Deployment of VMware NSX-T for Workload Domains

Modified on 02 MAY 2019

VMware Validated Design 5.0.1

VMware NSX-T 2.4

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About Deployment of VMware NSX-T for Workload Domains 1

Deployment of VMware NSX-T for Workload Domains provides step-by-step instructions for extending a Standard SDDC with a virtual infrastructure workload domain that uses VMware NSX-T for software-defined networking.

Intended Audience

The *Deployment of VMware NSX-T for Workload Domains* document is intended for architects and administrators who want to deploy NSX-T in a virtual infrastructure workload domain for tenant workloads.

Required VMware Software

Deployment of VMware NSX-T for Workload Domains is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

- Software components for VMware Validated Design for Software-Defined Data Center 5.0.1
- NSX-T 2.4

Prerequisites

Deploy the management workload domain and optionally the initial virtual infrastructure workload domain according to VMware Validated Design for Software-Defined Data Center at least in a single region. See the VMware Validated Design documentation page.

Updated Information

Deployment of VMware NSX-T for Workload Domains is updated with each release of the product or when necessary.

This table provides the update history of the *Deployment of VMware NSX-T for Workload Domains*.

Revision	Description
02 MAY 2019	■ The command to join an NSX-T Edge node to the management plane is referring to the NSX-T Manager node instead of to the NSX-T Edge node. See Join the NSX-T Edge Nodes to the Management Plane. ■ The configuration of the Tier-0 gateway includes the uplink interfaces to the NSX-T Edge nodes now. See Create and Configure the Tier-0 Gateway.
19 MAR 2019	Initial release.

Preparing for Deploying a Workload Domain with NSX-T 2

Deployment of VMware NSX-T for Workload Domains is based on VMware Validated Design for Software-Defined Data Center. You deploy the virtual network infrastructure on VMware NSX-T for a workload domain in a shared edge and compute cluster.

Deployment of VMware NSX-T for Workload Domains adds an additional workload domain to VMware Validated Design.

Before You Deploy a Compute Workload Domain with NSX-T

You must first deploy and configure the components of the SDDC management cluster. See Planning and Preparation and Deployment for Region A documentation.

- ESXi hosts
- Platform Services Controller pair and Management vCenter Server
- NSX for vSphere
- vRealize Lifecycle Manager
- vSphere Update Manager
- vRealize Operations Manager
- vRealize Log Insight
- vRealize Automation with embedded vRealize Orchestrator
- vRealize Business

If you implement the full guidance in VMware Validated Design, you also deploy a compute workload domain that uses NSX for vSphere as the solution for virtual networking.

1 Prerequisites for the NSX-T Deployment for the Shared Edge and Compute Cluster

  Before you deploy the NSX-T components, verify that your environment satisfies the requirements for this deployment.

2 Generate CA-Signed Certificates for the NSX-T Manager Nodes

By using the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`), generate certificates for the NSX-T Manager instances and cluster virtual IP that are signed by the Microsoft certificate authority (MSCA). You use these certificates for trusted communication between the NSX-T nodes and the other management components of the SDDC.

Prerequisites for the NSX-T Deployment for the Shared Edge and Compute Cluster

Before you deploy the NSX-T components, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that the static IP addresses and FQDNs for all components are allocated on the DNS server and are available for deployment.

Table 2-1. VLAN IDs and IP Subnets for the ESXi Hosts of the Workload Domain

VLAN Function	VLAN ID	Subnet	Gateway
ESXi Management	1641	172.16.41.0/24	172.16.41.253
vSphere vMotion	1642	172.16.42.0/24	172.16.42.253
vSAN	1643	172.16.43.0/24	172.16.43.253
Host overlay	1644	172.16.44.0/24	172.16.44.253
Uplink01	1647	172.16.47.0/24	172.16.47.253
Uplink02	1648	172.16.48.0/24	172.16.48.253
Edge overlay	1649	172.16.49.0/24	172.16.49.253

Table 2-2. FQDNs and IP Addresses for the ESXi Hosts of the Workload Domain

ESXi Host FQDN	Management IP Address	NTP Server
sfo01w02esx01.sfo01.rainpole.local	172.16.41.101	ntp.sfo01.rainpole.local
sfo01w02esx02.sfo01.rainpole.local	172.16.41.102	ntp.sfo01.rainpole.local
sfo01w02esx03.sfo01.rainpole.local	172.16.41.103	ntp.sfo01.rainpole.local
sfo01w02esx04.sfo01.rainpole.local	172.16.41.104	ntp.sfo01.rainpole.local

Table 2-3. FQDN and IP Address of the Compute vCenter Server

vCenter Server FQDN	IP Address
sfo01w02vc01.sfo01.rainpole.local	172.16.11.67

Table 2-4. IP Addresses and Host Names for the NSX-T Components

Role	FQDN	IP Address
NSX-T Manager instances	sfo01wnsx01a.sfo01.rainpole.local	172.16.11.82
	sfo01wnsx01b.sfo01.rainpole.local	172.16.11.83
	sfo01wnsx01c.sfo01.rainpole.local	172.16.11.84
	sfo01wnsx01.sfo01.rainpole.local (VIP)	172.16.11.81
Edge Services Gateway 01	sfo01wesg01.sfo01.rainpole.local	172.16.41.21 (Management)
		172.16.49.21 (Overlay)
		172.16.47.2 (Uplink 1)
		172.16.48.2 (Uplink 2)
Edge Services Gateway 02	sfo01wesg02.sfo01.rainpole.local	172.16.41.22 (Management)
		172.16.49.22 (Overlay)
		172.16.47.3 (Uplink 1)
		172.16.48.3 (Uplink 2)
Subnet mask	-	255.255.255.0
DNS	-	172.16.11.5
		172.16.11.4
NTP Servers	ntp.sfo01.rainpole.local	■ 172.16.11.251 ■ 172.16.11.252

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the deployment.

Prerequisite	Value
Storage in the Management Cluster	■ Virtual disk provisioning: Thin ■ Required storage per NSX-T Manager: ■ Initial storage: 200 GB ■ Initial storage aggregated for all NSX-T Managers: 600 GB
Memory in the Management Cluster	■ Required memory per NSX-T Manger node ■ Required memory: 48 GB ■ Required memory aggregated for all NSX-T Manager nodes: 144 GB
Network Connectivity	Verify that routing is in place between the management IP subnets of the management cluster and the new workload domain.

Prerequisite	Value
Software Features	- Verify that the Management vCenter Server is operational. - Verify that the management cluster has vSphere DRS and vSphere HA enabled. - Verify that you have the Postman REST client installed in your Web browser.
Installation Packages	- Download the `.iso` image for ESXi and the vCenter Server Appliance. - Download the `.ova` file for the NSX-T Unified Appliance and NSX-T Edge Node.
Boot Media for the ESXi Installer	Create a bootable USB drive and upload the ESXi installer to it. See the *vSphere Installation and Setup* documentation.
Active Directory	- Verify that you have a parent Active Directory with the SDDC user roles configured for the rainpole.local domain.
Certificate Authority and Custom Signed Certificates	- Configure the root Active Directory domain controller as a certificate authority for the environment. - Download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility and generate the signed certificate for the NSX-T Manager instances. See VMware Knowledge Base article 2146215.
Access to the data center	Provide a Microsoft Windows virtual machine or physical server to provide connection to the data center and store software downloads. The host must be connected to the external network and to the ESXi management network.

Generate CA-Signed Certificates for the NSX-T Manager Nodes

By using the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`), generate certificates for the NSX-T Manager instances and cluster virtual IP that are signed by the Microsoft certificate authority (MSCA). You use these certificates for trusted communication between the NSX-T nodes and the other management components of the SDDC.

Procedure

1. Log in to a Windows host that has access to your data center.
2. Download the `CertGenVVD-`*`version`*`.zip` file from VMware Knowledge Base article 2146215 and extract the ZIP file to `C:\CertGenVVD-`*`version`*.
3. In the `C:\CertGenVVD-`*`version`* folder, open the `default.txt` file in a text editor.

4 Verify that the following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

5 In the `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder, create four text files named `sfo01wnsx01a.txt`, `sfo01wnsx01b.txt`, `sfo01wnsx01c.txt`, and `sfo01wnsx01.txt` with the following content.

File Name	File Content

sfo01wnsx01a.txt	[CERT]
	NAME=default
	ORG=default
	OU=default
	LOC=SFO
	ST=default
	CC=default
	CN=sfo01wnsx01a.sfo01.rainpole.local
	keysize=default
	[SAN]
	sfo01wnsx01a
	sfo01wnsx01a.sfo01.rainpole.local

sfo01wnsx01b.txt	[CERT]
	NAME=default
	ORG=default
	OU=default
	LOC=SFO
	ST=default
	CC=default
	CN=sfo01wnsx01b.sfo01.rainpole.local
	keysize=default
	[SAN]
	sfo01wnsx01b
	sfo01wnsx01b.sfo01.rainpole.local

File Name	File Content

sfo01wnsx01c.txt	[CERT]
	NAME=default
	ORG=default
	OU=default
	LOC=SFO
	ST=default
	CC=default
	CN=sfo01wnsx01c.sfo01.rainpole.local
	keysize=default
	[SAN]
	sfo01wnsx01c
	sfo01wnsx01c.sfo01.rainpole.local

sfo01wnsx01.txt	[CERT]
	NAME=default
	ORG=default
	OU=default
	LOC=SFO
	ST=default
	CC=default
	CN=sfo01wnsx01.sfo01.rainpole.local
	keysize=default
	[SAN]
	sfo01wnsx01
	sfo01wnsx01.sfo01.rainpole.local

6. To open a Windows PowerShell terminal as administrator, click **Start**, right-click Windows PowerShell, and select **More > Run as Administrator**.
7. Configure the PowerShell execution policy with the permissions required for running commands.

   ```
   Set-ExecutionPolicy Unrestricted
   ```

8. Verify if the `CertGenVVD` utility is configured for the generation.

   ```
   cd c:\CertGenVVD-version
   .\CertGenVVD-version.ps1 -validate
   ```

9. Generate the MCSA-signed certificate.

   ```
   .\CertGenVVD-version.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
   ```

10. Navigate to the `C:\CertGenVVD-`*`version`* folder and verify that the `SignedByMSCACerts` folder contains the certificates for the NSX-T Manager nodes and for the virtual IP of the cluster.

Install and Configure the ESXi Hosts for the Shared Edge and Compute Cluster

3

Start the deployment of the virtual infrastructure workload domain by installing and configuring the additional ESXi hosts in Region A. ESXi acts as a platform for the tenant workloads that use the software-defined networking capabilities of NSX-T.

Procedure

1 Install ESXi Interactively on All Hosts in the Shared Edge and Compute Cluster

  Install manually ESXi from a USB drive on the hosts of the workload domain.

2 Configure the Management Network on the Hosts for the Shared Edge and Compute Cluster

  After the initial boot of ESXi, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

Install ESXi Interactively on All Hosts in the Shared Edge and Compute Cluster

Install manually ESXi from a USB drive on the hosts of the workload domain.

Procedure

1 Power on the sfo01w02esx01.sfo01.rainpole.local host.

2 Mount the USB drive containing the ESXi `.iso` file and boot from that USB drive.

3 On the **Welcome to the VMware 6.7.0 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 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, and press Enter.

8 On the **Confirm Install** screen, press F11 to start the installation.

9 After the installation finishes, unmount the USB drive and press Enter to reboot the host.

10 Repeat this procedure for all hosts.

Configure the Management Network on the Hosts for the Shared Edge and Compute Cluster

After the initial boot of ESXi, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

On each host, perform the following tasks to configure the host network settings:

- Configure the VMkernel network adapter vmk0 and VLAN ID for the management network.
- Configure the IP address, subnet mask, gateway, DNS server, and FQDN for the ESXi host.

