Deployment Guide

VMware NSX-T Workload Domains on VxRail

VMware Validated Design 5.1

VMware NSX-T 2.4.1

Abstract

This document provides guidance for the manual deployment of an NSX-T workload Domain in a VVD on VxRail environment.

October 2019

Revisions

Date	Description
October 2019	Initial release

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Table of contents

1 About Deployment of VMware NSX-T Workload Domains

This document provides step-by-step instructions for extending a Standard SDDC with a VxRail virtual infrastructure workload domain that uses VMware NSX-T™ Data Center for software-defined networking.

1.1 Intended audience

This document is intended for architects and administrators who want to deploy NSX-T in a virtual infrastructure workload domain for tenant workloads.

1.2 Required software

This document is compliant and validated with certain product versions. See VMware Validated Design Release Notes for more information about the supported product versions.

- Software components for VMware Validated Design™ for Software-Defined Data Center 5.1
- NSX-T 2.4.1
- VxRail version 4.7.212 or later

1.3 Prerequisites

Before you deploy VMware NSX-T workload domains, ensure the following:

- Your environment is a single region VVD deployment with a management workload domain, and optionally the initial virtual infrastructure workload domain.
- The deployment must align with the VMware Validated Design for Software-Defined Data Center on VxRail.

See the VVD 5.1 on Del EMC VxRail Appliance Version 4.7.2x Planning Guide on the Dell EMC support page.

2 Preparing to Deploy a Workload Domain with NSX-T

Deployment of VMware NSX-T workload domains is based on VMware Validated Design™ for Software-Defined Data Center. Deploy the virtual network infrastructure on VMware NSX-T for a virtual infrastructure (VI) workload domain in a Shared Edge and compute cluster.

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

2.1 Before you deploy a VI Workload Domain with NSX-T

You must first deploy and configure the following components of the SDDC management cluster.

- VMware ESXi™
- VMware Platform Services Controller™ pair and Management vCenter Server®
- VMware NSX® Data Center for vSphere®
- VMware vRealize® Lifecycle Manager™
- vSphere® Update Manager™
- VMware vRealize® Operations Manager™
- VMware vRealize® Log Insight™
- VMware vRealize® Automation™ with embedded vRealize® Orchestrator™
- VMware vRealize® Business™ for Cloud

See the *VVD 5.1 on Dell EMC VxRail Appliance Version 4.7.2x Planning Guide* and the *VVD 5.1 on Dell EMC VxRail for Region A Deployment Guide* at https://www.dell.com/support.

If you follow the Standard VMware Validated Design guidance, a VI workload domain that uses NSX for vSphere as the solution for virtual networking is also deployed.

Before you deploy the NSX-T Shared Edge and compute cluster, verify that your environment satisfies the requirements listed in the following sections. You must allocate VLANs, host names and IP address in the SDDC network. The environment also must have a specific configuration of external services and virtual infrastructure.

2.1.1 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 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
VxRail node discovery	3939	-	-
NFS (optional)	1650	172.16.50.0/24	172.16.50.253
		-	-
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 **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 3 **FQDN and IP Address of the Compute vCenter Server**

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

Table 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

2.1.2 Deployment prerequisites

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

Table 5 **Deployment Prerequisites**

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.

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 the vCenter Server Appliance. • Download the .ova file for the NSX-T Unified Appliance and NSX-T Edge Node.
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. • Create a Certificate Template called VMware for use with the CerGen certificate scripts. • Download the CertGenVVD-version.zip file of the Certificate Generation Utility for VMware Validated Design 5.0.1 and generate signed certificates 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.

2.2 Generate CA-signed certificates for the NSX-T Manager nodes

Using the Certificate Generation Utility for VMware Validated Design 5.1 (CertGenVVD), generate certificates for the NSX-T Manager instances and cluster virtual IP that are signed by the Microsoft certificate authority. Use these certificates for trusted communication between the NSX-T nodes and the other management components of the SDDC.

2.2.1 Procedure

1. Log in to the Windows Server host that you allocated for certificate generation.
2. Download the CertGenVVD-3.4.zip file from VMware Knowledge Base article 2146215. and extract the ZIP file to C:\CertGenVVD-3.4.
3. In the C:\CertGenVVD-3.4 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-3.4\ConfigFiles folder, create four text files named sfo01wnsx01a.txt, sfo01wnsx01b.txt, sfo01wnsx01c.txt, and sfo01wnsx01.txt with the following content.

Table 6 **Certificate Configuration Text Files**

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]
	sfo01wnsx01asfo01wnsx01a.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]
	sfo01wnsx01bsfo01wnsx01b.sfo01.rainpole.local

sfo01wnsx01c.txt	[CERT]
	NAME=default
	ORG=default
	OU=default
	LOC=SFO
	ST=default
	CC=default
	CN=sfo01wnsx01b.sfo01.rainpole.local
	keysize=default
	[SAN]
	sfo01wnsx01csfo01wnsx01c.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]
	sfo01wnsx01sfo01wnsx01.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-3.4
   .\CertGenVVD-3.4.ps1 -validate
   ```
9. Generate the MCSA-signed certificate.
   ```
   .\CertGenVVD-3.4.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.

3 Deploy and Configure the Shared Edge and Compute Cluster Components

Note: If a Workload Domain was deployed as part of a standard VVD deployment, a workload vCenter server exists within the management cluster.

The NSX-T VxRail Cluster can join that vCenter, and NSX-T manager can be configured to manage the network resources within that cluster. If the vCenter does not exist, or you require an isolated vCenter instance, proceed with the deployment, otherwise you can skip to Section 3.7.

3.1 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 with NSX-T and to provision tenant workloads from a centralized node, you must install and configure vCenter Server on the management cluster of Region A. Connect this vCenter Server instance to the Platform Services Controller pair that is available in the region to join the single vCenter Single Sign-on domain configured on the pair.

3.1.1 Procedure

1. Open a web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. 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.
3. 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.**

Table 7 **Appliance Deployment Target Settings**

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 Setup appliance VM page, enter the following settings, and click **Next**.

Table 8 **Appliance Setup Settings**

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**.

Table 9 **Network Configuration Settings**

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

4. 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**.

Table 10 **Appliance Configuration Settings**

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**.

Table 11 **SSO Configuration Settings**

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**.

