Installing Cisco VTS

If your Cisco NFVI package includes Cisco Virtual Topology System, the following topics tell you how to install Cisco VTS for use with Cisco NFVI. The Cisco VTS installation procedures are customized for Cisco NFVI from the standard Cisco VTS 2.3 installation procedures located on the Cisco VTS product site. You must install Cisco VTS before you install Cisco VIM.

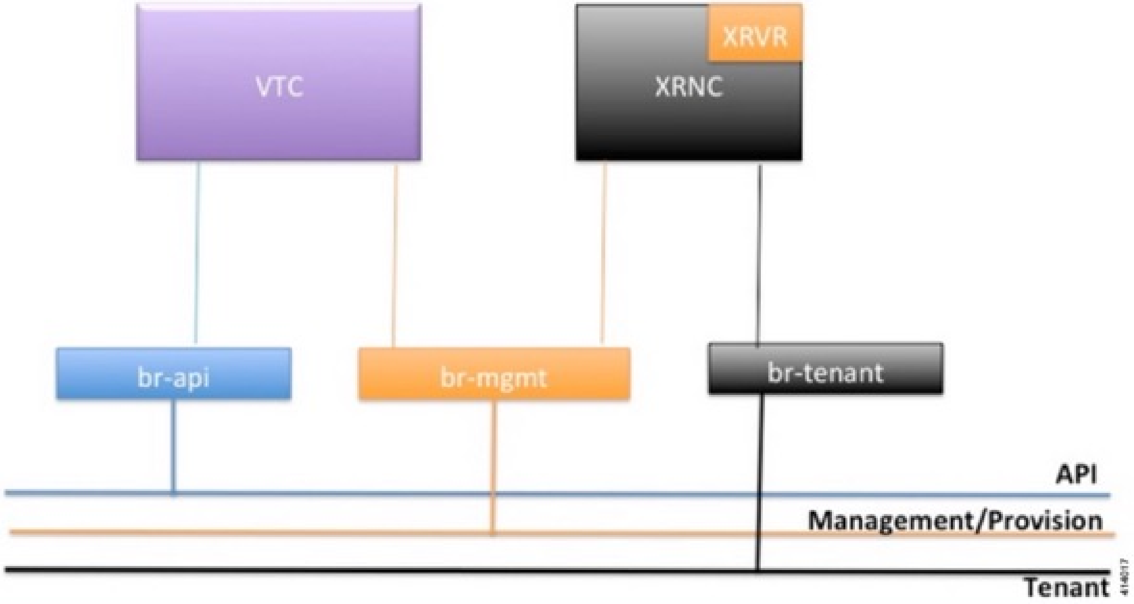
Overview to Cisco VTS Installation in Cisco NFVI

The Cisco Virtual Topology System (VTS) is an overlay management and provisioning system for data center networks. It automates data center overlay fabric provisioning for both physical and virtual workloads. It provides a policy-based approach for overlay provisioning, and can be used for multitenant data centers for cloud services, including Cisco NFVI.

To install Cisco VTS with Cisco NFVI, you must manually install the Cisco VTS Virtual Topology Controller (VTC) and its XRNC and XRVR VMs before you start the Cisco VIM installation. The VTC and XRNC VMs must be run on an independent pair of servers, that is, not on a Cisco NFVI control, compute, storage, or management node. You set up the networking on those servers as described below and outlined in the installation procedures. When you run the Cisco VIM installer, you will provide the VTC VIP and appropriate VTS credentials.

The following figure shows how Cisco VTS Virtual Topology Controller (VTC) and the IOS XRv (XRNC and XRVR) virtual machines (VMs) connect to the Cisco NFVI networks.

Figure 1: Cisco VTS Connectivity to Cisco NFVI



The following table maps Cisco VTS network names to Cisco VIM network names.