Repeat this procedure for all hosts in the shared edge and compute cluster.

Procedure

1 Open the DCUI on the physical ESXi host sfo01w02esx01.sfo01.rainpole.local.

  a Press F2 to enter the DCUI.

  b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Select **Configure Management Network** and press Enter.

3 Configure the VLAN ID of the management network.

  a On the **Configure Management Network** screen, select **VLAN (Optional)** and press Enter.

  b Enter **1641** as the VLAN ID for the management network and press Enter.

4 Configure the IPv4 settings of the host.

  a On the **Configure Management Network** screen, select **IPv4 Configuration** and press Enter.

  b Configure the IPv4 network by using the following settings and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.41.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.41.253

5. Configure the DNS settings of the host.
   a. On the **Configure Management Network** screen, select **DNS Configuration** and press Enter.
   b. Configure DNS on the host by 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	sfo01w02esx01.sfo01.rainpole.local

   c. On the **Configure Management Network** screen, select **Custom DNS Suffixes** and press Enter.
   d. Verify that the suffix list is empty and press Enter.
6. Press Escape to close the DCUI and press Y to confirm the changes.
7. Repeat this procedure on the other ESXi hosts.

Deploy and Configure the Shared Edge and Compute Cluster Components

4

Deploy and configure the shared edge and compute cluster components.

Procedure

1 Deploy the Compute vCenter Server Instance for the Shared Edge and Compute Cluster

   To manage and configure the ESXi hosts in the additional workload domain and to provision tenant workloads from a centralized node, you must install and configure vCenter Server on the management cluster of Region A. You connect this vCenter Server instance to the Platform Services Controller pair that is available in the region to take advantage of the high availability of and to join the single vCenter Single Sign-on domain configured on the pair.

2 Replace the Certificate of the Compute vCenter Server

   To establish a trusted connection to the other SDDC management components, you replace the default SSL certificate on the vCenter Server instance in the workload domain with a custom certificate that is signed by the certificate authority (CA) on the parent Active Directory (AD) server.

3 Set the SDDC Deployment Details on the Compute vCenter Server

   Update the identity of your SDDC deployment on the Compute vCenter Server in the workload domain. You can use this identity as a label in tools for automated SDDC deployment.

4 Add vSphere Licenses and Assign a License to the Compute vCenter Server

   Assign a license key to the Compute vCenter Server for the workload domain to use its features in production. If the capacity of the licenses for vCenter Server and ESXi is insufficient to license the new instances, add new licenses to the inventory of the License Service.

5 Add the Compute vCenter Server to the Virtual Machine Group for vCenter Server

   The Compute vCenter Server for the workload domain must be a member of the virtual machine group so that it is powered on, in a group with the other vCenter Server instances, after the Platform Services Controller pair. In this way, the services of the Platform Services Controller nodes are available to the Compute vCenter Server after a vSphere HA migration occurs.

6 Exclude the Compute vCenter Server from the Distributed Firewall

   To allow network access to the Compute vCenter Server for the workload domain, exclude it from all distributed firewall rules.

7 Configure the Shared Edge and Compute Cluster

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster for high availability of and resource usage policy for virtual machines, and for central user management using Active Directory.

8 Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster

After you add all ESXi hosts in the workload domain to the cluster, you can create the vSphere Distributed Switch for the system traffic. This switch handles traffic until you migrate the hosts to the N-VDS instance for the cluster.

9 Enable vSphere HA on the Shared Edge and Compute Cluster

vSphere High Availability protects virtual machines hardware and operating system outages.

10 Configure SSH, NTP, and Advanced Options on the First ESXi Host in the Shared Edge and Compute Cluster

Time synchronization issues can result in serious problems with your environment. Configure the Network Time Protocol (NTP) settings on each of your ESXi hosts in the shared edge and compute clusters. To achieve greater levels of security, change the default ESX Admins group and remove a known administrative access point.

11 Configure Syslog on the Shared Edge and Compute Cluster

To maintain centralized logging, enable the syslog service on the ESXi hosts in the shared edge and compute cluster . The syslog service provides a standard mechanism for logging messages from the VMkernel and other system components.

12 Create and Apply the Host Profile for the Shared Edge and Compute Cluster

Host Profiles maintain configuration consistency and correctness across your shared edge and compute cluster.

13 Use the UMDS Shared Repository as the Download Source in Update Manager

Configure Update Manager to use the vSphere Update Manager Download Service (UMDS) shared repository as a centralized source for downloading ESXi patches, extensions, and notifications.

Deploy the Compute vCenter Server Instance for the Shared Edge and Compute Cluster

To manage and configure the ESXi hosts in the additional workload domain and to provision tenant workloads from a centralized node, you must install and configure vCenter Server on the management cluster of Region A. You connect this vCenter Server instance to the Platform Services Controller pair that is available in the region to take advantage of the high availability of and to join the single vCenter Single Sign-on domain configured on the pair.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 To be able to deploy another vCenter Server instance, disable the lockdown mode on the sfo01m01esx01.sfo01.rainpole.local ESXi host in the management cluster.

   a In the **Navigator**, click **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Under the **sfo01-m01-mgmt01** cluster, select **sfo01m01esx01.sfo01.rainpole.local** and click the **Configure** tab.

   c Under the **System** section, select **Security Profile** and click **Edit** .

   d In the **sfo01m01esx01.sfo01.rainpole.local-Lockdown Mode** dialog box, select **Disabled** and click **OK**.

3 Start the **vCenter Server Appliance Deployment** wizard.

   a Browse to the `.iso` file of the vCenter Server Appliance.

   b Run the *`dvd-drive`*`:\vcsa-ui-installer\win32\Installer.exe` application file.

4 To perform the first stage of the installation, complete the **vCenter Server Appliance Deployment** wizard.

   a Click **Install**.

   b On the **Introduction** page, click **Next** .

   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**, select the **vCenter Server (Requires External Platform Services Controller)** radio button 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	sfo01m01vc01.sfo01.rainpole.local
HTTPS Port	443
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

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

g On the **Select folder** page, select **sfo01-m01fd-mgmt** and click **Next**.

h On the **Select compute resource** page, select the **sfo01m01esx01.sfo01.rainpole.local** host and click **Next**.

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

Setting	Value
VM name	sfo01w02vc01
Root password	*compvc_root_password*
Confirm root password	*compvc_root_password*

j On the **Select deployment size** page, select **Large vCenter Server** and click **Next**.

k On the **Select datastore** page, select the **sfo01-m01-vsan01** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.

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

Setting	Value
Network	sfo01-m01-vds01-management
IP version	IPv4
IP assignment	static
FQDN	sfo01w02vc01.sfo01.rainpole.local
IP Address	172.16.11.67
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
HTTP	80
HTTPS	443

m On the **Ready to complete stage 1** page, review the configuration and click **Finish**.

The deployment is started.

n After the deployment finishes, to proceed to the second stage of the installation, click **Continue** .

5 Complete the **Install - Stage 2: Set Up vCenter Server Appliance** wizard to complete the second stage of the installation.

   a On the **Introduction** page, click **Next**.

   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	sfo01psc01.sfo01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	*sso_password*

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

   e In the **Warning** dialog box, click **OK**.

   f On the **Complete** page, click **Close**.

6 Enable lockdown mode on sfo01m01esx01.sfo01.rainpole.local.

   a Back in the vSphere Client, expand the **sfo01-m01-mgmt01** cluster.

   b Select **sfo01m01esx01.sfo01.rainpole.local** and click the **Configure** tab.

   c Under the **System** section, select **Security Profile** and click **Edit** .

   d In the **sfo01m01esx01.sfo01.rainpole.local-Lockdown Mode** dialog box, select **Normal** and click **OK**.

Replace the Certificate of the Compute vCenter Server

To establish a trusted connection to the other SDDC management components, you replace the default SSL certificate on the vCenter Server instance in the workload domain with a custom certificate that is signed by the certificate authority (CA) on the parent Active Directory (AD) server.

Use the following certificate files to replace the certificate on the Compute vCenter Server:

Table 4-1. Certificate-Related Files on the vCenter Server Instance

vCenter Server FQDN	Files for Certificate Replacement
sfo01w02vc01.sfo01.rainpole.local	■ sfo01w02vc01.1.key ■ sfo01w02vc01.1.cer ■ Root64.cer

Procedure

1 Log in to vCenter Server by using Secure Shell (SSH) client.

  a Open an SSH connection to the sfo01w02vc01.sfo01.rainpole.local virtual machine.

  b Log in by using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 To enable secure copy (`scp`) connections for the **root** user, switch from the appliance shell to the Bash shell.

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

3 Copy the certificates that you generated by using the `CertGenVVD` utility 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 `sfo01w02vc01.1.cer`, `sfo01w02vc01.key`, and `Root64.cer` to the `/root/certs` folder.

  You can use an `scp` software such as WinSCP.

4 Replace the CA-signed certificate on the vCenter Server instance.

  a Run 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 ***`vsphere_admin_password`***.

c When prompted for the Infrastructure Server IP, enter the VIP address of the Platform Services Controller pair in Region A.

Setting	Value
Infrastructure server IP	172.16.11.71

d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.

e When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that you copied over earlier, and confirm the import with **Yes (Y)**.

Setting	Value
Custom certificate for Machine SSL	/root/certs/sfo01w02vc01.1.cer
Custom key for Machine SSL	/root/certs/sfo01w02vc01.key
Signing certificate of the Machine SSL certificate	/root/certs/Root64.cer

5 After the status is `100% Completed`, wait several minutes until all vCenter Server services are restarted.

6 Restart the vami-lighttp service to update the certificate on the virtual appliance management interface (VAMI) and to remove the certificate files.

```
service vami-lighttp restart
cd /root/certs/
rm sfo01w02vc01.1.cer sfo01w02vc01.key Root64.cer
```

Set the SDDC Deployment Details on the Compute vCenter Server

Update the identity of your SDDC deployment on the Compute vCenter Server in the workload domain. You can use this identity as a label in tools for automated SDDC deployment.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters**.

3 In the inventory tree, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab.

4 Under the **Settings** section, select **Advanced Settings**.

5 Locate the `config.SDDC.Deployed.InstanceId` setting and write down its value.

6 In the **Hosts and Clusters** inventory tree, select the **sfo01w02vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab.

7 Under the **Settings** section, select **Advanced Settings** and click **Edit**.

8 In the **Edit Advanced vCenter Server Settings** dialog box, set the following value pairs one by one, clicking **Add** after each entry, and click **OK**.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	5.0
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	Value obtained in Step 5.

Add vSphere Licenses and Assign a License to the Compute vCenter Server

Assign a license key to the Compute vCenter Server for the workload domain to use its features in production. If the capacity of the licenses for vCenter Server and ESXi is insufficient to license the new instances, add new licenses to the inventory of the License Service.

You assign the host license to the ESXi hosts when you add them to the workload domain.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Menu** menu, select **Administration**.

3 On the **Administration** page, select **Licenses**.

4 If the capacity of the available licenses is not sufficient to license the nodes of the workload domain, add the licenses to the inventory of the License Service.

   a On the **Licenses** tab, click**Add New Licenses**.

   b On the **Enter license keys** page, enter the license keys for vCenter Server and ESXi on separate lines, and click **Next**.

   c On the **Edit license name** page, enter a descriptive name for the license key, and click **Next**.

   d On the **Ready to complete** page, review your entries, and click **Finish**.

5 Assign the licenses to the Compute vCenter Server for the workload domain.

   a Click the **Assets** tab and click **vCenter Server systems**.

   b Select the **sfo01w02vc01.sfo01.rainpole.local** vCenter Server instance, and click the **Assign License** icon.

   c Select the license for the Compute vCenter Server and click **OK**.