5. Enable lockdown mode on sfo01m01esx01.sfo01.rainpole.local.
   a. 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**.

3.2 Replace the certificate of the Compute vCenter Server

To establish a trusted connection to the other SDDC management components, 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 12 **Certificate Files**

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

3.2.1 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 with username `root` and 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. Using a utility such as WinSCP, copy the certificate files `sfo01w02vc01.1.cer`, `sfo01w02vc01.key`, and `Root64.cer` to the `/root/certs` folder.

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.

Table 13 **Infrastructure Server IP**

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)**.

Table 14 **Path to Custom Certificate**

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
```

3.3 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.

3.3.1 Procedure

1. In a Web browser, log in to vCenter Server by using the vSphere Client.
2. In the Hosts and Clusters inventory, select the sfo01m01vc01.sfo01.rainpole.local vCenter Server object and click the Configure tab.
3. Under the Settings section, select **Advanced Settings**.
4. Locate the config.SDDC.Deployed.InstanceId setting and write down its value.
5. In the Hosts and Clusters inventory, select the sfo01w02vc01.sfo01.rainpole.local vCenter Server object and click the **Configure** tab.
6. Under the Settings section, select **Advanced Settings** and click **Edit**.
7. 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**.

Table 15 **Advanced vCenter Server Settings**

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	5.1
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	Value obtained in Step 4

3.4 Add 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.

3.4.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. From the 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.
5. On the Licenses tab, click Add New Licenses.
6. On the Enter license keys page, enter the license keys for vCenter Server and ESXi on separate lines, and click **Next**.
7. On the Edit license name page, enter a descriptive name for the license key, and click **Next**.
8. On the Ready to complete page, review your entries, and click **Finish**.
    a. Assign the license to the Compute vCenter Server for the workload domain.
    b. Click the Assets tab and click vCenter Server systems.
    c. Select the **sfo01w02vc01.sfo01.rainpole.local** vCenter Server instance, and click the **Assign License** icon.
    d. Select the license for the Compute vCenter Server and click **OK**.

3.5 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.

3.5.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. In the Hosts and clusters inventory, expand the sfo01m01vc01.sfo01.rainpole.local tree and expand the sfo01-m01dc data center.
3. Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.
4. On the Configure page, click **VM/Host Groups**.
5. On the VM/Host Groups page, under Configuration, select the **vCenter Servers VM Group**.
6. In the vCenter Servers Group Members pane, click **Add**.
7. In the Add Group Member dialog box, select **sfo01w02vc01** and click **OK**.

3.6 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.

3.6.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. In the Networking and security inventory, click **Firewall settings**.
3. Click the **Exclusion list** tab, and, from the NSX Manager drop-down menu, select **172.16.11.65**.
4. Click the **Add** button.
5. The Select VMs to exclude dialog box opens.
6. From the Available objects section, select **sfo01w02vc01**, add it to the Selected objects section, and click **OK**.

3.7 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.

To create and configure the Shared Edge and compute cluster, perform the following tasks:

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

3.7.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. Assign Host Licenses
3. Select all ESXi hosts, right-click, select **Assign license**, select the ESXi license from the inventory of the License Service, and click **OK**.
4. 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**.

Table 16 **Join Domain Settings**

Name	Value
Domain	sfo01.rainpole.local
User Name	svc-domain-join@rainpole.local
Password	svc-domain-join_password

5. 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 and click **Edit startup policy**.
   c. In the Edit startup policy dialog box, select **Start and stop with host** and click **OK**.
6. Create the resource pools for the Shared Edge and compute cluster.
   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**.

Table 17 **Resource Pool Settings**

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	32GB	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.

7. Create a folder for the virtual machines of the NSX-T Edge devices for the inbound and outbound traffic in the workload domain.
   a. In the VMs and templates inventory, expand the **sfo01w02vc01.sfo01.rainpole.local** tree.
   b. Right-click the **sfo01-w02dc** data center and select **New folder > New VM and template folder**.
   c. In the New folder dialog box, enter **sfo01-w02fd-nsx** and click **OK**.

4 Perform the VxRail initialization to deploy the NSX-T Shared Edge and Compute Cluster

4.1 Overview

The NSX-T cluster is deployed through the VxRail initialization wizard. The cluster bring up follows the standard VxRail deployment in which the Management, vSAN, and vMotion networks are deployed along with the ESXi hosts and the defined Cluster.

The VxRail cluster will be joined to the Workload Domain vCenter server that resides in the management domain and provide the platform for the tenant workloads that use the software-defined networking capabilities of NSX-T.

This section provides details for deploying the VxRail cluster for the N-VDS Shared Edge and Compute domain.

The VxRail cluster deployed for NSX-T has different requirements than the Management Domain which is deployed with NSX-V.

The primary difference is the network, and the ability to support NSX-T alongside the vDS that is being deployed for the VxRail cluster. These two constructs must be independent which means that we require additional pNICs for the N-VDS deployment.

In a standard VxRail deployment, a VDS is deployed with VLAN backed port groups for Management, vMotion, and VSAN networks. Additional port groups are added for the NSX-V as shown in Figure 1.

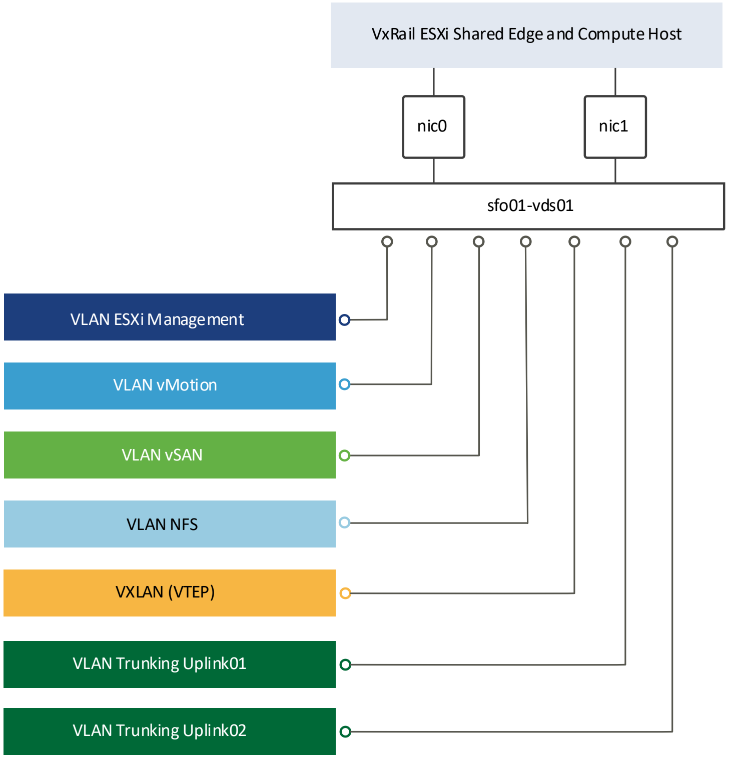


Figure 1 **VxRail vDS Network Design**

In an N-VDS deployment, the pNICs cannot be shared, so the physical host configuration is designed a bit differently as shown in Figure 2.