Table 1: Cisco VTS to Cisco VIM Network Name Mapping

Cisco VTS VM	Cisco VTS Network Name	Cisco VIM Network Name
VTC	Management Network	API (a)
VTC	Underlay Network	Management/Provision (mx)
XRNC/XRVR	Management Network	Management/Provision (mx)
XRNC/XRVR	Underlay Network	Tenant (t)

The following table describes the required IP address allocations for VTS components.

Table 2: Cisco VTS IP Address Allocations

Cisco VIM Network	Required Cisco VTS IP Addresses	Description
API (a)	3 total (1 VIP + 1 IP per VTC VM)	Set up in the VTC config.iso and cluster.conf

Cisco VIM Network	Required Cisco VTS IP Addresses	Description
Management/Provisioning (mx)	• 7 total—Three for VTC (one VTC VIP and one IP per VTC VM) • Four for XRNC: one IP address pair per XRNC/XRVR VM, one IP address for XRVR and the other to XRNC	Set up in XRNC config.iso and XRNC_HA.sh **Note**: VTS component IP addresses cannot overlap with the pool ranges configured in the Cisco VIM setup_data.yaml.
Tenant (t)	4 total—(one IP address pair per XRNC/XRVR VM, one IP address goes to the XRVR tenant interface and other to XRNC tenant interface	Set up in XRNC config.iso **Note**: The VTS component IPs cannot overlap with pool ranges configured in the Cisco VIM setup_data.yaml.

The VTS IP distribution and setup mechanism are listed below.

VIM API network

- VTC1—api (a) network IP1 (associated through the VTC1 config ISO)
- VTC2—api (a) network IP2 (associated through the VTC2 config ISO)
- VTC VIP—api (a) network IP3 (associated through the HA step cluster.conf)

VIM Management/Provisioning network

- VTC1—management/provisioning (mx) network IP1 (associated through the VTC1 config ISO)
- VTC2—management/provisioning (mx) network IP2 (associated through the VTC2 config ISO)
- VTC VIP—management/provisioning (mx) network IP3 (associated through the HA step cluster.conf)
- XRNC/XRv 1—management/provisioning (mx) network IP4 (associated through the XRNC-1 config ISO)
- XRNC/XRv 2—management/provisioning (mx) network IP5 (associated through the XRNC-2 config ISO)
- XRNC/XRv VIP—management/provisioning (mx) network IP6 (associated through the XRNC-1 & 2 config ISOs)

VIM Tenant network:

- XRNC/XRv 1—tenant (t) network IP1 (associated through the XRNC-1 config ISO)
- XRNC/XRv 2—tenant (t) network IP2 (associated through the XRNC-2 config ISO)
- XRNC/XRv VIP—tenant (t) network IP3 (associated through the XRNC-1 & 2 config ISOs)

Cisco VTS Usernames and Passwords in Cisco NFVI

The following table lists the Cisco VTS usernames and passwords that are employed after you install Cisco VTS in Cisco NFVI.

Table 3: Cisco VTS Usernames and Passwords in Cisco NFVI

Configuration Location	Value Requirements	Description/Comments
mercury: openstack-configs/setup_data.yaml VTS_PARAMETERS: VTS_USERNAME VTS_PASSWORD	VTS_USERNAME must be admin VTS_PASSWORD must match VTC UI login password for the admin user. Password must have a minimum of 8 characters and at least one uppercase letter, one digit, and one special character.	Used by VTF to register with the VTC / XRNC.
VTC ISO config.txt : vts-adminPassword	Must match the Cisco VIM setup_data.yaml VTS_PASSWORD parameter.	Configures VTC admin user initial password.
VTC ISO config.txt : AdministrativeUser AdministrativePassword	SSH username/password for VTC VM	SSH username/password for VTC VM
XRNC ISO: USERNAME PASSWORD_HASH	username cannot match XRVR_USERNAME PASSWORD_HASH must be generated from: openssl passwd -1 -salt xxx <password>	XRNC VM ssh username/password
XRNC ISO: XRVR_USERNAME XRVR_PASSWORD_HASH	username cannot match USERNAME	XRVR VM SSH username/password The XRVR adds this in VTS Inventory > Authorization Group > vtsgroup3 Device User Name associated with VTC admin user

