operator | Values |
|----------|----------|----------------------------|
| Hostname | matches | vra01svr01a.rainpole.local |

- h Click **Refresh** and verify that in the Agents list vRealize Log Insight receives data from the two agents in the filter.
 - i Click **Save Agent Group** at the bottom of the page.
- 2 Verify that the vRealize Log Insight server is receiving log events from the vRealize Orchestrator appliances.
 - a On the main navigation bar, click **Dashboards**.
 - b In the vRealize Log Insight user interface, click **VMware - Orchestrator - 7.0.1+** under Content Pack Dashboards.
 - c Verify that the Server nodes grouped by hostname widget on the **Server overview** dashboard shows the vRealize Appliance host name vra01svr01a.rainpole.local

Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Consolidated SDDC

Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances in vRealize Log Insight.


Procedure

- 1 Log in to the vRealize Log Insight user interface.


- a Open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|---------------------|
| User name | admin |
| Password | vrli_admin_password |

- 2 Install the content pack for VMware Linux.

- a In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
 - b Under Content Pack Marketplace, select **Marketplace**.
 - c In the list of content packs, locate the **Linux** content pack and click its icon.
 - d In the Install Content Pack dialog box, accept the License Agreement and click **Install**.
 - e After the installation is complete, the **Linux** content pack appears in the Installed Content Packs list on the left.

- 3 Configure the Log Insight Linux agent group for the virtual appliances from the vRealize Log Insight user interface.

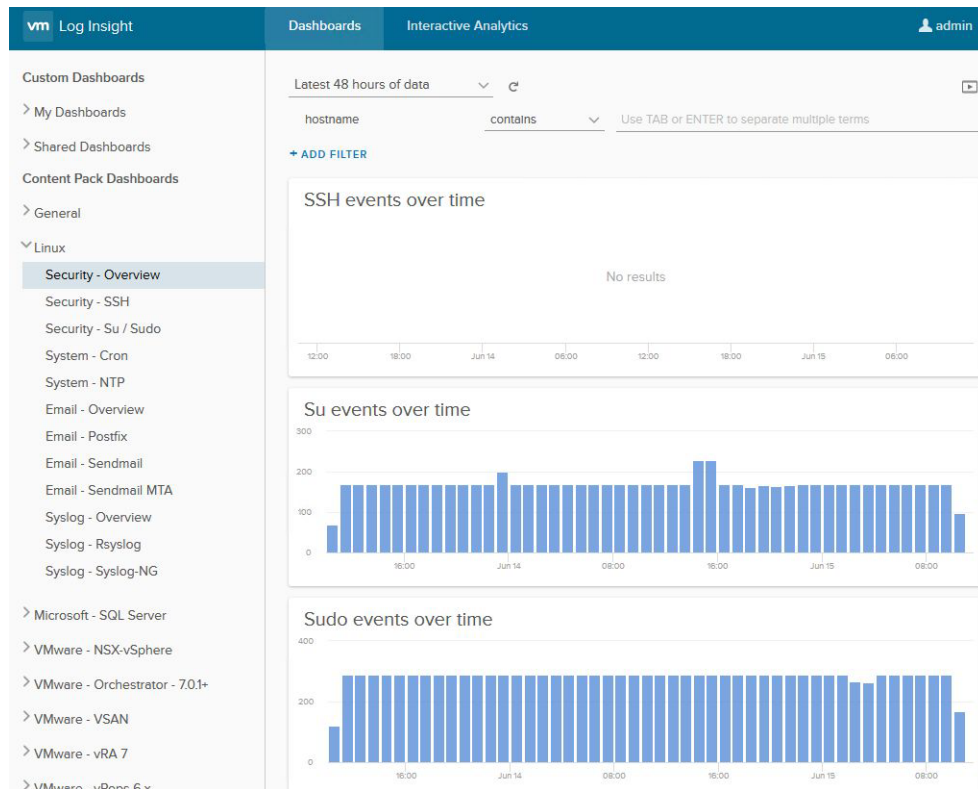
- a Click the configuration drop-down menu icon  and select **Administration**.
 - b Under Management, click **Agents**.
 - c From the drop-down at the top, select **Linux** from the Available Templates section.
 - d Click **Copy Template**.
 - e In the Copy Agent Group dialog box, enter **vAppliances - Agent Group** in the **Name** text box and click **Copy**.
 - f In the agent filter fields, use the following selections.

Press ENTER to separate the host name values.

| Filter | Operator | Values |
|----------|----------|---------------------------------------|
| Hostname | matches | ■ vrops01svr01a.rainpole.local |
| | | ■ sfo01vropsc01a.sfo01.rainpole.local |
| | | ■ vra01svr01a.rainpole.local |
| | | ■ vrb01svr01.rainpole.local |
| | | ■ sfo01vrbc01.sfo01.rainpole.local |

- g Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.
 - h Click **Save New Group** at the bottom of the page.