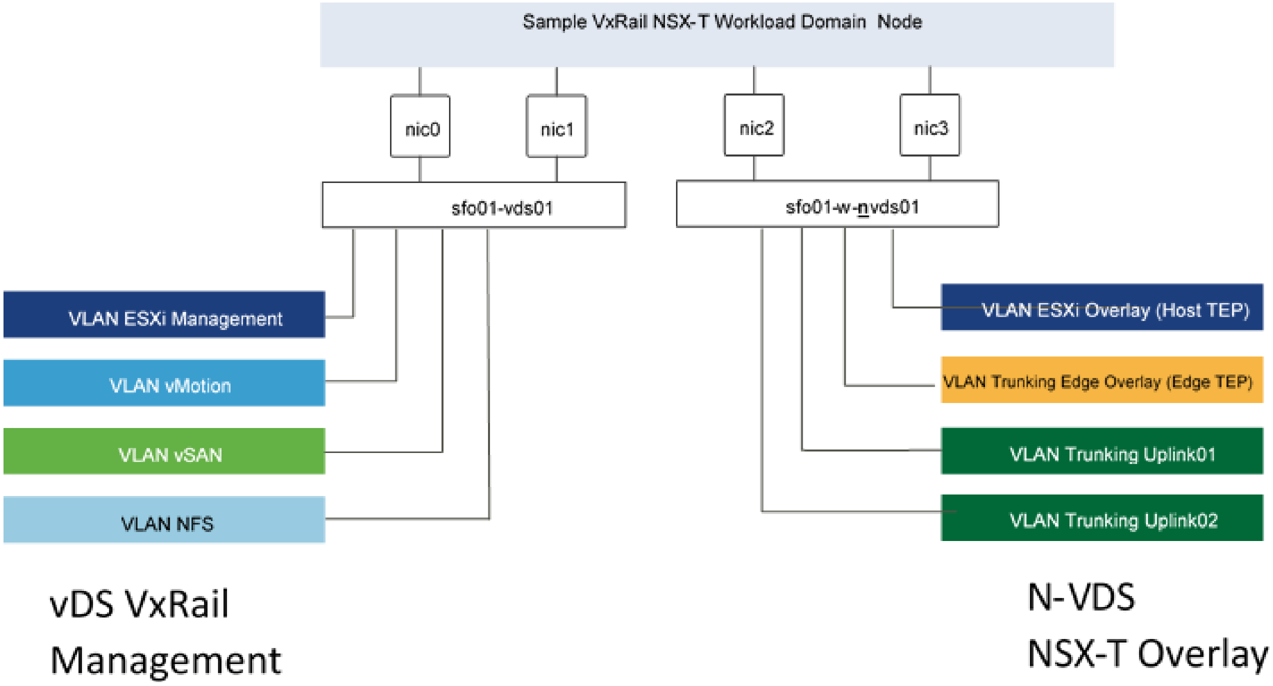


Figure 2 **VxRail vDS Network Design**

This diagram illustrates a couple of points that highlight the difference between NSX-V and NSX-T.

- The first item is that there are now two distributed switches. The vDS provides the network services for the VxRail network services, and the N-VDS provides the network services for the overlay network. The current NSX-T architecture does not permit sharing of the pNICs that support the N-VDS. You must create an additional distributed switch, and N-VDS.

- The second is the number of pNICs has doubled. As an extension to the bullet above the N-VDS deployment requires a separate set of pNICS for the deployment.

  Each VxRail node that will be used as a transport node, must include 4 pNICs which can be either 4 x 10 NDC, or a combination of NDC and PCIe.
  The first run VxRail Initialization process will deploy a vDS to support the management, vMotion, and VSAN services. The N-VDS will be deployed manually after the VxRail cluster has been deployed.

- The third item is the distribution of port groups for the NSX Overlay. In the NSX-T environment four VLAN-backed port groups are required for the overlay services. The N-VDS deployed for VVD leverages the host overlay port group for the ESXi or Host Transport zone. The uplink port groups to provide the North-South data paths and an Edge-Overlay port group provides a network for the Edge Services gateways. With the exception of the Edge Overlay, this is consistent with the VLAN requirements for the NSX-V that were used for the Management domain.

4.2 Deploy the Shared Edge and Compute VxRail cluster

When the vCenter deployment is complete, prepare the vCenter permissions and datacenter for VxRail external vCenter deployment, then perform the deployment of the VxRail Shared Edge and Compute Cluster. The full procedure is listed in the VxRail deployment with external vCenter SolVe procedure.

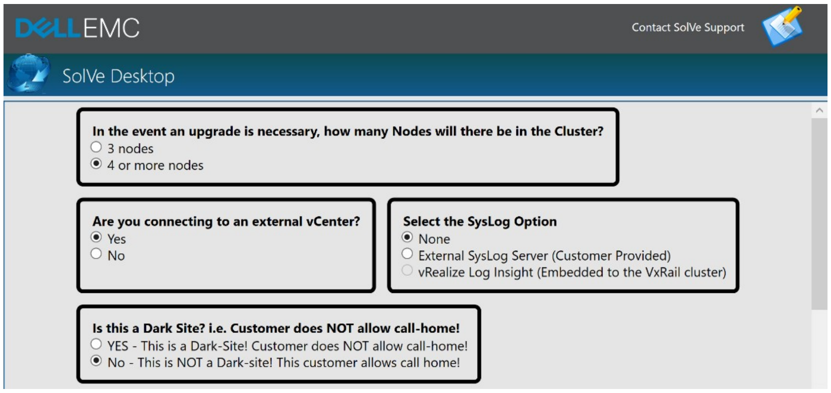
4.2.1 Before you begin

Ensure that the following tasks are complete:

- The Shared Edge and Compute vCenter Server is deployed in Region A.
- Network and top-of-rack switches are configured with the required VLANs and BGP peer interfaces.
- A Windows host exists that has access to VxRail Manager within your data center.
- (Optional) VxRail deployment JSON file exists.

4.2.2 Procedure

1. Download the VxRail Installation with External vCenter procedure from SolVe Online using the selections shown in the following figure.



In the event an upgrade is necessary, how many Nodes will there be in the Cluster?
○ 3 nodes
● 4 or more nodes

Are you connecting to an external vCenter?
● Yes
○ No

Select the SysLog Option
● None
○ External SysLog Server (Customer Provided)
○ vRealize Log Insight (Embedded to the VxRail cluster)

Is this a Dark Site? i.e. Customer does NOT allow call-home!
○ YES - This is a Dark-Site! Customer does NOT allow call-home!
● No - This is NOT a Dark-site! This customer allows call home!

Figure 4 **Installation Guide Selections**

The SolVe Tool produces the deployment guide with the detailed instructions and dependencies for deploying the VxRail external cluster.

2. Follow the procedures in the SolVe deployment documentation to complete the Shared Edge and Compute VxRail cluster deployment.
3. Refer to the information in the following tables for the manual VxRail deployment.

Table 18 **VxRail Manager, vCenter, and Platform Services Controller Details**

FQDN	IP address	VLAN ID	Default gateway
sfo01w01vxm01.sfo01.rainpole.local	172.16.11.69	1611	172.16.11.253
sfo01m01psc01.sfo01.rainpole.local	172.16.11.63	1611	172.16.11.253
sfo01w01vc01.sfo01.rainpole.local	172.16.11.64	1611	172.16.11.253

Table 19 **Management Cluster Hosts**

FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.31.101 … 172.16.31.104	1631	172.16.31.253

Table 20 **Table 15 vSAN Host Configuration**

FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.33.101 … 172.16.33.104	1633	172.16.33.253

Table 21 **Table 16 vMotion Host Configuration**

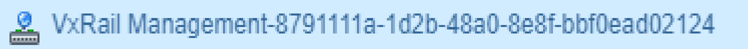
FQDN	IP address	VLAN ID	Default gateway
sfo01w01esx01 … sfo01w01esx04	172.16.32.101 … 172.16.32.104	1632	172.16.32.253

After completion of the VxRail Manager deployment, connect to VxRail Manager and confirm the health of the system.

4.3 Rename the VxRail assigned vCenter objects (optional)

The VxRail deployment assigns dynamic names to various vCenter components including the Cluster, Network Port Groups, and VSAN Datastore. VxRail allows certain objects to be renamed. This optional task renames the objects to more user-friendly names to support the ease of deployment and use within the SDDC environment.

1. Log in to the Management vCenter server (entire **sfo01w01vc01.sfo01.rainpole.local)**
2. Rename the vSAN datastore.
   a. In the Navigation pane, click **Storage** and expand the entire **sfo01w01vc01.sfo01.rainpole.local** tree.
   b. Select the **NSX-T workload domain cluster**.
   c. Select **vsanDatastore<hex id>** and select **Actions > Rename.**
   d. In the **Datastore - Rename** dialog box, enter **sfo01-w02-vsan01** as the datastore name and click **OK**.
3. Rename the vDS Switch
   a. In the navigator, click **Networking** and expand the sfow01vc01.sfo01.rainpole.local tree.
   b. Select the **sfo01-w02dc** datacenter, and select **Networking** to display the virtual distributed switch.
   c. Right-click the vDS deployed by VxRail. Right-click and select **rename**.
   d. On the Name and location page, enter **sfo01-w02-vds01** as the name and click **Ok**.
4. Rename the VxRail-defined port groups in the `sfo01-w02-vds01` distributed switch.
   a. Select the vDS for the Compute Domain vCenter in Region A.
   b. Locate each port group that was deployed by VxRail Manager.



VxRail Management-8791111a-1d2b-48a0-8e8f-bbf0ead02124

   c. Right-click the port group and rename using the following table for reference.

Table 22 **Port Group Names**

Original Group Name	New Port Group Name
sfo01-w02-vds01-management-8791111a…	sfo01-w02-vds01-management-vxrail
sfo01-w02-vds01-vmotion-8791111a…	sfo01-w02-vds01-vmotion
sfo01-m02-vds01-vsan-8791111a…	sfo01-w02-vds01-vsan
sfo01-w02-vds01-vcenter server network -8791111a…	sfo01-w02-vds01-management
sfo01-w02-vds01-VxRail-Manager-8791111a…	sfo01-w02-vds01-management-internal

5. Change the vcenter Server Network binding to **ephemeral.**
   a. Migrate the existing VM NIC of the VxRail manager and other VMs from the vCenter Network port group to the Management Port group.
   b. Select the **sfo01-w02-vds01-management** and right-click **Edit Settings.**
   c. Set the Port Binding to **Ephemeral**.
   d. Select the **Management Network → VMs**.