Add the Compute vCenter Server to the Virtual Machine Group for vCenter Server

The Compute vCenter Server for the workload domain must be a member of the virtual machine group so that it is powered on, in a group with the other vCenter Server instances, after the Platform Services Controller pair. In this way, the services of the Platform Services Controller nodes are available to the Compute vCenter Server after a vSphere HA migration occurs.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Home** menu, select **Hosts and Clusters**.

3 In the inventory tree, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

4 Select the **sfo01-m01-mgmt01** cluster and click **Configure**.

5 On the **Configure** page, click **VM/Host Groups**.

6 On the **VM/Host Groups** page, select the **vCenter Servers** VM Group.

7 In the **vCenter Servers Group Members** pane, click **Add**.

8 In the **Add Group Member** dialog box, select **sfo01w02vc01** and click **OK**.

Exclude the Compute vCenter Server from the Distributed Firewall

To allow network access to the Compute vCenter Server for the workload domain, exclude it from all distributed firewall rules.

Procedure

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.
   b. Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2. Click **Menu** and select **Networking and Security**.
3. Click **Firewall Settings** and select the **Exclusion List** tab.
4. Select **172.16.11.65** from the **NSX Manager** drop-down menu.
5. Click the **Add** button.
6. Add sfo01w02vc01 to the **Selected Objects** list, and click **OK**.

Configure the Shared Edge and Compute Cluster

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster for high availability of and resource usage policy for virtual machines, and for central user management using Active Directory.

To create and configure the shared edge and compute cluster, you perform the following tasks:

- Create the cluster.
- Configure vSphere HA and vSphere DRS.
- Add the ESXi hosts to the cluster.
- Add the ESXi hosts to the Active Directory domain.
- Create resource pools for the NSX-T edge devices and for the tenant workloads.
- Create folders for the virtual appliances of the NSX-T Edge devices for inbound and outbound network traffic in the workload domain.

Procedure

1. Log in to vCenter Server by using the vSphere Client.

   a. Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b. Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2. Create a data center object.

   a. From the **Home** menu, select **Hosts and Clusters**.

   b. In the inventory tree, right-click the **sfo01w02vc01.sfo01.rainpole.local** vCenter Server instance and select **New Datacenter**.

   c. In the **New Datacenter** dialog box, enter `sfo01-w02dc` and click **OK**.

3. Create the shared edge and compute cluster.

   a. In the inventory tree, right-click the **sfo01-w02dc** data center and select **New Cluster**.

   b. In the **New Cluster** wizard, enter the following values and click **OK**.

Setting		Value
Name		sfo01-w02-shared01
DRS	**Turn ON**	Selected
	Other DRS options	Default values
vSphere HA	**Turn ON**	Deselected
EVC		Set the EVC mode to the highest available baseline that is supported for the lowest CPU architecture on the hosts in the cluster
vSAN	**Turn ON**	Deselected

4 Add the ESXi hosts to the shared edge and compute cluster.

a Right-click the **sfo01-w02-shared01** cluster, and select **Add Hosts**.

b On the **Add hosts** page, select **Use same credentials for all hosts**, enter the following information, and click **Next**.

IP Address or FQDN	Username	Password
`sfo01w02esx01.sfo01.rainpole.local`	root	*esxi_root_user_password*
`sfo01w02esx02.sfo01.rainpole.local`	-	-
`sfo01w02esx03.sfo01.rainpole.local`	-	-
`sfo01w02esx04.sfo01.rainpole.local`	-	-

c In the **Security Alert** dialog box, select all ESXi hosts, and, to confirm the validity of the host certificates, click **OK** .

A trusted connection between vCenter Server and the ESXi hosts is established using the host certificates for SSL handshake.

d On the **Host summary page**, review the host information and click **Next**.

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

f On the **Hosts** tab for the cluster, select all ESXi hosts, right-click, and select **Maintenance Mode > Exit Maintenance Mode**.

g Select all ESXi hosts, right-click, select **Assign License**, select the ESXi license from the inventory of the License Service, and click **OK**.

5 Add an ESXi host to the Active Directory domain

a In the inventory tree, expand the entire **sfo01w02vc01.sfo01.rainpole.local** tree.

b Select the **sfo01w02esx01.sfo01.rainpole.local** host.

c On the **Configure** tab, under **System**, select **Authentication Services**.

d On the **Authentication Services** page, click the **Join Domain** button.

e In the **Join Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	sfo01.rainpole.local
User name	svc-domain-join@rainpole.local
Password	*svc-domain-join_password*

6 Set the Active Directory service to start and stop with host.

   a On the **Configure** tab for the host, under **System**, select **Services**.

   b Select the **Active Directory** service, click **Edit Startup Policy**, select **Start and stop with host**, and click **OK**.

7 Create the resource pools for the shared edge and compute cluster.

   You create resource pools for the following components:

   - NSX-T Edge devices that control the network traffic in and out of the workload domain
   - Tenant workloads in the workload domain
   - NSX-T Edge devices that provide networking services to the tenant workloads in the workload domain

   a Right-click the **sfo01-w02-shared01** cluster and select **New Resource Pool**.

   b In the **New Resource Pool** dialog box, enter the values for the sfo01-w02rp-sddc-edge resource pool and click **OK**.

Setting	Resource Pool 1	Resource Pool 2	Resource Pool 3
Name	sfo01-w02rp-sddc-edge	sfo01-w02rp-user-edge	sfo01-w02rp-user-vm
CPU-Shares	High	Normal	Normal
CPU-Reservation	0	0	0
CPU-Reservation Type	Expandable selected	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited	Unlimited
Memory-Shares	Normal	Normal	Normal
Memory-Reservation	32 GB	0	0
Memory-Reservation type	Expandable selected	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited	Unlimited

   c Repeat the step to add the remaining resource pools.

8 Create a folder for the virtual machines of the NSX-T Edge devices for the inbound and outbound traffic in the workload domain.

   a From the **Home** menu, select **VMs and Templates**.

   b In the inventory tree, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

   c Right-click the **sfo01-w02dc** data center and select **New Folder > New VM and Template Folder**.

   d In the **New Folder** dialog box, enter **`sfo01–w02fd–nsx`** and click **OK**.

Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster

After you add all ESXi hosts in the workload domain to the cluster, you can create the vSphere Distributed Switch for the system traffic. This switch handles traffic until you migrate the hosts to the N-VDS instance for the cluster.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create a vSphere Distributed Switch for the shared edge and compute cluster.

   a From the **Home** menu, select **Networking**.

   b In the inventory tree, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

   c Right-click the **sfo01-w02dc** data center and select **Distributed Switch > New Distributed Switch**.

   The **New Distributed Switch** wizard appears.

   d On the **Name and location** page, enter `sfo01-w02-vds01` as the name and click **Next**.

   e On the **Select version** page, verify that the **Distributed switch version: 6.6.0** radio button is selected and click **Next**.

   f On the **Configure 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

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

3 Enable jumbo frames on the sfo01-w02-vds01 distributed switch.

   a Right-click the **sfo01-w02-vds01** distributed switch and select **Settings > Edit Settings**.

   b On the **Advanced** tab, enter `9000` as **MTU (Bytes)** value and click **OK**.

4 Create the port groups for the system traffic on the sfo01-w02-vds01 distributed switch.

   a Right-click the **sfo01-w02-vds01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.

   b Create the sfo01-w02-vds01-management port group with the following settings and click **Next**.

Port Group Name	Port Binding	Port Allocation	Number of Ports	VLAN Type	VLAN ID
sfo01-w02-vds01-management	Ephemeral	Elastic	8	VLAN	1641
sfo01-w02-vds01-vmotion	Ephemeral	Elastic	8	VLAN	1642
sfo01-w02-vds01-vsan	Ephemeral	Elastic	8	VLAN	1643
sfo01-w02-vds01-nfs	Ephemeral	Elastic	8	VLAN	1625

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

   d Repeat this step for the other port groups.

5 Connect the sfo01w02esx01.sfo01.rainpole.local ESXi host to the sfo01-w02-vds01 distributed switch.

   a Right-click the **sfo01-w02-vds01** distributed switch, and select **Add and Manage Hosts**.

   The **Add and Manage Hosts** wizard appears.

   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 **sfo01w02esx01.sfo01.rainpole.local**, click **OK**, and click **Next**.

   e On the **Manage physical network adapters** page, click **vmnic1**, and click **Assign uplink**.

   f In the **Select an Uplink for vmnic1** dialog box, select **Uplink2** and click **OK**.

   g On the **Manage physical network adapters** page, click **Next**.

6 Configure the VMkernel network adapters.

   a On the **Manage VMkernel network adapters** page, click **vmk0** and click **Assign port group**.

   b Select **sfo01-w02-vds01-management** and click **OK**.

   c On the **Manage VMkernel network adapters** page, click **Next**.

   d On the **Migrate VM Networking** page, click **Next**.

   e On the **Analyze impact** page, click **Next**.

   f On the **Ready to complete** page, review your entries and click **Finish**.

7 Create additional VMkernel network adapters.

   a From the **Home** menu, select **Hosts and Clusters**.

   b In the inventory tree, expand the **sfo01w02vc01.sfo01.rainpole.local** tree

   c Select the **sfo01w02esx01.sfo01.rainpole.local** host.

d On the **Configure** tab, click **VMkernel adapters**.

e Click the **Add Networking** button and select **VMKernel Network Adapter** and click **Next**.

f On the **Select target device** page, click **Select an existing network**, select the **sfo01-w02-vds01-vmotion** port group, click **OK**, and click **Next**.

g On the **Port properties** page, select **vMotion** from the **TCP/IP stack** drop-down menu and click **Next**.

h On the **IPv4 settings** page, configure the following settings and click **Next**.

Setting	Value
Use static IPv4 settings	Selected
IPv4 address	172.16.42.101
Subnet mask	255.255.255.0

i Click **Finish**.

8 Configure the vMotion TCP/IP stack.

a Under **Networking** , click **TCP/IP configuration.**

b Select **vMotion** and click the **Edit** icon.

c On the **Routing** page, enter `172.16.42.253` for the **VMkernel gateway**, and click **OK**.

9 Migrate the last physical adapter from the standard switch to the sfo01-w02-vds01 distributed switch.

a Select **sfo01w02esx02.sfo01.rainpole.local** ESXi host.

b On the **Configure** tab, click **Virtual Switches** and expand **vSwitch0**.

c From the ellipsis menu, select **Remove** and click **Yes** in the **Remove Standard Switch** warning dialog box.

d Expand **sfo01-w02-vds01** and click **Manage Physical Adapters**.

e In the **Uplink ports** pane, click the **Add** button, select **vmnic0**, click **OK**, and click **OK** again.

Enable vSphere HA on the Shared Edge and Compute Cluster

vSphere High Availability protects virtual machines hardware and operating system outages.

Procedure

1. Log in to vCenter Server by using the vSphere Client.

   a. Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b. Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2. In the **Hosts and Clusters** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

3. Select the **sfo01-w02-shared01** cluster.

4. On the **Configure** tab, select **Services > vSphere Availability** .

5. Click **Edit**.

6. In the **Edit Cluster Settings** dialog box, enable **vSphere HA**.

7. On the **Failures and responses** tab, configure the following settings.

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

8. On the **Admission Control**tab, configure the following settings and click **OK**.

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%

Configure SSH, NTP, and Advanced Options on the First ESXi Host in the Shared Edge and Compute Cluster

Time synchronization issues can result in serious problems with your environment. Configure the Network Time Protocol (NTP) settings on each of your ESXi hosts in the shared edge and compute clusters. To achieve greater levels of security, change the default ESX Admins group and remove a known administrative access point.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

  a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

  b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Enable SSH.

  a In the **Hosts and Clusters** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

  b Select the **sfo01w02esx01.sfo01.rainpole.local** host.

  c On the **Configure** tab, select **System > Services**.

  d Select **SSH** and click the **Start** button.

  e Click the **Edit Startup Policy** button, select **Start and stop with host**, and click **OK**.