System Requirements for VTC VM

The following table provides information about the minimum system requirements for the VTC virtual machine:

Requirement	Details
Disk space	48 GB
CPU	8
Memory	16 GB

Requirement	Details
Computing Host	Certified with Cisco UCS B-series, Cisco UCS C-series Rack Servers
Hypervisor	• VMware ESXi 5.5 • VMware ESXi 6.0U1 or later • Red Hat Enterprise Linux 7.1 with KVM

System Requirements for IOS XRv VM

The following table gives details about the minimum system requirements for the IOS XRv virtual machine:

Note The IOS XRv VM serves two purposes. It is required to enable VTS High Availability. It also acts as the control plane for the VTF. You need to install IOS XRv only if you consider enabling High Availability or if you plan to have a VTF in your set up.

Requirement	Details
Disk Space	Primary disk must be 2 GB.
CPUs	6
Memory	32 GB RAM
Computing Host	Certified with Cisco UCS B-series, Cisco UCS C-series Rack Servers
Hypervisor	• VMware ESXi 5.5 or VMware ESXi 6.0 • Red Hat Enterprise Linux 7.1 with KVM

System Requirements for VTF

The following table gives details about the minimum system requirements for the VTF virtual machine:

Note This section is applicable only if you have VTFs in your setup.

Requirement	Details
Disk Space	8 GB

CPU Cores	2
Memory	16 GB RAM
Hypervisor	• VMware ESXi 5.5 or VMware ESXi 6.0 • Red Hat Enterprise Linux 7.1 with KVM
Server network interface card (NIC)	Intel DPDK-supported NIC

For details about the requirements to install VTF in vhost mode, you must have Red Hat Enterprise Linux 7.2 running on the host machine. Additional requirements are: VIC Details-Cisco UCS VIC 1225,1227, and 1385.

Supported Virtual Machine Managers

Cisco VTS can be installed on the following supported versions of VMMs:

- OpenStack
- VMware vCenter

Supported Platforms

The following tables provide information about the platforms that Cisco VTS support, and their roles.

Note VTS supports VXLAN overlays using the BGP EVPN control plane.

Role	Platform Supported
Top-of-rack (ToR) leaf switch	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9332PQ and 93128TX switches • Cisco Nexus 9200 platform switches • Cisco Nexus 5600 platform switches • Cisco Nexus 9500 platform switches • Cisco Nexus 7x00 platform switches

Data center spine	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9500 platform switches • Cisco Nexus 9200 platform switches • Cisco Nexus 7x00 Series switches • Cisco Nexus 5600 platform switches
Border leaf	• Cisco Nexus 9300TX and 9300PX platform switches • Cisco Nexus 9500 platform switches • Cisco Nexus 9200 platform switches • Cisco Nexus 5600 platform switches • Cisco Nexus 7x00 platform switches
Data center interconnect (DCI)	• Cisco ASR 9000 Series Aggregation Services routers • Cisco Nexus 7x00 Series switches • Cisco Nexus 9300 platform switches
Fabric Extenders (FEX)	• Cisco Nexus C2248TP-E9500 • Cisco Nexus C2232PP FEX support is available for Cisco Nexus 9300, Cisco Nexus 5600, Cisco Nexus 9500 and Cisco Nexus 7x00 switches.
Hypervisor	• VMware ESXi 5.5; VMware ESXi 6.0 • Red Hat Enterprise Linux 7.1 with KVM

Note Cisco Nexus 5672 does not interoperate with Cisco Nexus 93xx or 95xx.

The following table lists the software images supported for the different devices.