   e. For each VM that was migrated, highlight the **VM → Edit Settings** to set the Network Adapter back to the vCenter Network port group.

Note: The vCenter Network port group is the recommended management interface for all VMs deployed in the environment.

6. 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** page, enter **9000** as MTU (Bytes) value and click **OK**.

7. Configure the MTU of the ESXi host vMotion VMkernel adapter.
   a. Select the vMotion VMkernel adapter and click **Edit Settings**.
   b. Click the **NIC Settings** page.
   c. Enter **9000** for the MTU value and click **OK**.
   d. Repeat this task for each ESXi host.
8. Set the default gateway for the vMotion Interface
   a. Select the **vMotion VMkernel** adapter and click **Edit Settings**.
   b. Click the **IPv4 Settings** page.
   c. Select the **override default gateway for this adapter** setting.
   d. Enter the gateway address for the configured network and click **OK**.
   e. Repeat this task for each ESXi host.

4.4 Modify vSphere HA on the Shared Edge and Compute Cluster

Modify the vSphere High Availability settings on the cluster.

4.4.1 Procedure

1. Open a Web browser and log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. In the Navigator, click **Host and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.
3. Select the **sfo01-m01-mgmt01** cluster.
4. Click the **Configure** tab and click **vSphere Availability**.
5. Click **Edit**.
6. Click **Failures and Responses**, modify the following property:

Table 23 **vSphere VM Availability Settings**

Setting	Value
VM Monitoring	VM Monitoring Only

7. Click **OK**.

4.5 Configure SSH advanced options on the ESXi hosts in the Shared Edge and Compute Cluster

Enable SSH on all ESXi Hosts to support remote access. To achieve greater levels of security, change the default ESX Admins group and remove a known administrative access point.

4.5.1 Procedure

1. Open a Web browser and log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and 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. 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**.
4. 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**.

4.6 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.

4.6.1 Procedure

1. Open a Web browser and log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui https://sfo01vrli01.sfo01.rainpole.local, using with username `admin` and the vrli_admin_password
2. Click the **configuration** drop-down menu icon and select **Administration**.
3. Under Integration, click **vSphere**.
4. In the vCenter Servers pane, enter the connection settings for the vCenter Server instance.
   a. Enter the host name, user credentials, and collection options for the vCenter Server instance, and click **Test Connection**.

Table 24 **vCenter Server Connection Settings**

vCenter Server Option	**Value**
Hostname	sfo01w02vc01.sfo01.rainpole.local
Username	svc-vrli-vsphere@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 connected to the Compute vCenter Server for the additional workload domain, 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**.

5 Deploy the NSX-T instance for the Shared Edge and Compute Cluster

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, 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, deploy a cluster of three NSX-T Manager nodes.

5.1 Deploy the First NSX-T Manager Appliance

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

5.1.1 Procedure

1. Open a Web browser and log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. In the Hosts and clusters inventory, expand the sfo01m01vc01.sfo01.rainpole.local tree and expand the sfo01-m01dc data center.
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**.

Table 25 **Name and Location Settings**

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**.

Table 26 **Storage Settings**

Setting	Value
Select virtual disk format	Thin
VM Storage Policy	vSAN Default Storage Policy
Datastore	*Wld02-vSAN*

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**.

Table 27 **Customize Template Settings**

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

Table 28 **First NSX Manager Network Details**

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

Table 29 **NSX Manager Configuration Details**

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 https://sfo01wnsx01a.sfo01.rainpole.local with username admin and 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.

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

After you deploy the first NSX-T Manager appliance and 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, replace the certificate on each node.

Table 30 **Certificate Settings**

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	cert_password	cert_password	cert_password	cert_password	cert_password
Confirm Password	cert_password	cert_password	cert_password	cert_password	cert_password
Service Certificate	No	No	No	No	No

5.2.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and 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 values for sfo01wnsx01a from Table 30 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.

5.3 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. Replace the existing certificates by using the REST API of NSX-T Manager.

5.3.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username *admin* and password *nsx_admin_password*.
2. Retrieve the ID of the certificate.
3. On the main navigation bar, click **System**.
4. In the navigation pane, select **Certificates**.
5. Click the **ID** value of the sfo01wnsx01a certificate and copy it from the text box.
6. Log in to the host that has access to your data center.
7. Replace the default certificate on the NSX-T Manager appliance with the CA-signed certificate.
8. Start the Postman application in your web browser and log in.
9. On the Authorization tab, enter the following settings and click **Update Request**.

Table 31 **Authorization Settings**

Setting	Value
Type	Basic Auth
User name	Admin
Password	nsx_admin_password

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

Table 32 **Key Settings**

Setting	Value
Key	Content-Type
Key Value	Application/xml

b. In the request pane at the top, send the following HTTP request.

Table 33 **HTTP Request Settings**

Setting	Value
HTTP request method	POST
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.

10. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
11. Restart the NSX-T Manager appliance.
12. In the VMs and Templates inventory, expand the sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-nsx tree.
13. Right-click the **sfo01wnsx01a** virtual machine, and select **Power > Restart Guest OS**.

5.4 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. Connect the first NSX-T to the Management vCenter Server so that you can place the remaining NSX-T Manager nodes on the management cluster later.