3 Configure the NTP Daemon (ntpd) options.

  a On the **Configure** tab, select **System > Time Configuration**.

  b Click **Edit**.

  c In the **Edit Time Configuration** dialog box, configure the following settings and click **OK**.

Setting	Value
Use Network Time Protocol (Enable NTP client)	Selected
NTP Servers	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local
Start NTP Service	Selected
NTP Service Startup Policy	Start and stop with host

4 Change the default ESX Admins group.

  a On the **Configure** tab, select **System > Advanced System Settings**.

  b Click **Edit**.

  c In the **Filter** text box, enter **`esxAdmins`**.

  d Change the value of `Config.HostAgent.plugins.hostsvc.esxAdminsGroup` to **`SDDC-Admins`** .

5 Disable the SSH warning banner.

  a In the **Filter** text box, enter **`ssh`**.

  b Change the value of `UserVars.SuppressShellWarning` to **1** and click **OK**.

Configure Syslog on the Shared Edge and Compute Cluster

To maintain centralized logging, enable the syslog service on the ESXi hosts in the shared edge and compute cluster . The syslog service provides a standard mechanism for logging messages from the VMkernel and other system components.

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 by using the following credentials.

Setting	Value
User name	admin
Password	*deployment_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 the vCenter Server instance.

  a Enter the host name, user credentials, and collection options for the vCenter Server instance, and click **Test Connection**.

vCenter Server Option	Value
Hostname	sfo01w02vc01.sfo01.rainpole.local
Password	*svc-vrli-vsphere_user_password*
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected
Target	sfo01vrli01.sfo01.rainpole.local

  b To verify that you connect to the correct vCenter Server, click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance.

  c In the **Advanced Options** configuration window, select **Configure all ESXi hosts**, select **UDP** under **Syslog protocol**, and click **OK**.

Create and Apply the Host Profile for the Shared Edge and Compute Cluster

Host Profiles maintain configuration consistency and correctness across your shared edge and compute cluster.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create a host profile from the sfo01w02esx01.sfo01.rainpole.local ESXi host.

   a In the **Hosts and Clusters** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

   b Right-click the **sfo01w02esx01.sfo01.rainpole.local** ESXi host and select **Host Profiles > Extract Host Profile**.

   c In the **Extract Host Profile** dialog box, enter **`sfo01-w02hp-shared01`** in the **Name** text box and click **OK**.

3 Attach the host profile to the shared edge and compute cluster.

   a Right-click the **sfo01-w02-shared01** cluster and select **Host Profiles > Attach Host Profile**.

   b In the **Attach Host Profile** dialog box, select the **sfo01-w02hp-shared01** host profile, and click **OK**.

4 Export a host customization specification for the hosts in the shared edge and compute cluster.

   a Right-click the **sfo01-w02-shared01** cluster and select **Host Profiles > Export Host Customizations**

   b In the **Export Host Customizations** dialog box, click **Save**.

   The `sfo01-w02hp-shared01_host_customizations.csv` file is downloaded.

   c Open the `sfo01-w02hp-shared01_host_customizations.csv` file in Excel.

d Edit the host customization file using these configuration values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
sfo01w02esx01.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo01w02esx01
sfo01w02esx02.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo01w02esx02
sfo01w02esx03.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo01w02esx03
sfo01w02esx04.sfo01.rainpole.local	*svc-domain-join_password*	svc-domain-join@rainpole.local	sfo01w02esx04

ESXi Host	Host virtual NIC sfo01-w02-vds01:sfo01-w02-vds01-management:management->IP address settings IPv4 address	Host virtual NIC sfo01-w02-vds01:sfo01-w01-vds01-management:management->IP address settings SubnetMask
sfo01w02esx01.sfo01.rainpole.local	172.16.41.101	255.255.255.0
sfo01w02esx02.sfo01.rainpole.local	172.16.41.102	255.255.255.0
sfo01w02esx03.sfo01.rainpole.local	172.16.41.103	255.255.255.0
sfo01w02esx04.sfo01.rainpole.local	172.16.41.104	255.255.255.0

ESXi Host	Host virtual NIC sfo01-w02-vds01:sfo01-w02-vds01-vmotion:vmotion->IP address settings IPv4 address	Host virtual NICsfo01-w02-vds01:sfo01-w02-vds01-vmotion:vmotion->IP address settings SubnetMask
sfo01w02esx01.sfo01.rainpole.local	172.16.42.101	255.255.255.0
sfo01w02esx02.sfo01.rainpole.local	172.16.42.102	255.255.255.0
sfo01w02esx03.sfo01.rainpole.local	172.16.42.103	255.255.255.0
sfo01w02esx04.sfo01.rainpole.local	172.16.42.104	255.255.255.0

e Right-click the **sfo01-w02-shared01** cluster and select **Host Profiles > Export Host Customizations**.

The **Edit Host Customizations** wizard appears.

f In the **Select hosts** dialog box, select all ESXi hosts and click **Next**

g Click **Import Host Customizations**, navigate to the `sfo01–w02hp–shared01_host_customizations.csv` file, click **Open**, and click **Finish**.

5 Remediate the ESXi hosts in the shared edge and compute cluster.

   a Navigate to the **Policies and Profiles** view and click **Host Profiles**.

   b Click the **sfo01-w02hp-shared01** host profile, click the **Monitor** tab, and click **Check Compliance**.

   The compliance test shows the first host as `Compliant` and the remaining hosts as `Not Compliant`.

   c Click **Remediate**, select all non-compliant ESXi hosts from the list and click **Remediate**.

   All hosts now have `Compliant` status in the **Host Profile Compliance** column.

6 Remove the sfo01-w02hp-shared01 host profile from the shared edge and compute cluster.

   You must remove the host profile because Host Profiles are not compatible with NSX-T .

   a In the **Hosts and Clusters** inventory, right-click the **sfo01-w02-shared01** cluster and select **Host Profiles > Detach**.

   b In the **Detach profile** dialog box click **Yes**.

Use the UMDS Shared Repository as the Download Source in Update Manager

Configure Update Manager to use the vSphere Update Manager Download Service (UMDS) shared repository as a centralized source for downloading ESXi patches, extensions, and notifications.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Menu**, select **Update Manager**.

3 Select **sfo01w02vc01.sfo01.rainpole.local** from the drop-down menu.

4 Click **Settings** and select **Administration Settings > Patch Setup**.

5 Click **Change Download Source** and select **Download patches from a UMDS shared repository**.

6 In the **Url** text box, enter **`https://sfo01umds01.sfo01.rainpole.local`** and click **Save**.

7 Click the **Updates** tab and click **Download Now**.

   A new task `Download patch definitions` with a `Completed` status appears in the **Recent Tasks** pane.

Deploy the NSX-T Instance for the Shared Edge and Compute Cluster

5

NSX-T Manager implements both the management and central control planes in an NSX-T system. For dynamic routing between the tenant workloads in the domain, you deploy a pair of NSX-T Edge nodes.

NSX-T Manager also provides the user interface and REST APIs for creating, configuring, and monitoring NSX-T components in a workload domain, such as segments, gateways, and security policies.

For high availability of the management and control planes, you deploy a cluster of three NSX-T Manager nodes.

1. Deploy the First NSX-T Manager Appliance

   To create a cluster of NSX-T Manager nodes, first you deploy one NSX-T Manager appliance and configure it. After you complete the configuration of the first node, you add the other two nodes of the cluster.

2. Import the CA-Signed Certificates for the NSX-T Manager Cluster

   After you deploy the first NSX-T Manager appliance and you generate the certificates for each NSX-T Manager node and for the virtual IP address of the cluster, import the certificates in to the appliance by using the NSX-T Manager user interface. Later, you replace the certificate on each node.

3. Replace the Certificate for the First NSX-T Manager Appliance

   After you deploy the first NSX-T Manager appliance, replace its default certificate to establish a trusted connection with the management components in the SDDC. You replace the existing certificates using the REST API of NSX-T Manager.

4. Connect NSX-T Manager to the vCenter Server Instances

   Connect the first NSX-T Manager appliance to the Compute vCenter Server for the workload domain so that tenant workloads can use NSX-T networking components and to Management vCenter Server so that you can place the remaining NSX-T Manager nodes on the management cluster later.

5. Deploy the Remaining Nodes of the NSX-T Manager Cluster

   To start implementing high availability of NSX-T Manager, deploy the remaining two nodes of the NSX-T Manager cluster on the management cluster.

6. Create an Anti-Affinity Rule for the NSX-T Manager Appliances

   Create a VM-Host anti-affinity rule to ensure that the NSX-T Manager virtual machines run on different ESXi hosts. If an ESXi host is unavailable, the NSX-T Manager virtual machines on the other hosts continue to provide support for the NSX-T management and control planes.

7 Move the NSX-T Manager Appliances to the NSX Folder

After you deploy the remaining appliances of the NSX-T Manager cluster, move them to the virtual machine folder for NSX and NSX-T.

8 Replace the Certificates for the Remaining NSX-T Manager Appliances

After you deploy the remaining NSX-T Manager appliances, replace the default certificate for them to establish a trusted connection with the management components in the SDDC. To replace the certificate for an NSX-T Manager instance, you import the certificates through the NSX-T Manager user interface and replace the existing certificates using a REST API client.

9 Assign a Virtual IP Address and Certificate to the NSX-T Manager Cluster

After you deploy all three NSX-T Manager nodes, assign the virtual IP (VIP) address of the NSX-T Manager cluster and assign a certificate for the VIP address for trusted access to the user interface and API.

10 Assign a License to NSX-T

By using the user interface of NSX-T Manager, replace the evaluation license for NSX-T with a production one.

11 Create the Transport Zones for System and Overlay Traffic

After you deploy the NSX-T Manager cluster, configure the NSX-T logical networks by creating the transport zones for ESXi management, uplink, and overlay traffic.

12 Create Uplink Profiles and the Network I/O Control Profile

Uplink profiles define the policies for the links from ESXi hosts to NSX-T segments or from NSX Edge nodes to top of rack switches. During network contention Network I/O Control allocates bandwidth to a system traffic type according to priority of the traffic.

13 Create the NSX-T Segments for System, Uplink, and Overlay Traffic

Create the segments to connect nodes that send VLAN and overlay traffic.

14 Create a Transport Node Profile

Create a transport node profile for the ESXi management and overlay traffic to and from the ESXi hosts in the workload domain. By using this profile, all hosts in the domain have the same transport node configuration.

15 Configure the ESXi Host Transport Nodes

To use NSX-T, configure the ESXi hosts in the shared edge and compute cluster as transport nodes. As a result, the NSX-T Manager installs the NSX-T kernel modules on the hosts as VIB files.

16 Remove the ESXi Hosts for the vSphere Distributed Switch

After you configure the ESXi hosts in the shared edge and compute cluster as transport nodes, the NSX-T infrastructure starts handling the system and virtual machine traffic to the hosts. You can remove the hosts from the vSphere Distributed Switch.

17 Configure Dynamic Routing in the Shared Edge and Compute Cluster

   To support the communication between tenant workloads by using application virtual networks in NSX-T and to connect tenant workloads to the external network, configure dynamic routing in the shared edge and compute cluster.

18 Deploy a Segment for a Sample Tenant Workload

   You create logical segments and connect them to the Tier-1 gateway for your tenant workloads. For example, you can create a segment for Ubuntu workloads and connect it to the Tier-1 gateway.

Deploy the First NSX-T Manager Appliance

To create a cluster of NSX-T Manager nodes, first you deploy one NSX-T Manager appliance and configure it. After you complete the configuration of the first node, you add the other two nodes of the cluster.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In **Hosts and Clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Right-click the **sfo01-m01-mgmt01** cluster and click **Deploy OVF Template**.