Table 4: Software Images Supported

Cisco Nexus 93xx	NX OS Release 7.0(3)I2(2a) or 7.0(3)I2(2c)
Cisco Nexus 95xx	NX OS Release 7.0(3)I1(1b).

Cisco Nexus 7x00	• Data center spine —For Cisco Nexus 7000—7.3(0)D1(1); For Cisco Nexus 7700—7.3(0)DX(1) • Data center interconnect (DCI): • VRF Peering mode—NX OS Release 7.3.1 and later. • Integrated DCI mode—NX OS Release 7.3.1 and later.
Cisco Nexus 5600	NX OS Release 7.3(0)N1(1) and later.
Cisco ASR 9000	Cisco IOS XR Software Release 5.3.2 and later.

The following table lists the VPC modes supported for the different devices.

Note If Cisco Nexus 9000 series ToR is not configured with vPC related configuration, including peer-link, also known as a multichassis etherChannel trunk (MCT), you must not configure feature vpc on the ToR. This may bring loopback interface used for NVE to admin down state.

Table 5: VPC Modes Supported

Cisco Nexus 93xx	Server VPC
Cisco Nexus 95xx	Server VPC
Cisco Nexus 5600	Server VPC, FEX VPC, Enhanced VPC
Cisco Nexus 7000	Host VPC and single-homed host in port channel mode.

Installing Cisco VTS in a Cisco NFVI Environment

Installing Cisco VTS inside Cisco NFVI involves installing the Virtual Topology Controller (VTC) VM. You can install the VTC VM using either the automatic or manual configuration options.

- To install the VTC VM using an ISO file (auto configuration), see Installing VTC VM - Automatic Configuration Using ISO File, on page 8.
- To install the VTC VM using the virt-manager application (manual configuration), see Installing VTC VM - Manual Configuration Using virt-manager, on page 10.
- To install the VTC VM using VNC (manual configuration), see Installing VTC VM - Manual Configuration using VNC, on page 11

Installing VTC VM - Automatic Configuration Using ISO File

To install a VTC VM and enable configuration using an ISO file, create a text file with the VM settings, wrap the text file in an ISO file, and then attach the ISO file to the VM CD drive.

Step 1 Connect to the controller node via SSH, and copy the vtc.qcow2 file to /var/lib/libvirt/images/ folder.

Step 2 Copy the vtc.sample.xml file to your controller. The Sample Cisco VTS Configurations for Cisco NFVI, on page 23 topic provides the file contents.

Step 3 Create a **config.txt** file containing the following parameters:

```
    Hostname=vtc
ManagementIPv4Method=Static
ManagementIPv4Address= <VM's a-net IP address in a.b.c.d form>
ManagementIPv4Netmask= <a-net IP mask in a.b.c.d form>
ManagementIPv4Gateway= <a-net gateway IP address in a.b.c.d form>
UnderlayIPv4Method=Static
UnderlayIPv4Address= <VM's mx-net IP address in a.b.c.d form>
UnderlayIPv4Netmask=<mx-net IP mask in a.b.c.d form>
DNSv4=<DNS server--ie. setup_data.yaml::NETWORKING['domain_name_servers'][0]>
Domain=<domain name--ie. setup_data.yaml::NETWORKING['domain_name']>
NTPv4=<NTP server--ie. setup_data.yaml::NETWORKING['ntp_servers'][0]>
vts-adminPassword=<password for user 'admin'--setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']>
AdministrativeUser=<VM ssh login user--can be setup_data.yaml::VTS_PARAMETERS['VTS_USERNAME']>
AdministrativePassword=<VM ssh login user--can be setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']>
```

Note The *config.txt file* must have a blank line at the end.

Note Before entering the VTS_PASSWORD, review Cisco VTS Usernames and Passwords in Cisco NFVI, on page 4.