Table 34 **vCenter Server Settings**

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	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

5.4.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_admin_password.
2. Add the Compute vCenter Server for the workload domain to NSX-T Manager.
3. On the main navigation bar, click **System**.
4. In the navigation pane, select **Fabric > Compute Managers**.
5. Click **Add**, enter the following values, and click **Add**.

Table 35 **Compute vCenter Server Settings**

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

6. 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, the Compute Managers page shows the following status.

Table 36 **Compute Managers Status**

Setting	Value
Registration Status	Registered
Connection Status	Up

7. Repeat the previous step to connect the first NSX-T Manager node to the Management vCenter Server.

5.5 Deploy the Remaining Nodes of the NSX-T Manage Cluster

Implement high availability of NSX-T Manager by deploying the remaining two nodes of the NSX-T Manager cluster on the management cluster.

5.5.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username *admin* and 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**.

Table 37 **Common Attributes Settings**

Setting	Value
Compute Manager	sfo01m01vc01
Enable SSH	Yes
Enable Root Access	No
CLI Password / Confirm CLI Password	nsx_cli_password
Root Password / Confirm Root	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.

Table 38 **NSX-T Node 2 Settings**

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

Table 39 **NSX-T Node 3 Settings**

Setting	Value
Name	sfo01wnsx01b
Cluster	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Network	sfo01-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.

5.6 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.

5.6.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_admin_password`.
2. In the Hosts and clusters inventory, expand the sfo01m01vc01.sfo01.rainpole.local tree and expand the sfo01-m01dc data center.
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 rule settings and click **Add**.

Table 40 **Affinity Rule Settings**

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**.

5.7 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.

5.7.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and 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 in the **sfo01-m01fd-nsx** folder.
4. Drag sfo01wnsx01c and drop it in the **sfo01-m01fd-nsx** folder.

5.8 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, import the certificates through the NSX-T Manager user interface and replace the existing certificates using a REST API client.

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

Table 41 **NSX-T Manager Certificate Replacement REST API**

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

5.8.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username *admin* and 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 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 these settings and click **Update Request**.

Table 42 **REST API Authorization Settings**

Setting	Value
Type	Basic Auth
User name	admin
Password	nsx_admin_password

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

Table 43 **REST API Header Settings**

Setting	Value
Key	Content-Type
Key Value	Application/xml

d. In the request pane at the top, send the URL query.

Table 44 **REST API URL Settings**

Setting	Value
HTTP request method	POST
URL	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. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and 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.

5.9 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.

5.9.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username *admin* and 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 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 these settings and click **Update Request**.

Table 45 **Authorization Settings**

Setting	Value
Type	Basic Auth
User name	Admin
Password	Nsx_admin_password

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

Table 46 **Header Settings**

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, send the URL query.

Table 47 **Post Settings**

Setting	Value
Key	Content-Type
Key Value	https://sfo01wnsx01b.sfo01.rainpole.local/api/v1/node/services/http?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.

5.10 Assign a Production License to NSX-T

Use the user interface of NSX-T Manager to replace the evaluation license for NSX-T with a production one.

5.10.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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**.

5.11 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.

Table 48 **NSX-T Logical Network Settings**

Name	N-VDS Name	N-VDS Mode	Traffic Type
sfo01-w02-uplink01	sfo01-w02-uplink01	Standard	VLAN
sfo01-w02-uplink02	sfo01-w02-uplink02	Standard	VLAN
sfo01-esxi-vlan	sfo01-w02-nvds01	Standard	VLAN
sfo01-w02-overlay	sfo01-w02-nvds01	Standard	Overlay

5.11.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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**.

Table 49 **Transport Zone Settings**

Setting	Value
Name	sfo01-w02-uplink01
N-VDS Name	sfo01-w02-uplink01
N-VDS Mode	Standard
Traffic Type	VLAN

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

5.12 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 the priority of the traffic.

5.12.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_admin_password.
2. On the main navigation bar, click System.
3. In the navigation pane, select **Fabric > Profiles**.
4. To define policies for the links between the ESXi hosts and segments and between NSX-T Edge nodes and top of rack switches, create uplink profiles.
   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**.

Table 50 **Uplink Profile Settings**

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

5. In the esxi-w02-uplink-profile profile, create two teaming policies for ECMP uplinks.
    a. On the Uplink Profiles tab, select the **esxi-w02-uplink-profile** profile and click **Edit**.
    b. In the Edit Uplink Profile dialog box, under Teamings, click the **Add** button, enter the following information, and click **Save**.

Table 51 **Teaming Policy Settings**

Name	Teaming Policy	Active Uplinks
Uplink01	Failover Order	Uplink-1
Uplnk02	Failover Order	Uplink-2

6. Include the new teaming policies in the transport zone.
    a. Navigate to **Fabric > Transport Zones**, select **sfo01-esxi-vlan** and click **Edit**.
    b. In the Edit Transport Zone dialog box, add Uplink01 and Uplink02 to Uplink Teaming Policy Names and click **Save**.