- 4 Verify logs data is showing up on the Linux dashboards.
 - a On the main navigation bar, click **Dashboards**.
 - b Expand Linux and click **Security - Overview**.




Configure Log Retention and Archiving for Consolidated SDDC

Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **<https://sfo01vrli01.sfo01.rainpole.local>**.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|---------------------|
| User name | admin |
| Password | vrli_admin_password |

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.

3 Configure retention threshold notification.

Log Insight continually estimates how long data can be retained with the currently available pool of storage.

If the estimation drops below the retention threshold of one week, Log Insight immediately notifies the administrator that the amount of searchable log data is likely to drop.

- a Under Configuration, click **General**.
- b On the General Configuration page, under the Alerts section, select the **Send a notification when capacity drops below** check box next to **Retention Notification Threshold**, and enter a 1-week period in the text box.
- c Click **Save**.

The screenshot shows the VMware Log Insight web interface. The left-hand navigation pane is expanded to the 'Configuration' section, with 'General' selected. The main panel displays the 'General Configuration' settings. Under the 'ALERTS' section, the 'Email System Notifications To' field is set to 'administrator@rainpole.local'. The 'Send HTTP Post System Notifications To' field is set to 'https://sfo01vrlt01.sfo01.rainpole.local'. The 'Retention Notification Threshold' section has a checked box for 'Send a notification when capacity drops below' and a dropdown menu set to '1 weeks'. The 'BROWSER SESSION' section shows a 'Session Timeout' of '30 minutes'. The 'CUSTOMER EXPERIENCE IMPROVEMENT PROGRAM' section has a checked box for 'Join the VMware Customer Experience Improvement Program'. The 'LANGUAGE' section has a toggle for 'Always Use English'. The 'EXPERIMENTAL FEATURES' section has a toggle for 'Enable User Impersonation'. At the bottom of the configuration area are 'SAVE' and 'RESET TO DEFAULTS...' buttons.

4 Configure data archiving.

- a Under Configuration, click **Archiving**.
- b Toggle **Enable Data Archiving** on.
- c In the **Archive Location** text box, enter the path in the form of **nfs://nfs-server-address/V2D_vRLT_Consolidated_250GB** to an NFS partition where logs will be archived.
- d Click **Test** next to the **Archive Location** text box to verify that the share is accessible.
- e Click **Save**.

vSphere Update Manager Download Service Implementation for Consolidated SDDC

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository for consolidated SDDC.

Procedure

- 1 [Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS for Consolidated SDDC](#) on page 253
On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.
- 2 [Install UMDS on Ubuntu OS for Consolidated SDDC](#) on page 255
After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.
- 3 [Set Up the Download on UMDS for Consolidated SDDC](#) on page 256
By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download on UMDS in the Consolidated SDDC.
- 4 [Install and Configure the UMDS Web Server for Consolidated SDDC](#) on page 257
The UMDS server in the Consolidated SDDC downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.
- 5 [Use the UMDS Shared Repository as the Download Source in Update Manager for Consolidated SDDC](#) on page 258
Configure Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS for Consolidated SDDC

On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.

Prerequisites

- Create a virtual machine for UMDS on the consolidated cluster. See *Virtual Machine Specifications* from the *Planning and Preparation* documentation.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password | vsphere_admin_password |

- 2 In the vSphere Web Client, right-click the **sfo01umds01** virtual machine and select **Open Console** to open the remote console to the virtual machine.
- 3 At the command prompt, log in as the **svc-umds** user using **svc-umds_password**.

- 4 Install Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

- 5 Log back in to the UMDS virtual machine using Secure Shell (SSH) client and the `svc-umds` service account credentials.

- 6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

- 7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the `umds_db_user_password` password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_user -P
```

- 8 Enable password authentication for the database user.

- a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

| Linux system | Default Location |
|--------------|---------------------------------------|
| Ubuntu 14.04 | /etc/postgresql/postgres_version/main |

```
cd /etc/postgresql/postgres_version/main
```

- b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

You can use the `vi` editor to make and save the changes.

| #TYPE | DATABASE | USER | ADDRESS | METHOD |
|-------|----------|--------------|---------|--------|
| local | umds_db | umds_db_user | | md5 |

- c Log out as a PostgreSQL user by running the following command.

```
logout
```

- 9 Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

- a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

- b Replace the file with the following content and save the change using `:wq`.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

- c Edit the system file `/etc/odbc.ini`.


```
sudo vi /etc/odbc.ini
```
- d Replace the file with the following content and save the change using `:wq`,


```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = database_name
;USER_ID = database_username
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_user
User = umds_db_user
Database = umds_db
```
- 10 Create a symbolic link between the UMDS and the PostgreSQL by running the following command.