4 On the **Select template** page, navigate to the `.ova` file of the NSX-T unified appliance, and click **Next**.

5 On the **Select name and location** page, enter the following settings and click **Next**.

Setting	Value
Name	sfo01wnsx01a
Folder or data center	sfo01-m01fd-nsx

6 On the **Select a resource** page, select the **sfo01-m01-mgmt01** cluster and click **Next**.

7 On the **Review details** page, review the **extra configuration option** message and click **Next**.

8 On the **Select Configuration** page, select **Large** and click **Next.**

9 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-m01-vsan01

10 On the **Select networks** page, select **sfo01-m01-vds01-management** as the **Destination Network** and click **Next.**

11 On the **Customize template** page, enter the following settings, and click **Next.**

Setting	Value
System Root User Password / Confirm Password	*nsx_t_root_password*
CLI "admin" User Password / Confirm Password	*nsx_t_admin_password*
CLI "audit" User Password / Confirm Password	*nsx_t_audit_password*

Setting	Value
Host name	sfo01wnsx01a.sfo01.rainpole.local
Role name	nsx-manager nsx-controller
Default IPv4 Gateway	172.16.11.253
Management Network IPv4 Address	172.16.11.82
Management Network Netmask	255.255.255.0

Setting	Value
DNS Server List	172.16.11.5 172.16.11.4
Domain Search List	sfo01.rainpole.local
NTP Server List	ntp.sfo01.rainpole.local
Enable SSH	Selected
Allow root SSH login	Deselected

12 On the **Ready to complete** page, click **Finish**.

13 After the deployment is complete, power on the NSX-T Manager appliance.

a In the **VMs and Templates** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

b Expand the **sfo01-m01fd-nsx** folder.

c Right-click the **sfo01wnsx01a** virtual machine, and select **Power > Power On**.

14 Log in to the user interface of the first NSX-T Manager appliance.

   a Open a Web browser and go to **`https://sfo01wnsx01a.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

15 Accept the end-user license agreement and click **Continue**.

16 Join the VMware Customer Experience Program and click **Save**.

17 Close the alert stating the management cluster is degraded.

Import the CA-Signed Certificates for the NSX-T Manager Cluster

After you deploy the first NSX-T Manager appliance and you generate the certificates for each NSX-T Manager node and for the virtual IP address of the cluster, import the certificates in to the appliance by using the NSX-T Manager user interface. Later, you replace the certificate on each node.

Table 5-1.

Setting	Value for sfo01wnsx01a	Value for sfo01wnsx01b	Value for sfo01wnsx01c	Value for the Cluster Virtual IP	Value for the CA Certificate
Name	sfo01wnsx01a	sfo01wnsx01b	sfo01wnsx01c	sfo01wnsx01	Rainpole Root CA
Certificate Contents	sfo01wnsx01a.1.cer	sfo01wnsx01b.1.cer	sfo01wnsx01c.1.cer	sfo01wnsx01.1.cer	Root64.cer
Private Key	sfo01wnsx01a.key	sfo01wnsx01b.key	sfo01wnsx01c.key	sfo01wnsx01.key	N/A
Password	*certificate_password*	*certificate_password*	*certificate_password*	*certificate_password*	*certificate_password*
Confirm Password	*certificate_password*	*certificate_password*	*certificate_password*	*certificate_password*	*certificate_password*
Service Certificate	No	No	No	Yes	No

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

   a Open a Web browser and go to **`https://sfo01wnsx01a.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Import the certificates for the NSX-T Manager appliances and for the virtual IP address of the cluster, and the CA certificate.

   a In the **Navigator**, click **System > Certificates**.

   b Click **Import > Import Certificate** or **Import > Import CA Certificate** according to the type of certificate being imported.

   c Enter the following values and click **Import**.

   d Repeat this step to import all NSX-T Manager and CA Certificates.

3 On the main navigation bar, click **System**.

4 In the navigation pane, select **Certificates**.

5 Select **Import > Import Certificate** and import the certificate for the first NSX-T Manager appliance.

6 Repeat the step to import the certificates for the other NSX-T Manager appliances and for the virtual IP of the cluster.

7 Select **Import > Import CA Certificate** and import the certificate of the CA on the Active Directory domain.

Replace the Certificate for the First NSX-T Manager Appliance

After you deploy the first NSX-T Manager appliance, replace its default certificate to establish a trusted connection with the management components in the SDDC. You replace the existing certificates using the REST API of NSX-T Manager.

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

   a Open a Web browser and go to `https://sfo01wnsx01a.sfo01.rainpole.local`.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Retrieve the ID of the certificate.

   a On the main navigation bar, click **System**.

   b In the navigation pane, select **Certificates**.

   c Click the **ID** value of the sfo01wnsx01a certificate and copy it from the text box.

3 Log in to the Windows host that has access to your data center.

4 Replace the default certificate on the NSX-T Manager appliance with the CA-signed certificate.

   a Start the Postman application in your Web browser and log in.

   b On the **Authorization** tab, enter the following settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	*nsx_admin_password*

   c On the **Headers** tab, add a key by using the following details.

Setting	Value
Key	Content-Type
Key Value	application/xml

   d In the request pane at the top, from the drop-down menu that contains the HTTP request methods, select **POST**, and in the **URL** text box, enter the following URL.

   `https://sfo01wnsx01a.sfo01.rainpole.local/api/v1/node/services/http?action=apply_certificate&certificate_id=`*`sfo01wnsx01a_certificate_ID`*

   After the NSX-T Manager sends a response back, on the **Body** tab, you see a `202 Accepted` status.

5 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

6 Restart the NSX-T Manager appliance.

   a In the **VMs and Templates** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-nsx** tree.

   b Right-click the **sfo01wnsx01a** virtual machine, and select **Power > Restart Guest OS**.

Connect NSX-T Manager to the vCenter Server Instances

Connect the first NSX-T Manager appliance to the Compute vCenter Server for the workload domain so that tenant workloads can use NSX-T networking components and to Management vCenter Server so that you can place the remaining NSX-T Manager nodes on the management cluster later.

Setting	Value for the Compute vCenter Server for the Workload Domain	Value for the Management vCenter Server
Name	sfo01w02vc01	sfo01m01vc01
Domain Name or IP Address	sfo01w02vc01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
Compute Manager Type	vCenter	vCenter
User Name	svc-nsxmanager@rainpole.local	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*	*svc-nsxmanager_password*

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

a Open a Web browser and go to **`https://sfo01wnsx01a.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Add the Compute vCenter Server for the workload domain to NSX-T Manager.

a On the main navigation bar, click **System**.

b In the navigation pane, select **Fabric > Compute Managers**.

c Click **Add**, enter the following values, and click **Add**.

Setting	Value
Name	sfo01w02vc01
Domain Name/IP Address	sfo01w02vc01.sfo01.rainpole.local
Type	vCenter
User name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

d To establish a trusted connection to the Compute vCenter Server, verify the thumbprint of the vCenter Server certificate and click **Add**.

After the connection to the Compute vCenter Server is established, on the **Compute Managers** page, the following status appears.

Setting	Expected Value
Registration Status	Registered
Connection Status	UP

3 Repeat Step 2 to connect the first NSX-T Manager node to the Management vCenter Server.

Deploy the Remaining Nodes of the NSX-T Manager Cluster

To start implementing high availability of NSX-T Manager, deploy the remaining two nodes of the NSX-T Manager cluster on the management cluster.

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

a Open a Web browser and go to `https://sfo01wnsx01a.sfo01.rainpole.local`.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Overview** and click **Add Nodes**.

The **Add Nodes** wizard appears.

4 On the **Common Attributes** page, enter the following settings and click **Next**.

Setting	Value
Compute Manager	sfo01m01vc01
Enable SSH	Yes
Enable Root Access	No
CLI Password / Confirm CLI Password	*nsx_cli_password*
Root Password / Confirm Root Password	*nsx_root_password*
DNS Servers	172.16.11.5 172.16.11.4
NTP Servers	ntp.sfo01.rainpole.local
Form Factor	Large

5 On the **Nodes** page, enter the following settings to create the sfo01wnsx01b NSX-T Manager node.

Setting	Value
Name	sfo01wnsx01b
Cluster	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Network	sfo01-m01-vds01-management
IP Assignment Type	Static

Setting	Value
Management IP/Netmask	172.16.11.83/24
Management Gateway	172.16.11.253

6 To create sfo01wnsx01c, on the **Add Node** page of the wizard, click **Add Node**, enter the following settings, and click **Finish**.

Setting	Value
Name	sfo01wnsx01b
Cluster	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Network	sfo01-m01-vds01-managementsfo01-m01-vds01-management
IP Assignment Type	Static
Management IP/Netmask	172.16.11.84/24
Management Gateway	172.16.11.253

Each NSX-T Manager nodes has a **Repository Status** equal to `Sync Complete`, and the status of the management cluster is `Stable`.

Create an Anti-Affinity Rule for the NSX-T Manager Appliances

Create a VM-Host anti-affinity rule to ensure that the NSX-T Manager virtual machines run on different ESXi hosts. If an ESXi host is unavailable, the NSX-T Manager virtual machines on the other hosts continue to provide support for the NSX-T management and control planes.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Hosts and Clusters** inventory tree, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

4 Under the **Configuration** section, select **VM/Host Rules** and click **Add**.

5 In the **Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-sfo01wnsx01
Enable rule	Selected
Type	Separate Virtual Machine

6 In the **Add Rule Member** dialog box, select the three NSX-T Manager virtual machines and click **OK**.

- sfo01wnsx01a
- sfo01wnsx01b
- sfo01wnsx01c

7 In the **Create VM/Host Rule** dialog box, click **OK**.

Move the NSX-T Manager Appliances to the NSX Folder

After you deploy the remaining appliances of the NSX-T Manager cluster, move them to the virtual machine folder for NSX and NSX-T.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **VMs and Templates** inventory tree, expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Drag sfo01wnsx01b and drop it on the **sfo01-m01fd-nsx** folder.

4 Drag sfo01wnsx01c and drop it on the **sfo01-m01fd-nsx** folder.

Replace the Certificates for the Remaining NSX-T Manager Appliances

After you deploy the remaining NSX-T Manager appliances, replace the default certificate for them to establish a trusted connection with the management components in the SDDC. To replace the certificate for an NSX-T Manager instance, you import the certificates through the NSX-T Manager user interface and replace the existing certificates using a REST API client.

You use the `CertGenVVD` utility to generate a certificate that is signed by a certificate authority (CA) on the parent Active Directory server.

Table 5-2. URLs for Replacing the Certificates for the NSX-T Manager Appliances

NSX-T Manager Appliance	POST URL for Certificate Replacement
sfo01wnsx01b	`https://sfo01wnsx01b.sfo01.rainpole.local/api/v1/node/services/http?action=apply_certificate&certificate_id=`*`sfo01wnsx01b_certificate_ID`*
sfo01wnsx01c	`https://sfo01wnsx01c.sfo01.rainpole.local/api/v1/node/services/http?action=apply_certificate&certificate_id=`*`sfo01wnsx01c_certificate_ID`*

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

a Open a Web browser and go to **`https://sfo01wnsx01a.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Retrieve the ID of the certificate for the NSX-T Manager node.

a On the main navigation bar, click **System**.

b In the navigation pane, select **Certificates**.

c Click the **ID** value of the sfo01wnsx01b certificate and copy its value from the text box that appears.

3 Log in to the Windows host that has access to your data center.

4 Replace the default certificate for the NSX-T Manager appliance with the CA-signed certificate.

a Start the Postman application in your Web browser and log in.

b On the **Authorization** tab, configure the following settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	*nsx_admin_password*

c On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Key Value	application/xml

d In the request pane at the top, from the drop-down menu that contains the HTTP request methods, select **POST**, and in the **URL** text box, enter the following URL query.