7. Create a Network I/O Control profile for allocating 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.

Table 52 **NOIC Profile Settings**

Setting	Value
Name	sfo01-w02-nioc-profile
Status	Enabled

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

Table 53 **Host Infra Traffic Settings**

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

5.13 Create the NSX-T segments for system, uplink, and overlay traffic

Create the segments to connect nodes that send VLAN and overlay traffic. Perform this procedure for each segment.

Table 54 **NSX-T Segments**

Segment Name	Uplink & Type	Transport Zone	VLAN
sfo01-w02-nvds01-uplink01	None	sfo01-esxi-vlan	0-4094
sfo01-w02-nvds01-uplink02	None	sfo01-esxi-vlan	0-4094
sfo01-w02-uplink01	None	sfo01-w02-uplink01	1647
sfo01-w02-uplink02	None	sfo01-w02-uplink01	1648
sfo01-w02-overlay	None	sfo01-esxi-vlan	0-4094
sfo01-w02-ubuntu-01	None	sfo01-esxi-vlan	1649

Note: Certain network segments for VxRail are not configured in the NSX-T environment. Those networks for Management, vMotion and VSAN will remain on the vDS network deployed during the VxRail initialization.

5.13.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and password `vsphere_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-w02-nvds01-uplink01 segment and click **Save**.

Table 55 **Segment Settings**

Setting	Value
Name	sfo01-w02-nvds01-uplink01
Uplink & Type	None
Transport Zone	sfo01-esxi-vlan
VLAN	0-4094

6. Repeat this procedure to create the remaining segments.
7. On the main navigation bar, click **Advanced Networking and Security**.
8. Under Networking, click **Switching**.
9. Change the teaming policy for sfo01-w02-nvds01-uplink01 and sfo01-w02-nvds01-uplink02.
    a. Select **sfo01-w02-nvds01-uplink01** and click **Edit**.
    b. In the **Edit** dialog box, select **Uplink01** from the Uplink Teaming Policy Name drop-down menu and click **Save**.
    c. Select **sfo01-w02-nvds01-uplink02** and click **Edit**.
    d. In the Edit dialog box, select **Uplink02** from the Uplink Teaming Policy Name drop-down menu and click **Save**.

5.14 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.

5.14.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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.

Table 56 **Transport Node Profile settings**

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

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

Table 57 **Node Switch Settings**

Setting	Value
N-VDS Name	sfo01-w02-nvds01
NIOC Profile	sfo01-w02-nioc-profile
Uplink Profile	esxi-w02-uplink-profile
LLDP Profile	LLDP [Send Packet Enabled]
IP Assignment	Use DHCP
Physical NICs	vmnic2 > uplink-1 vmnic3> uplink-2

7. Click Add to save the profile.

5.15 Configure the ESXi Host Transport Nodes

To use NSX-T, configure the ESXi hosts in the Shared Edge and compute cluster as transport nodes. The NSX-T Manager then 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.

5.15.1 Procedure

1. Log into the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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-shared01 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.

Table 58 **Transport Node Settings**

Setting	Value
NSX Configuration	Configured
Configuration State	Success
Node State	Up
Transport Zones	sfo01-esxi-vlan sfo01-w02-overlay
NSX Version	2.4.1
N-VDS	1

6 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.

6.1 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.

6.1.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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**.

Table 59 **Edge Cluster Profile Settings**

Setting	Value
Name	sfo01-w02-edge-cluster01-profile
BFD Probe	1000
BFD Declare Dead Multiple	3

6.2 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.

Table 60 **NSX-T Edge Node Settings**

Setting Value for sfo01wesg01	Value for sfo01wesg01	Value for sfo01wesg02
Name	sfo01wesg01 sfo01wesg01	sfo01wesg01 sfo01wesg02
Port Groups	sfo01-w02vds01-management	sfo01-w02vds01-management
Primary IP Address	172.16.41.21	172.16.41.22

The following figure illustrates the logical deployment of an Edge Virtual Machine deployed within a VVD on VxRail environment.

There is no management port group within the N-VDS. The management interface for the Edge VM must be assigned to the management network defined for the VxRail cluster.

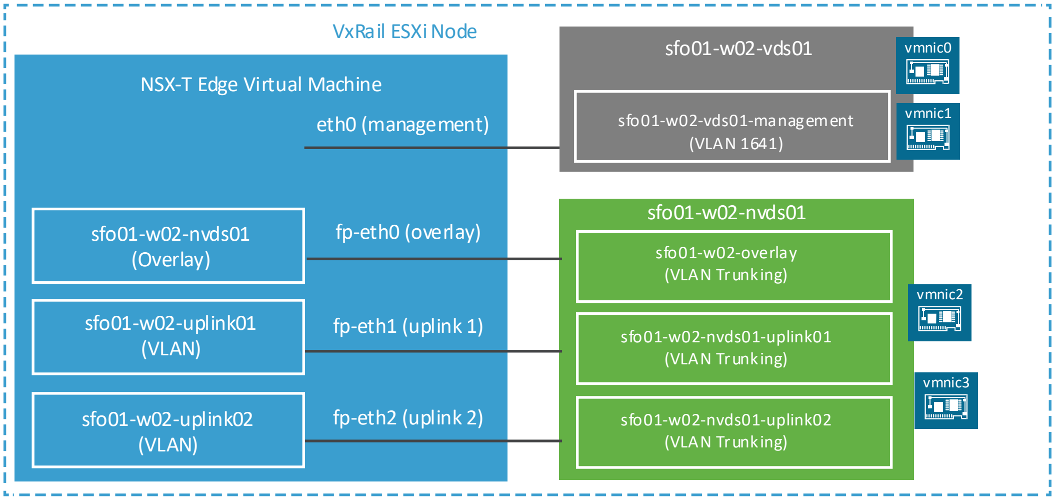

VxRail ESXi Node
NSX-T Edge Virtual Machine
eth0 (management)
sfo01-w02-nvds01 (Overlay)
fp-eth0 (overlay)
sfo01-w02-uplink01 (VLAN)
fp-eth1 (uplink 1)
sfo01-w02-uplink02 (VLAN)
fp-eth2 (uplink 2)
sfo01-w02-vds01
sfo01-w02-vds01-management (VLAN 1641)
sfo01-w02-nvds01
sfo01-w02-overlay (VLAN Trunking)
sfo01-w02-nvds01-uplink01 (VLAN Trunking)
sfo01-w02-nvds01-uplink02 (VLAN Trunking)
vmnic0
vmnic1
vmnic2
vmnic3

Figure 3 Edge Virtual Machine logical network design.

6.2.1 Procedure

1. Open a Web browser, log in to vCenter Server, https://sfo01m01vc01.sfo01.rainpole.local/ui, using the vSphere Client with username `administrator@vsphere.local` and 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**.

Table 61 **Name and Location Settings**

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**.

Table 62 **Network Settings**

Source Network	Destination Network
Network 3	sfo01-w02-nvds01-uplink02
Network 2	sfo01-w02-nvds01-uplink01
Network 1	sfo01-w02-overlay
Network 0	sfo01-w02-**vds01**-management*

*This port group resides on the workload cluster vDS.

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

Table 63 **User/Password Settings**

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_audit_password

Table 64 **Need table title**

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
DNS Server	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.

6.3 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, connect them to the NSX-T Manager cluster by joining them to the management plane.

Table 65 **Port Group Settings**

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Name	sfo01wesg01	sfo01wesg02
Port Groups	sfo01-w02-vds01-management*	sfo01-w02-vds01-management*
Primary IP Address	172.16.41.21	172.16.41.22

*This port group resides on the workload cluster vDS.

6.3.1 Procedure

1. Log in to the NSX-T Manager cluster Open a Web browser, log in to the NSX-T Manager cluster https://sfo01wnsx01a.sfo01.rainpole.local with username `admin` and 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 command `get certificate cluster thumbprint`
3. Log in to the first NSX-T Edge node by using Secure Shell (SSH) client with the following values.

Table 66 **Log in Credentials**

Setting	Value
FQDN	sfo01wesg01.sfo01.rainpole.local
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
```
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.