Parameter descriptions:

- Hostname—The VM hostname.
- ManagementPv4Method—Whether to use DHCP or static addressing for the Cisco NFVI API network (a-net) interface (eth0).
- ManagementIPv4Address—The api (a) network IPv4 address of the VM (required only for static addressing).
- ManagementIPv4Netmask—The a network IPv4 netmask of the VM (required only for static addressing).
- ManagementIPv4Gateway—The a network API IPv4 gateway of the VM (required only for static addressing).
- UnderlayIPv4Method—Whether to use DHCP or static addressing for the Cisco NFVI management/provisioning (mx) network interface (eth1).
- UnderlayIPv4Address—The mx network IPv4 address of the VM (required only for static addressing).
- UnderlayIPv4Netmask—The mx network IPv4 netmask of the VM (required only for static addressing).
- DNSv4—DNS IPv4 address (required only for static addressing).
- Domain—DNS search domain (required only for static addressing).
- NTPv4—NTP IPv4 address or FQDN (required only for static addressing).
- vts-adminPassword—Password for the vts-admin user. This should match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']
- AdministrativeUser—New administrative user for login using SSH.
- AdministrativePassword—Password for the new administrative user.

Step 4 Use mkisofs to create an ISO file, for example:

```
mkisofs -o config.iso config.txt
```

Step 5 Create the VTC VM using following command:

```
virsh create vtc.sample.xml
```

Installing VTC VM - Manual Configuration Using virt-manager

To install the VTC VM configuring it manually using the virt-manager application:

Step 1 Connect to the controller node via SSH, and copy the vtc.qcow2 file to /var/lib/libvirt/images/ folder.

Step 2 Copy the Cisco NFVI vtc.sample.xml file to your controller. Modify it as per your setup. See Sample Cisco VTS Configurations for Cisco NFVI, on page 23 for examples.

Step 3 Create the VTC VM using following command:

```
virsh create vtc.sample.xml
```

Step 4 Run the command:

```
virsh list --all
```

It should display:

```
Id      Name      State
--------------------------------------------------
2 VTC running
```

Step 5 Start virt-manager. Run:

```
virt-manager
```

Step 6 After the virt-manager window opens, click the VTC VM to open up the VTC VM console.

The console displays an installation wizard that takes you through the initial VTC VM configuration.

Step 7 Enter the following:

Note For items that take multiple values, such as DNS and NTP, each value must be separated by a space.

- VTS Hostname
- DHCP / Static IP configuration for static IP
- Management IP address for VTC—This is the Cisco NFVI api (a) network IP address.
- Management IP Netmask (api network)
- Management Gateway address (api network)
- DNS Address—One of the DNS servers in setup_data.yaml::NETWORKING['domain_name_servers'
- DNS Search domain—-- setup_data.yaml::NETWORKING['domain_name']
- Underlay IP address—This is the IP address for Cisco NFVI management/provisioning (mx) network.
- Underlay IP Netmask (mx network)
- NTP address—One of the setup_data.yaml::NETWORKING['ntp_servers'] addresses

- Password change for user vts-admin—Enter the default user vts-admin password. The vts-admin user is used for password recovery and to revisit a configuration screen if you make a mistake or need to change the information. If you log in to the VTC VM using vts-admin username and password again, you will get the same dialog to go through the VTC VM setup again. The password must match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']

  Before entering the VTS_PASSWORD, reviewing Cisco VTS Usernames and Passwords in Cisco NFVI, on page 4 is recommended.

- Administrator User—Enter administrative username and password. This username and password are used to login to the VM via SSH.

- Password for administrator user

VTC VM reboots at this time. Wait for two minutes for the VTC VM to be up. You can ping the IP address given for VTC VM in the setup process to verify whether the VTC VM is up.

Step 8 SSH into VTC VM using the IP address, administrative username/password given in the setup process (not vts-admin user).

Installing VTC VM - Manual Configuration using VNC

If the server where you will install VTC is in a remote location with network latency or low bandwidth, you can use VNC to access the VTC VM and manually configure it using the CTC VM graphic console. To do this:

Step 1 Connect to the controller node via SSH, and copy the vtc.qcow2 file to /var/lib/libvirt/images/ folder.