`https://sfo01wnsx01b.sfo01.rainpole.local/api/v1/node/services/http?action=apply_certificate&certificate_id=`*`sfo01wnsx01b_certificate_ID`*

After the NSX-T Manager appliance sends a response back, on the **Body** tab, you see a `202 Accepted` status.

5 To upload the CA-signed certificate on the sfo01wnsx01c NSX-T Manager appliance, repeat Step 2 to Step 4.

6 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

7 Restart the NSX-T Manager appliances.

a In the **VMs and Templates** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-nsx** tree.

b Right-click the **sfo01wnsx01b** virtual machine, and select **Power > Restart Guest OS**.

c Right-click the **sfo01wnsx01c** virtual machine, and select **Power > Restart Guest OS**.

8 In the user interface of NSX-T Manager, verify that the **Repository Status** for each NSX-T Manager appliance is `Sync Complete` , and that the status of the management cluster is `Stable`.

Assign a Virtual IP Address and Certificate to the NSX-T Manager Cluster

After you deploy all three NSX-T Manager nodes, assign the virtual IP (VIP) address of the NSX-T Manager cluster and assign a certificate for the VIP address for trusted access to the user interface and API.

Procedure

1 Log in to the user interface of the first NSX-T Manager appliance.

  a Open a Web browser and go to **`https://sfo01wnsx01a.sfo01.rainpole.local`**.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Assign the virtual IP address to the NSX-T Manager cluster.

  a In the **Navigator**, click **System > Overview**.

  b Click **Edit** next to **Virtual IP**, enter **`172.16.11.81`**, and click **Save**.

  c When prompted click **Refresh**.

3 Retrieve the ID of the certificate for the NSX-T Manager node.

  a On the main navigation bar, click **System**.

  b In the navigation pane, select **Certificates**.

  c Click the **ID** value of the sfo01wnsx01 certificate and copy its value from the text box that appears.

4 Log in to the Windows host that has access to your data center.

5 Assign a certificate to the NSX-T Manager cluster.

  a Start the Postman application in your Web browser and log in.

  b On the **Authorization** tab, configure the following settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	*nsx_admin_password*

c On the **Headers** tab, enter the following header details.

Setting	Value
Key	Content-Type
Key Value	application/xml

d In the request pane at the top, from the drop-down menu that contains the HTTP request methods, select **POST**, and in the **URL** text box, enter the following URL query.

`https://sfo01wnsx01a.sfo01.rainpole.local/api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=`*`sfo01wnsx01_certificate_ID`*

After the NSX-T Manager appliance sends a response back, on the **Body** tab, you see a `202 Accepted` status.

Assign a License to NSX-T

By using the user interface of NSX-T Manager, replace the evaluation license for NSX-T with a production one.

Procedure

1 Log in to the user interface of NSX-T Manager.

a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Licenses**.

4 Click **Add**, enter the license key, and click **Add**.

Create the Transport Zones for System and Overlay Traffic

After you deploy the NSX-T Manager cluster, configure the NSX-T logical networks by creating the transport zones for ESXi management, uplink, and overlay traffic.

Table 5-3. NSX-T Transport Zones in a Workload Domain

Name	N-VDS Name	N-VDS Mode	Traffic Type
sfo01-w-uplink01	sfo01-w-uplink01	Standard	VLAN
sfo01-w-uplink02	sfo01-w-uplink02	Standard	VLAN

Table 5-3. NSX-T Transport Zones in a Workload Domain (Continued)

Name	N-VDS Name	N-VDS Mode	Traffic Type
sfo01-esxi-vlan	sfo01-w-nvds01	Standard	VLAN
sfo01-w-overlay	sfo01-w-nvds01	Standard	Overlay

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 Navigate to **Fabric > Transport Zones** and click **Add**.

4 On the **New Transport Zone** page, enter the following settings for the first transport zone and click **Add**.

Setting	Value
Name	sfo01-w-uplink01
N-VDS Name	sfo01-w-uplink01
N-VDS Mode	Standard
Traffic Type	VLAN

5 Repeat the previous step to create the remaining transport zones.

Create Uplink Profiles and the Network I/O Control Profile

Uplink profiles define the policies for the links from ESXi hosts to NSX-T segments or from NSX Edge nodes to top of rack switches. During network contention Network I/O Control allocates bandwidth to a system traffic type according to priority of the traffic.

Procedure

1 Log in to the user interface of NSX-T Manager.

  a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, click **Fabric > Profiles**.

4 Create uplink profiles to define policies for the links between the ESXi hosts and segments and between NSX-T Edge nodes and top of rack switches.

  a On the **Profiles** page, click the **Uplink Profiles** tab and click **Add**.

  b On the **New Uplink Profile** page, enter the following values and click **Add**.

Name	Teaming - Teaming Policy	Teaming - Active Uplinks	Transport VLAN	MTU
esxi-w02-uplink-profile	Load Balance Source	uplink-1,uplink-2	1644	9000
sfo01-w-overlay-profile	Failover Order	uplink-1	1649	9000
sfo01-w-uplink01-profile	Failover Order	uplink-1	1647	9000
sfo01-w-uplink02-profile	Failover Order	uplink-1	1648	9000

5 Create a Network I/O Control profile to allocate network bandwidth to system traffic and virtual machine traffic in the workload domains.

a On the **Profiles** page, click the **NIOC Profiles** tab and click **Add**.

b On the **New NIOC Profile** page, enter the following values.

Setting	Value
Name	sfo01-w-nioc-profile
Status	Enabled

c Modify the **Host Infra Traffic Resource** shares and click **Add**.

Traffic Type / Traffic Name	Shares
Fault Tolerance (FT) Traffic	25
vSphere Replication (VR) Traffic	25
iSCSI Traffic	25
Management Traffic	50
NFS Traffic	25
vSphere Data Protection Backup Traffic	25
Virtual Machine Traffic	100
vMotion Traffic	25
vSAN Traffic	100

Create the NSX-T Segments for System, Uplink, and Overlay Traffic

Create the segments to connect nodes that send VLAN and overlay traffic.

You perform this procedure for each segment.

Table 5-4. NSX-T Logical Networks in a Workload Domain

Segment Name	Uplink & Type	Transport Zone	VLAN
sfo01-w-nvds01-management	Isolated - No Logical Connection	sfo01-esxi-vlan	1641
sfo01-w-nvds01-vmotion	Isolated - No Logical Connection	sfo01-esxi-vlan	1642
sfo01-w-nvds01-nfs	Isolated - No Logical Connection	sfo01-esxi-vlan	1643
sfo01-w-nvds01-uplink01	Isolated - No Logical Connection	sfo01-esxi-vlan	0-4094
sfo01-w-nvds01-uplink02	Isolated - No Logical Connection	sfo01-esxi-vlan	0-4094

Table 5-4. NSX-T Logical Networks in a Workload Domain (Continued)

Segment Name	Uplink & Type	Transport Zone	VLAN
sfo01-w-uplink01	Isolated - No Logical Connection	sfo01-w-uplink01	1647
sfo01-w-uplink02	Isolated - No Logical Connection	sfo01-w-uplink02	1648
sfo01-w-overlay	Isolated - No Logical Connection	sfo01-esxi-vlan	0-4094
sfo01-w-ubuntu-01	Isolated - No Logical Connection	sfo01-w-overlay	-

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, select **Segments**.

4 On the **Segments** tab, click **Add Segment**.

5 Enter the following values for the sfo01-w-nvds01-management segment and click **Save**.

Setting	Value
Name	sfo01-w-nvds01-management
Uplink & Type	Isolated - No Logical Connection
Transport Zone	sfo01-esxi-vlan
VLAN	1641

6 Repeat this procedure to create the remaining segments.

Create a Transport Node Profile

Create a transport node profile for the ESXi management and overlay traffic to and from the ESXi hosts in the workload domain. By using this profile, all hosts in the domain have the same transport node configuration.

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Fabric > Profiles**.

4 On the **Profiles** page, click the **Transport Node Profiles** tab and click **Add**.

5 On the **General** tab of the **Add Transport Node Profile** dialog box, enter the following settings.

Setting	Value
Name	sfo01-w02-shared01-profile
Transport Zones	■ sfo01-esxi-vlan ■ sfo01-w-overlay

6 On the **N-VDS** tab, under **New Node Switch**, enter the following settings.

Setting	Value
N-VDS Name	sfo01-w-nvds01
NIOC Profile	sfo01-w-nioc-profile
Uplink Profile	esxi-w02-uplink-profile
LLDP Profile	LLDP [Send Packet Enabled]
IP Assignment	Use DHCP
Physical NICs	vmnic0 > uplink-1 vmnic1 > uplink-2

7 Next to **Network Mappings for Install**, click **Add Mapping**, enter the following settings, and click **Add**.

VMkernel Adapter	VLAN Segment/Logical Switch
vmk0	sfo01-w-nvds01-management
vmk1	sfo01-w-nvds01-vmotion

Note If your hosts have other VMkernel adapters, for example, for vSAN or NFS storage, create a mapping so that they do not lose connectivity.

8 Click **Add Mapping** for **Network Mappings for Uninstall**, enter the following settings, and click **Add**.

Table 5-5. VMkernel Mappings

VMkernel Adapter	Port Group
vmk0	sfo01-w02-vds01-management
vmk1	sfo01-w02-vds01-vmotion

Table 5-6. Physical NIC Mappings

Physical NIC
vmnic0
vmnic1

9 Click **Add** to save the profile.

Configure the ESXi Host Transport Nodes

To use NSX-T, configure the ESXi hosts in the shared edge and compute cluster as transport nodes. As a result, the NSX-T Manager installs the NSX-T kernel modules on the hosts as VIB files.

The NSX-T kernel modules provide services such as distributed routing and distributed firewall.

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Fabric > Nodes**.

4 On the **Host Transport Nodes** tab, from the **Managed by** drop-down menu, select **sfo01w02vc01**.

5 Select the **sfo01-w02-comp01** cluster and click **Configure NSX**.

6 Select the **sfo01-w02-shared01-profile** transport node profile and click **Save**.

Each ESXi host has the following transport node configuration:

Setting	Value
NSX Configuration	Configured
Configuration State	Success
Node State	Up

Setting	Value
Transport Zones	■ sfo01-esxi-vlan ■ sfo01-w-overlay
NSX Version	2.4.0
N-VDS	1

Remove the ESXi Hosts for the vSphere Distributed Switch

After you configure the ESXi hosts in the shared edge and compute cluster as transport nodes, the NSX-T infrastructure starts handling the system and virtual machine traffic to the hosts. You can remove the hosts from the vSphere Distributed Switch.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Networking** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

3 Expand the **sfo01-w02dc** data center object.

4 Right-click the **sfo01-w02-vds01** vSphere Distributed Switch and select **Add and Manage Hosts**.

5 In the **sfo01-w02-vds01 - Add and Manage Hosts** wizard, select **Remove hosts** and click **Next**.

6 Click **Attached Hosts**, select all hosts in the shared edge and compute cluster, click **OK**, and click **Next**.

7 On the **Ready to complete** page, click **Finish**.

Configure Dynamic Routing in the Shared Edge and Compute Cluster

To support the communication between tenant workloads by using application virtual networks in NSX-T and to connect tenant workloads to the external network, configure dynamic routing in the shared edge and compute cluster.

Routing occurs in both the North-South and East-West directions.

- North-South traffic leaving or entering the workload domain, for example, a virtual machine on an overlay network communicating with an end-user device on the corporate network.

- East-West traffic remains in the workload domain, for example, two virtual machines on the same or different segments communicating with each other.

Procedure

1 Create an NSX-T Edge Cluster Profile

For availability of the routing services and connectivity to the external network, you create a multi-node cluster of NSX-T Edge nodes. To define a common configuration for both NSX-T Edge nodes, you create an edge cluster profile.

2 Deploy the NSX-T Edge Appliances

To provide tenant workloads with routing services and connectivity to networks that are external to the workload domain, deploy two NSX-T Edge nodes.