6.4 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.

6.4.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with user name `admin` and password `nsx_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**.

Table 67 **Anti-Affinity Rule Settings**

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**.

6.5 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, connect the nodes to the workload domain by adding them to the transport zones for uplink and overlay traffic, and configure the NVDS switches on each edge node.

6.5.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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**.

Table 68 **Transport Zone Settings**

Setting	Value for sfo01wesg01	Value for sfo01wesg02

Transport Zones	sfo01-w02-uplink01(VLAN)
	sfo01-w02-uplnk02(VLAN)
	sfo01-w02-overlay (Overlay)
		sfo01-w02-uplink01(VLAN)
		sfo01-w02-uplnk02(VLAN)
		sfo01-w02-overlay (Overlay)

7. Under Edit Transport Node - sfo01wesg01, click the **N-VDS** tab.
8. Under **New Node Switch**, enter the switch configuration.

Table 69 **New Node Switch Configuration Settings**

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w02-nvds01	sfo01-w02-nvds01
Uplink Profile	sfo01-w02-overlay-profile	sfo01-w02-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 uplink01	fp-eth0 uplink01

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

Table 70 **N-VDS Switch Configuration Settings**

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w02-nvds01-uplink01	sfo01-w02-nvds01-uplink01
Uplink Profile	sfo01-w02-uplink01-profile	sfo01-w02-uplink01-profile
IP Assignment	Greyed Out	Greyed Out
Virtual NICs	fp-eth0 uplink01	fp-eth0 uplink01

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

Table 71 **N-VDS Settings**

Setting	Value for sfo01wesg01	Value for sfo01wesg02
Edge Switch Name	sfo01-w02-nvds01-uplink02	sfo01-w02-nvds01-uplink02
Uplink Profile	sfo01-w02-uplink02-profile	sfo01-w02-uplink02-profile
IP Assignment	Greyed Out	Greyed Out
Virtual NICs	fp-eth0 uplink01	fp-eth0 uplink01

11. Repeat the step on sfo01wesg02.

The edge transport nodes have the following configuration:

Table 72 **Edge Transport Node Settings**

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-w02-overlay • sfo01-w02-uplink01 • sfo01-w02-uplink02	• sfo01-w02-overlay • sfo01-w02-uplink01 • sfo01-w02-uplink02
N-VDS	3	3

6.6 Create an NSX-T Edge Cluster

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

6.6.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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.