Step 2 Copy the vtc.sample.xml file to your controller. Modify it as per your setup. The sample VTC XML file output is provided in Sample Cisco VTS Configurations for Cisco NFVI, on page 23.

Step 3 Replace the following sections of the vtc.sample.xml file:

```
 <graphics type='spice' port='5900' autoport='yes' listen='127.0.0.1'>
      <listen type='address' address='127.0.0.1'/>
    </graphics>
```

with the following:

```
<graphics type='vnc' port='5900' autoport='yes' listen='0.0.0.0'>
      <listen type='address' address='0.0.0.0'/>
    </graphics>
```

Note Setting the listen address to 0.0.0.0 allows external clients to connect to the VNC port (5900). You will also need to make sure that iptables configuration (if any) allows inbound TCP port 5900 connections.

Step 4 Create the VTC VM using following command:

```
virsh create vtc.sample.xml
```

You should now be able to use a VNC client to connect to the VTC VM graphic console and continue the setup.

Step 5 Enter the following:

Note For items that take multiple values, such as DNS and NTP, use a space to separate each value.

- VTS Hostname
- DHCP/Static IP configuration for static IP
- Management IP address for VTC—This is the Cisco NFVI api (a) network IP address.
- Management IP Netmask (api network)
- Management Gateway address (api network)
- DNS Address—One of the DNS servers in setup_data.yaml::NETWORKING['domain_name_servers'
- DNS Search domain—-- setup_data.yaml::NETWORKING['domain_name']
- Underlay IP address—This is the IP address for Cisco NFVI management/provisioning (mx) network.
- Underlay IP Netmask (mx network)
- NTP address—One of the setup_data.yaml::NETWORKING['ntp_servers'] addresses
- Password change for user vts-admin—Enter the default user vts-admin password. The vts-admin user is used for password recovery and to revisit a configuration screen if you make a mistake or need to change the information. If you log into the VTC VM using vts-admin username and password again, you will get the same dialog to go through the VTC VM setup again. This should match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD'] or subsequently changed through the VTC UI to match the value in setup_data.yaml::VTS_PARAMETERS['VTS_PASSWORD']
- Administrator User—Enter administrative username and password. This username and password are used to login to the VM via SSH.
- Password for administrator user.

VTC VM reboots at this time. Wait for two minutes for the VTC VM to come up. You can ping the IP address given for VTC VM in the setup process to verify whether the VTC VM is up.

Step 6 SSH into VTC VM using the IP address, administrative username/password given in the setup process (not vts-admin user).

Installing the XRNC and XRv VMs

Before you can install Cisco VTS for Cisco NFVI, you must install the IOS XRv VM and register it to VTS. IOS XRv VM is the control plane VM. Installing and registering the IOS XRv VM requires you to complete the following procedures:

- Creating an IOS XRv VM , on page 12
- Creating an ISO for IOS XRv, on page 14

Creating an IOS XRv VM

The IOS XRv VM is essential to the Virtual VTEP topology. The IOS XRv VM contains a nested VM so IOS XRv must enable nesting.

Before you begin

You must complete a VTS VM installation, and the VTC UI initial password must be changed to the password that you will enter for Cisco VIM when you install Cisco VIM. This password is set in setup_data.yaml or the Cisco VIM Insight.

Setting up Nested VM in RedHat

This has been verified with RedHat 7.1 OSP.

Step 1 Run **cat /sys/module/kvm_intel/parameters/nested**.

Step 2 If the output is N, shut down all active VMs, then enable the nested KVM feature:

```
echo "options kvm-intel nested=1" | sudo tee /etc/modprobe.d/kvm-intel.conf
    rmmod kvm_intel
    modprobe kvm_intel
```

Step 3 Run **cat /sys/module/kvm_intel/parameters/nested** and verify that it gives Y.