3 Join the NSX-T Edge Nodes to the Management Plane

After you deploy the NSX-T Edge appliances in the shared edge and compute cluster, to connect them to the NSX-T Manager cluster, join them to the management plane.

4 Create an Anti-Affinity Rule for the NSX-T Edge Nodes in the Shared Edge and Compute Cluster

To ensure that the two NSX-T Edge appliances run on different ESXi hosts, create a DRS VM-host anti-affinity rule. If a failure occurs on one of the hosts, the appliance on the other host continues providing routing services.

5 Add the NSX-T Edge Nodes to the Transport Zones

After you deploy the NSX-T Edge nodes and join them to the management plane, to connect the nodes to the workload domain, add them to the transport zones for uplink and overlay traffic, and configure the N-VDS switches on each edge node.

6 Create an NSX-T Edge Cluster

Adding multiple NSX-T Edge nodes to a cluster increases the availability of networking services. An NSX-T Edge cluster is necessary to support the Tier-0 and Tier-1 gateways in the workload domain.

7 Create and Configure the Tier-0 Gateway

The Tier-0 gateway in the NSX-T Edge cluster provides a gateway service between the logical and physical network. The NSX-T Edge cluster can back multiple Tier-0 gateways.

8 Create and Configure the Tier-1 Gateway

Create and configure the Tier-1 gateway to re-distribute routes to the Tier-0 gateway and to provide routing between tenant workloads.

9 Verify BGP Peering and Route Redistribution

The Tier-0 gateway must establish a connection to each of the upstream Layer 3 devices before BGP updates can be exchanged. Verify that the NSX-T Edge nodes are successfully peering and that BGP routing is established.

Create an NSX-T Edge Cluster Profile

For availability of the routing services and connectivity to the external network, you create a multi-node cluster of NSX-T Edge nodes. To define a common configuration for both NSX-T Edge nodes, you create an edge cluster profile.

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Fabric > Profiles**.

4 On the **Edge Cluster Profiles** tab, click **Add**.

5 On the **New Edge Cluster Profile** page, enter the following values and click **Add**.

Setting	Value
Name	sfo01-w-edge-cluster01-profile
BFD Probe	1000
BFD Allowed Hops	255
BFD Declare Dead Multiple	3

Deploy the NSX-T Edge Appliances

To provide tenant workloads with routing services and connectivity to networks that are external to the workload domain, deploy two NSX-T Edge nodes.

Table 5-7. NSX-T Edge Nodes

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Name	sfo01wesg01	sfo01wesg02
Port Groups	sfo01-w-nvds01-management	sfo01-w-nvds01-management
Primary IP Address	172.16.41.21	172.16.41.22

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Hosts and Clusters** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree and expand the **sfo01-w02dc** tree.

3 Expand the **sfo01-w02-shared01** cluster.

4 Right-click the **sfo01-w02rp-sddc-edge** resource pool and select **Deploy OVF Template**.

5 On the **Deploy OVF Template** page, navigate to the `.ova` file of the NSX-T Edge appliance and click **Next**.

6 On the **Select name and location** page, enter the following settings and click **Next**.

Setting	Value
Name	sfo01wesg01
Folder or data center	sfo01-w02fd-nsx

7 On the **Select a resource** page, select the **sfo01-w02rp-sddc-edge** resource pool and click **Next**.

8 On the **Select storage** page, select the *shared_edge_datastore* and click **Next**.

9 On the **Select networks** page enter the following and click **Next**.

Source Network	Destination Network
Network 3	sfo01-w-nvds01-uplink02
Network 2	sfo01-w-nvds01-uplink01
Network 1	sfo01-w-overlay
Network 0	sfo01-w-nvds01-management

10 On the **Customize template** page, expand the setting groups, enter the following settings, and click **Next**.

Setting	Value
System Root User Password / Confirm Password	*nsx_edge_root_password*
CLI "admin" User Password / Confirm Password	*nsx_edge_admin_password*
CLI "audit" User Password / Confirm Password	*nsx_edge_admin_password*

Setting	Value
Hostname	sfo01wesg01.sfo01.rainpole.local
Default IPv4 Gateway	172.16.41.253
Management Network IPv4 Address	172.16.41.21
Management Network Netmask	255.255.255.0

Setting	Value
DNS Server List	172.16.11.5 172.16.11.4
Domain Search List	sfo01.rainpole.local
NTP Server List	ntp.sfo01.rainpole.local
Enable SSH	Selected
Allow root SSH login	Deselected

11 On the **Ready to complete** page, click **Finish**.

12 After the deployment finishes, power on the NSX-T Edge appliance.

  a In the **VMs and Templates** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.

  b Expand the sfo01-w02fd-nsx folder, right-click the **sfo01wesg01** virtual machine, and select **Power > Power On**.

13 Repeat this procedure to deploy the sfo01wesg02 NSX-T Edge appliance.

Join the NSX-T Edge Nodes to the Management Plane

After you deploy the NSX-T Edge appliances in the shared edge and compute cluster, to connect them to the NSX-T Manager cluster, join them to the management plane.

Table 5-8. NSX Edge Nodes

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Name	sfo01wesg01	sfo01wesg02
Port Groups	sfo01-w-nvds01-management	sfo01-w-nvds01-management
Primary IP Address	172.16.41.21	172.16.41.22

Procedure

1 Log in to the first NSX-T Manager node by using Secure Shell (SSH) client.

  a Open an SSH connection to the `sfo01wnsx01a.sfo01.rainpole.local` appliance.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 Retrieve the thumbprint ID of the certificate for the NSX-T Manager cluster by running and copying the output from the following command.

```
get certificate cluster thumbprint
```

3 Log in to the first NSX-T Edge node by using Secure Shell (SSH) client.

   a Open an SSH connection to the sfo01wesg01.sfo01.rainpole.local appliance.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*edge_admin_password*

4 Join the NSX-T Edge node to the management plane by running the following command.

```
join management-plane sfo01wnsx01.sfo01.rainpole.local thumbprint thumbprintid username admin
```

5 Enter the password for the **admin** account.

6 Repeat Step 3 to Step 5 on the sfo01wesg02.sfo01.rainpole.local NSX-T Edge appliance.

Create an Anti-Affinity Rule for the NSX-T Edge Nodes in the Shared Edge and Compute Cluster

To ensure that the two NSX-T Edge appliances run on different ESXi hosts, create a DRS VM-host anti-affinity rule. If a failure occurs on one of the hosts, the appliance on the other host continues providing routing services.

Procedure

1 Log in to vCenter Server by using the vSphere Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Hosts and Clusters** inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree and expand the **sfo01-w02dc** tree.

3 Select the **sfo01-w02-shared01** cluster and click the **Configure** tab.

4 Under **Configuration**, select **VM/Host Rules** and click **Add**.

5 In the **sfo01-w02-shared01- 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 Machines

6 In the **Add Rule Member** dialog box, select the check boxes next to **sfo01wesg01** and **sfo01wesg02**, and click **OK**.

7 In the **sfo01-w02-shared01- Create VM/Host Rule** dialog box, click **OK**.

Add the NSX-T Edge Nodes to the Transport Zones

After you deploy the NSX-T Edge nodes and join them to the management plane, to connect the nodes to the workload domain, add them to the transport zones for uplink and overlay traffic, and configure the N-VDS switches on each edge node.

Procedure

1 Log in to the user interface of NSX-T Manager.

a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Fabric > Nodes > Edge Transport Nodes**.

4 Select the **sfo01wesg01** edge node and click **Configure NSX**.

5 Under **Edit Transport Node - sfo01wesg01**, click the **General** tab.

6 Under **Transport Zones**, move the following transport zones to the **Selected** list and click **Add**.

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Transport Zones	sfo01-w-uplink01(VLAN)	sfo01-w-uplink01(VLAN)
	sfo01-w-uplink02(VLAN)	sfo01-w-uplink02(VLAN)
	sfo01-w-overlay(Overlay)	sfo01-w-overlay(Overlay)

7 Under **Edit Transport Node - sfo01wesg01**, click the **N-VDS** tab.

8 Under **New Node Switch**, enter the following values.

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w-nvds01	sfo01-w-nvds01
Uplink Profile	sfo01-w-overlay-profile	sfo01-w-overlay-profile
IP Assignment	Use Static IP List	Use Static IP List
Static IP List	172.16.49.21	172.16.49.22
Gateway	172.16.49.253	172.16.49.253
Subnet Mask	255.255.255.0	255.255.255.0
Virtual NICs	fp-eth0 uplink-1	fp-eth0 uplink-1

9 Click **Add N-VDS**, enter the following values.

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w-nvds01-uplink01	sfo01-w-nvds01-uplink01
Uplink Profile	sfo01-w-uplink01-profile	sfo01-w-uplink01-profile
IP Assignment	*Greyed Out*	*Greyed Out*
Virtual NICs	fp-eth1 uplink-1	fp-eth1 uplink-1

10 Click **Add N-VDS**, enter the following values, and click **Save**.

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w-nvds01-uplink02	sfo01-w-nvds01-uplink02
Uplink Profile	sfo01-w-uplink02-profile	sfo01-w-uplink02-profile
IP Assignment	*Greyed Out*	*Greyed Out*
Virtual NICs	fp-eth2 uplink-1	fp-eth2 uplink-1

11 Repeat the step on sfo01wesg02.

The edge transport nodes have the following configuration:

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge	sfo01wesg01	sfo01wesg02
Management IP	172.16.41.21	172.16.41.22
Configuration State	Success	Success
Node Status	Up	Up
Transport Zones	■ sfo01-w-overlay ■ sfo01-w-uplink01 ■ sfo01-w-uplink02	■ sfo01-w-overlay ■ sfo01-w-uplink01 ■ sfo01-w-uplink02
N-VDS	3	3

Create an NSX-T Edge Cluster

Adding multiple NSX-T Edge nodes to a cluster increases the availability of networking services. An NSX-T Edge cluster is necessary to support the Tier-0 and Tier-1 gateways in the workload domain.

Procedure

1 Log in to the user interface of NSX-T Manager.

   a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **System**.

3 In the navigation pane, select **Fabric > Nodes**.

4 On the **Edge Clusters** tab, click **Add**.

5 In the **Add Edge Cluster** dialog box, configure the following settings.

Setting	Value
Name	sfo01-w-edge-cluster01
Edge Cluster Profile	sfo01-w-edge-cluster01-profile

6 From the **Member Type** drop-down menu, select **Edge Node**.

7 Move the sfo01wesg01.sfo01.rainpole.local and sfo01wesg02.sfo01.rainpole.local nodes the **Selected** list.

8 Click **OK** and click **Add**.

Create and Configure the Tier-0 Gateway

The Tier-0 gateway in the NSX-T Edge cluster provides a gateway service between the logical and physical network. The NSX-T Edge cluster can back multiple Tier-0 gateways.

Procedure

1 Log in to the user interface of NSX-T Manager.

  a Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 Create the Tier-0 gateway.

  a On the main navigation bar, click **Networking**.

  b Select **Tier-0 Gateways** and click **Add Tier-0 Gateway**.

  c Enter the following values and click **Save**.

Setting	Value
Name	sfo01-w-tier-0-01
High Availability Mode	Active-Active
Edge Cluster	sfo01-w-edge-cluster01

3 Confirm that you want to continue configuring the Tier-0 gateway.

4 Configure route redistribution.

  a Expand **Route Re-Distribution** and click **Set**.

  b Select all sources and click **Apply**.

5 Add the uplink interfaces to the NSX-T Edge nodes.

  a Expand **Interfaces** and click **Set**.

  b In the **Set Interfces** dialog box, click **Add Interface** and enter the settings of the uplink interface.