Table 73 **Edge Cluster Settings**

Setting	Value
Name	sfo01-w02-edge-cluster01
Edge Cluster Profile	sfo01-w02-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 to the selected list.
8. Click **OK** and click **Add**.

6.7 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.

6.7.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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**.

Table 74 **Tier-0 Gateway Settings**

Setting	Value
Name	sfo01-w02-tier-0-01
High Availability Mode	Active-Active
Edge Cluster	sfo01-w02-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 Interfaces dialog box, click **Add Interface** and enter the settings of the uplink

Table 75 **User Interface Settings**

Name	Type	IP Address / Mask	Connected To (segment)	Edge Node	MTU
sfo01wesg01-Uplink01	External	172.16.47.2/24	sfo01-w02-uplink01	sfo01wesg01	9000
sfo01wesg01-Uplink02	External	172.16.48.2/24	sfo01-w02-uplink02	sfo01wesg01	9000
sfo02wesg01-Uplink01	External	172.16.47.3/24	sfo01-w02-uplink01	sfo01wesg02	9000
sfo02wesg01-Uplink02	External	172.16.48.3/24	sfo01-w02-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**.

Table 76 **BGP Settings**

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.

Table 77 **Layer 3 Device Settings**

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 only if the network supports and is configured for BFD.

7. Repeat for the other neighbor, click **Save** and click **Close**.
8. Click **Close Editing**.

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

6.7.2.1 Procedure

1. In the main navigation bar, click **Advanced Networking & Security.**
2. Select Routers and select sfo01-w02-tier-0-01.
3. Select Actions > Generate BGP Summary.
4. Verify the Connection Status of each transport node is Established.

6.8 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.

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

6.8.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username `admin` and password `nsx_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 configuration of the Tier-1 gateway.

Table 78 **Tier-1 Gateway Configuration Settings**

Setting	Value
Name	sfo01-w02-tier-1-01
Linked Tier-0 Gateway	sfo01-w02-tier0-01
Failover	Preemptive
Edge Cluster	sfo01-w02-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 configuring the Tier-1 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 Linked Port has the following settings.

Table 79 **Linked Port Settings**

Setting	Expected Value
Logical Router	LinkedPort_sfo01-w02tier-0-01
Type	Linked Port
IP Address/mask	x.x.x.x/31
Connected To	sfo01-w02-tier-0-01
Transport Node	• sfo01wesg01, • sfo01wesg02

   e. Select the **sfo01-w02-tier-0-01** gateway.
   f. Select **Configuration > Router Ports**, and verify that the existing Linked Port has the following settings.

Table 80 **Router Port Settings**

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

6.9 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.

6.9.1 Procedure

1. Log in to sfo01wesg01 by using a Secure Shell (SSH) client and the following settings.

Table 81 **Log in Credentials**

Setting	Value
FQDN	sfo01wesg01
User name	admin
Password	nsx_edge_admin_password

2. Get information about the Tier-0 and Tier-1 service routers and distributed router using the following command: `get logical-router`.
   For example, the output of the command might contain the following configuration:

Table 82 **Command Output Example**

UUID	VRF	LR-ID	Name	Type	Ports
sample_uuid	0	0		TUNNEL	3
Type	1	5	SR-tier0-01	SERVICE_ROUTER_TIER0	6
IP Address/ mask	2	2	DR-tier1-01	DISTRIBUTED_ROUTER_TIER1	5
Connected To	3	3	DR-tier0-01	DISTRIBUTED_ROUTER_TIER1	4
Transport Node	4	11	SR-tier1-01	SERVICE_ROUTER_TIER0	5

3. Use the VRF value for SERVICE_ROUTER_TIER0 to 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 using the following command: `get route`
6. Repeat this procedure on sfo01wesg02.

7 Deploy a segment for a sample tenant workload

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.

7.1.1 Procedure

1. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with username admin and password nsx_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-w02-ubuntu-01 segment, click the **vertical ellipsis icon** and click **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**.

7.1.2 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.

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

After you deploy the NSX-T components in the new workload domain, connect vRealize Log Insight to the NSX-T instance to start collecting log information.

8.1 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.

Repeat this procedure for the following NSX-T components.

Table 83 **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

8.1.1 Procedure

1. Open an SSH connection to the first NSX-T Manager appliance.
2. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with user name `admin` and password `nsx_admin_password`.
3. To set up log forwarding to vRealize Log Insight, run the following command.

   ```
   set logging-server 192.168.31.10 proto udp level info
   ```
4. To verify that log forwarding is configured, run the following command.

   ```
   get logging-servers
   ```
5. Repeat the procedure for all NSX-T Manager and NSX-T Edge nodes.

9 Back Up and Restore the NSX-T Instance for the Shared Edge and Compute Cluster

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 cannot make any configuration changes.

9.1 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.

9.1.1 Procedure

1. In a Web browser, log in to the user interface of NSX-T Manager.
2. Log in to the user interface of the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with user name `admin` and password `nsx_admin_password`.
3. On the main navigation bar, click **System**.
4. In the navigation page, select **Backup & Restore**.
5. On the Backup tab, click **Edit**.
6. On the File Server page, enter the following values and click **Save**.

Table 84 **Backup and Restore Settings**

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.

.

7. On Schedule tab, configure the following settings and click **Save**.

Table 85 **Schedule Settings**

Setting	Value
Automatic Backup	Enabled
Frequency	Weekly
Days	All days
Time	22:00
Detect NSX configuration change	Enabled
Update Interval	5 min

9.2 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.

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.

9.2.1 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 the first NSX-T Manager appliance https://sfo01wnsx01a.sfo01.rainpole.local with user name `admin` and password `nsx_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**.

Table 86 **Restore Settings**

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.