```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.5432
```
- 11 Restart PostgreSQL.


```
sudo service postgresql restart
```

Install UMDS on Ubuntu OS for Consolidated SDDC

After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.

Prerequisites

- Verify you have administrative privileges on the UMDS Ubuntu virtual machine.
- Mount the ISO file of the vCenter Server Appliance to the Linux machine.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `sfo01umds01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|--------------------------------|
| User name | <code>svc-umds</code> |
| Password | <code>svc-umds_password</code> |

- 2 Mount the vCenter Server Appliance ISO to the UMDS virtual machine.


```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```
- 3 Unarchive the `VMware-UMDS-6.5.0-build_number.tar.gz` file:


```
tar -xzf /mnt/cdrom/umds/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```
- 4 Run the UMDS installation script.


```
sudo /tmp/vmware-umds-distrib/vmware-install.pl
```

- 5 Read and accept the EULA.
- 6 Press Enter to install UMDS in the default directory `/usr/local/vmware-umds` and enter **yes** to confirm directory creation.
- 7 Enter the UMDS proxy settings if needed according to the settings of your environment.
- 8 Press Enter to set the default patch location to `/var/lib/vmware-umds` and enter **yes** to confirm directory creation.
- 9 Provide the database details.

| Option | Description |
|--------------------------------------|------------------------------|
| Provide the database DSN | UMDS_DSN |
| Provide the database username | <i>umds_db_user</i> |
| Provide the database password | <i>umds_db_user_password</i> |

- 10 Type **yes** and press Enter to install UMDS.

Set Up the Download on UMDS for Consolidated SDDC

By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download on UMDS in the Consolidated SDDC.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `sfo01umds01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

| Setting | Value |
|------------------|--------------------------|
| User name | <i>svc-umds</i> |
| Password | <i>svc-umds_password</i> |

- 2 Navigate to the directory where UMDS is installed.


```
cd /usr/local/vmware-umds/bin
```
- 3 Disable the updates for older hosts and virtual appliances.


```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```
- 4 Configure automatic daily downloads by creating a cron job file.


```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```
- 5 Edit the download command of the cron job.


```
sudo vi umds-download
```
- 6 Add the following lines to the file.


```
#!/bin/sh
/usr/local/vmware-umds/bin/vmware-umds -D
sudo chmod -R 755 /var/lib/vmware-umds
```

- 7 Test the UMDS Download cron job.

```
sudo ./umds-download
```

Install and Configure the UMDS Web Server for Consolidated SDDC

The UMDS server in the Consolidated SDDC downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds`. You share this folder out to the VUM instances within the region using an Nginx Web server.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `sfo01umds01.sfo01.rainpole.local`.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|-------------------|
| User name | svc-umds |
| Password | svc-umds_password |

- 2 Install the Nginx Web server with the following command.


```
sudo apt-get -y install nginx
```
- 3 Change the patch repository directory permissions by running the command.


```
sudo chmod -R 755 /var/lib/vmware-umds
```
- 4 Copy the default site configuration to use it with the UMDS configuration.


```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/umds
```
- 5 Edit the new `/etc/nginx/sites-available/umds` site configuration file and replace the `server {}` block with the following content.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/lib/vmware-umds;
    index index.html index.htm;

    # Make site accessible from http://localhost/
    server_name localhost sfo01umds01 sfo01umds01.sfo01.rainpole.local;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
        # Uncomment to enable naxsi on this location
        # include /etc/nginx/naxsi.rules
        autoindex on;
    }
}
```

- 6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

- 7 Enable the new UMDS site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

- 8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

- 9 Ensure you can browse the files on the UMDS Web server by opening a Web browser to `http://sfo01umds01.sfo01.rainpole.local`.

Use the UMDS Shared Repository as the Download Source in Update Manager for Consolidated SDDC

Configure Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.
 - b Log in using the following credentials.

| Setting | Value |
|-----------|-----------------------------|
| User name | administrator@vsphere.local |
| Password | vsphere_admin_password |

- 2 On the Home page of the vSphere Web Client, click the **Update Manager** icon.
- 3 On the **Objects** tab, click the `sfo01w01vc01.sfo01.rainpole.local` vCenter Server.
The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.
- 5 On the Download sources page, click **Edit**.
The Edit Download Sources dialog box opens.
- 6 Enter the following setting and click **OK**.

| Setting | Value |
|-------------------------|---|
| Use a shared repository | Selected |
| URL | http://sfo01umds01.sfo01.rainpole.local |

The vSphere Web Client performs validation of the URL.

- 7 In the Download sources page, click **Download Now** to run the download patch definitions.
Verify that a new task **Download Patch Definition** appears in the Recent Tasks pane and completes successfully.