Name	Type	IP Address / Mask	Connected To (Segment)	Edge Node	MTU
sfo01wesg01-Uplink01	External	172.16.47.2/24	sfo01-w-uplink01	sfo01wesg01	9000
sfo01wesg01-Uplink02	External	172.16.48.2/24	sfo01-w-uplink02	sfo01wesg01	9000
sfo01wesg02-Uplink01	External	172.16.47.3/24	sfo01-w-uplink01	sfo01wesg02	9000
sfo01wesg02-Uplink02	External	172.16.48.3/24	sfo01-w-uplink02	sfo01wesg02	9000

  c Click **Save**.

  d Repeat this step for the other interfaces and click **Close**.

6 Configure BGP.

   a Expand **BGP**, enter the following settings, and click **Save**.

Setting	Value
Local AS	65000
BGP	On
Graceful Restart	Off
Inter SR iBGP	On
ECMP	On
Multipath Relax	On

   b Click **Set** for **BGP Neighbors**.

   c In the **Set BGP Neighbors** dialog box, click **Add BGP Neighbor** and enter the following settings for the first Layer 3 device.

IP Address	BFD	Remote AS	Hold Down Time	Keep Alive Time	Password
172.16.47.1	Disabled	65001	12	4	*bgp_password*
172.16.48.1	Disabled	65001	12	4	*bgp_password*

Note Enable BFD if the network supports and is configured for BFD.

   d Repeat for the other neighbor, click **Save** and click **Close**.

7 Click **Close Editing**.

8 Generate a BGP summary for the Tier-0 gateway.

   a In the main navigation bar, click **Advanced Networking & Security.**

   b Select **Routers** and select **sfo01-w-tier-0-01**.

   c Select **Actions > Generate BGP Summary**.

   d Verify the **Connection Status** of each transport node is `Established`.

Create and Configure the Tier-1 Gateway

Create and configure the Tier-1 gateway to re-distribute routes to the Tier-0 gateway and to provide routing between tenant workloads.

Tier-1 gateways have downlink ports to connect to NSX-T segments and uplink ports to connect to NSX-T Tier-0 gateways.

Procedure

1 Log in to the user interface of NSX-T Manager.

  a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 Create the Tier-1 gateway.

  a On the main navigation bar, click **Networking**.

  b Select **Tier-1 Gateways** and click **Add Tier-1 Gateway**.

  c Enter the following values.

Setting	Value
Name	sfo01-w02-tier-1-01
Linked Tier-0 Gateway	sfo01-w-tier0-01
Failover	Preemptive
Edge Cluster	sfo01-w-edge-cluster-01

  d Next to **Edges**, click **Set**.

  e In the **Select Edges** dialog box, click **Add Edge**.

  f Add the **sfo01wesg01** and **sfo01wesg02** edge nodes and click **Apply**.

3 Confirm that you want to continue with configuring the Tier-0 gateway.

4 Expand **Route Advertisement**, enable all types, and click **Save**.

5 Verify the connection between the Tier-1 and Tier-0 gateways.

  a On the main navigation bar, click **Advanced Networking & Security.**

  b Select **Routers**.

  c Select the **sfo01-w02-tier-1-01** gateway.

d Select **Configuration > Router Ports** and verify that the existing LinkedPort has the following settings.

Setting	Expected Value
Logical Router	LinkedPort_sfo01-w-tier-0-01
Type	Linked Port
IP Address/mask	x.x.x.x/31
Connected To	sfo01-w-tier-0-01
Transport Node	■ sfo01wesg01, ■ sfo01wesg02

e Select the **sfo01-w-tier-0-01** gateway.

f Select **Configuration > Router Ports**, and verify that the existing LinkedPort has the following settings.

Setting	Expected Value
Logical Router	LinkedPort_sfo01-w-tier-0-01
Type	Linked Port
IP Address/mask	x.x.x.x/31
Connected To	sfo01-w02-tier-1-01
Transport Node	-

Verify BGP Peering and Route Redistribution

The Tier-0 gateway must establish a connection to each of the upstream Layer 3 devices before BGP updates can be exchanged. Verify that the NSX-T Edge nodes are successfully peering and that BGP routing is established.

Procedure

1 Log in to sfo01wesg01 by using a Secure Shell (SSH) client.

a Open an SSH connection and go to sfo01wesg01.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_edge_admin_password*

2 Get information about the Tier-0 and Tier-1 service routers and distributed router.

```
get logical-router
```

For example, the output of the command might contain the following configuration:

UUID	VRF	LR-ID	Name	Type	Ports
sample_uuid	0	0		TUNNEL	3
sample_uuid	1	5	SR-tier0-01	SERVICE_ROUTER_TIER0	6
sample_uuid	2	2	DR-tier1-01	DISTRIBUTED_ROUTER_TIER1	5
sample_uuid	3	3	DR-tier0-01	DISTRIBUTED_ROUTER_TIER0	4
sample_uuid	4	11	SR-tier1-01	SERVICE_ROUTER_TIER1	5

3 By using the `VRF` value for `SERVICE_ROUTER_TIER0` connect to the service router for Tier 0.

```
vrf 1
```

The prompt changes to *`hostname`*`(tier0_sr)>`. All commands are associated with this object.

4 Verify the BGP connections to the neighbors of the service router for Tier 0.

```
get bgp neighbor
```

The `BGP State` for each neighbor appears as `Established, up for` *`hh:mm:ss`*.

5 Verify that you are receiving routes by using BGP and that multiple routes to BGP-learned networks exist.

```
get route
```

6 Repeat this procedure on sfo01wesg02.

Deploy a Segment for a Sample Tenant Workload

You create logical segments and connect them to the Tier-1 gateway for your tenant workloads. For example, you can create a segment for Ubuntu workloads and connect it to the Tier-1 gateway.

Procedure

1 Log in to the user interface of NSX-T Manager.

a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, select **Segments**.

4 On the **Segments** tab, next to the **sfo01-w-ubuntu-01** segment, click the three vertical dots and select **Edit**.

5 Change the **Uplink & Type** from **Isolated - Flexible** to **sfo01-w02-tier1-01 | Tier 1**.

6 Assign a subnet to the segment.

   a Click **Set Subnets**.

   b In the **Set Subnets** dialog box, click **Add Subnet**, enter **`192.168.200.1/24`**, click **Add**, and click **Apply**.

7 In the segment pane, click **Save**.

What to do next

After you place workloads on the new segment by connecting them to the segment port group in vSphere, configure 192.168.200.1 as the default gateway for the workloads.

Connect vRealize Log Insight to the NSX-T Instance for the Shared Edge and Compute Cluster

6

After you deploy the NSX-T components in the new workload domain, you connect vRealize Log Insight to the NSX-T instance to start collecting log information.

1 Install the vRealize Log Insight Content Pack for NSX-T

To view log dashboards in vRealize Log Insight with details on the NSX-T operation, install the NSX-T content pack.

2 Configure the NSX-T Components to Forward Log Events to vRealize Log Insight

Configure the NSX-T Manager and NSX-T Edge nodes to send audit logs and system events to vRealize Log Insight.

Install the vRealize Log Insight Content Pack for NSX-T

To view log dashboards in vRealize Log Insight with details on the NSX-T operation, install the NSX-T content pack.

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 by using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

2 Click the configuration drop-down menu icon ☰ and select **Content Packs**.

3 Select **Content Pack Marketplace > Marketplace**.

4 Select **VMware - NSX-T**.

The **Install Content Pack** dialog box appears.

5 Accept the license agreement and click **Install**.

6 Click **OK**.

Configure the NSX-T Components to Forward Log Events to vRealize Log Insight

Configure the NSX-T Manager and NSX-T Edge nodes to send audit logs and system events to vRealize Log Insight.

You repeat this procedure for the following NSX-T components.

NSX-T Component	Hostname
Managers	■ sfo01wnsx01a.sfo01.rainpole.local ■ sfo01wnsx01b.sfo01.rainpole.local ■ sfo01wnsx01c.sfo01.rainpole.local
Edges	■ sfo01wesg01.sfo01.rainpole.local ■ sfo01wesg02.sfo01.rainpole.local

Procedure

1 Open an SSH connection to the first NSX-T Manager appliance.

  a Open an SSH connection to sfo01wnsx01a.sfo01.rainpole.local.

  b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*nsx_admin_password*

2 To set up log forwarding to vRealize Log Insight, run the following command.

```
set logging-server 192.168.31.10 proto udp level info
```

3 To verify that log forwarding is configured, run the following command.

```
get logging-servers
```

4 Repeat the procedure for all NSX-T Manager and NSX-T Edge nodes.

Back Up and Restore the NSX-T Instance for the Shared Edge and Compute Cluster

7

Back up the NSX-T Manager cluster so that you can restore its operation and modify the NSX-T configuration in the workload domain after failures.

The NSX-T Manager cluster stores the configured state of the segments. If the NSX-T Manager appliances become unavailable, the network traffic in the data plane is intact but you can make no configuration changes.

1 Configure Automatic Backups of the NSX-T Configuration

  Configure NSX-T Manager to store daily configuration backups to a Secure File Transfer Protocol (SFTP) server. The NSX-T configuration backup contains the NSX-T Manager nodes backup, cluster backup, and inventory backup.

2 Restore the NSX-T Manager Cluster

  If the NSX-T Manager cluster for the workload domain becomes unavailable, deploy another NSX-T Manager cluster and use a backup to import the configuration.

Configure Automatic Backups of the NSX-T Configuration

Configure NSX-T Manager to store daily configuration backups to a Secure File Transfer Protocol (SFTP) server. The NSX-T configuration backup contains the NSX-T Manager nodes backup, cluster backup, and inventory backup.

Procedure

1. Log in to the user interface of NSX-T Manager.
   a. Open a Web browser and go to `https://sfo01wnsx01.sfo01.rainpole.local`.
   b. Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

2. On the main navigation bar, click **System**.
3. In the navigation page, select **Backup & Restore**.
4. On the **Backup** tab, click **Edit**.

5 On the **File Server** page, enter the following values and click **Save**.

Setting	Value
Automatic Backup	Enabled
IP/Host	*nsx_backup_server*
Port	22
Protocol	SFTP
User name	*sftp_username*
Password	*sftp_password*
Destination Directory	*backup_directory*
Backup encryption passphrase	*password_for_backups*
SSH fingerprint	Leave blank to fetch fingerprint automatically.

6 On **Schedule** tab, configure the following settings and click **Save**.

Setting	Value
Automatic Backup	Enabled
Frequency	Weekly
Days	All days
Time	22:00
Detect NSX configuration change	Enabled
Update Interval	5 min

Restore the NSX-T Manager Cluster

If the NSX-T Manager cluster for the workload domain becomes unavailable, deploy another NSX-T Manager cluster and use a backup to import the configuration.

You restore the following configuration:

- State of the network
- Configuration that is maintained by the NSX-T Manager cluster

After you restore the NSX-T Manager cluster, you must apply again the changes, such as adding or deleting nodes, made to the fabric after the backup is taken.

Important Do not change the configuration of the NSX-T Manager cluster while the restore process is in progress.

Procedure

1 Power off the original NSX-T Manager appliances and deploy a new NSX-T Manager cluster.

The new and original NSX-T Manager cluster appliances must have the same product version and the management IP addresses.

2 Log in to the user interface of NSX-T Manager.

a Open a Web browser and go to **`https://sfo01wnsx01.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

3 On the main navigation bar, click **System**.

4 In the navigation page, select **Backup & Restore**.

5 On the **Restore** tab, click **Edit**.

6 On the **File Server** page, enter the following values and click **Save**.

Setting	Value
IP/Host	*nsx_backup_server*
Port	22
Protocol	SFTP
User name	*sftp_username*
Password	*sftp_password*
Destination Directory	*backup_directory*
Backup encryption passphrase	*password_for_backups*
SSH fingerprint	Leave blank to fetch fingerprint automatically.

7 Select a backup and click **Restore**.