Bringing up the KVM-based IOS XRv VM

Step 1 Create the IOS XRv VM XML referring the Cisco NFVI sample (XRNC.XML).

Step 2 Generate an ISO file for the IOS XRv. See Creating an ISO for IOS XRv, on page 14.

Step 3 Create the VM using the XML.

```
virsh create XRNC.xml
```

Deploying the vCenter-based IOS XRv VM

Step 1 Generate an ISO file for the IOS XRv VM. See Creating an ISO for IOS XRv, on page 14.

Step 2 In the vSphere Client, select **File** > **Deploy OVF Template**. The Deploy OVF Template wizard appears.

Step 3 Select XRNC.ova from the source location, and click **Next**. The OVF template details are displayed.

Step 4 Click **Next** to specify the destination. Enter the following details:

- Name for the VM.
- Folder or datacenter where the VM will reside.

Step 5 Click **Next** to select the storage location to store the template files. You do not need to change the default values for virtual disk format and VM Storage Policy.

Step 6 Click **Next** to set up the networks. Specify the first network as the Underlay (Cisco NFVI t-net) Network and the second network as the Management (Cisco NFVI mx-net) Network.

Step 7 Click **Next**. Review the settings selections.

Step 8 Click **Finish** to start the deployment.

Step 9 After the deployment is complete, edit the VM settings. Add a CD/DVD Drive selecting Datastore ISO file and point to the XRNC.iso file that was generated and uploaded to the host.

Step 10 Power on the VM.

Running the Setup Script

Run the setup script on the IOS XRv to complete the configuration:

Before you begin

Ensure the tenant network (t) gateway and management network (mx) gateway are reachable from the XRNC server.

SSH into your IOS XRv.

- If you do not want to run in High Availability mode, run the setup script as in the below example:

```
cisco@XRVR-DL1:~$ sudo /opt/cisco/package/sr/bin/setupXRNC_HA.sh 0.0.0.0
```

- If you do want to run in HA mode, see the Installing VTS in an HA Configuration, on page 19 procedure.

Creating an ISO for IOS XRv

To create an ISO file for IOS XRv:

Step 1 Create the system.cfg file based on the sample below.

Note Verify that the configuration files has no spaces or extra characters.

Note Before you enter the VTS_USERNAME and VTS_PASSWORD, review Cisco VTS Usernames and Passwords in Cisco NFVI, on page 4.

```
# This is a sample day0 configuration file
# Copyright (c) 2015 cisco Systems

# VTS Information
VTS_ADDRESS=" <VTC's mx-net VIP address in a.b.c.d form>"
VTS_REGISTRATION_USERNAME=" < must match VTS_PARAMETERS.VTS_USERNAME >"
VTS_REGISTRATION_PASSWORD=" <must match VTS_PARAMETERS.VTS_PASSWORD >!"

# VTC/VTF Network Configuration
HOSTNAME="DL-XRVR6"
NTP_SERVER=" <NTP server--ie. setup_data.yaml::NETWORKING['ntp_servers'][0]>"
NETWORK_CONFIG_METHOD="static"
NETWORK_NAMESERVER_IP=" <DNS server--ie. setup_data.yaml::NETWORKING['domain_name_servers'][0]>"
UNDERLAY_NETWORK_CONFIG_METHOD="static"
UNDERLAY_NETWORK_IP_ADDRESS=" <VM's t-net IP address in a.b.c.d form>"
UNDERLAY_NETWORK_IP_NETMASK=" <t-net IP mask in a.b.c.d form>"
#NETWORK_IP_NETMASK=24
UNDERLAY_NETWORK_IP_GATEWAY=" t-net gateway IP address in a.b.c.d form>"

MGMT_NETWORK_CONFIG_METHOD="static"
```

```
MGMT_NETWORK_IP_ADDRESS=" <VM's mx-net IP address in a.b.c.d form>"
MGMT_NETWORK_IP_NETMASK=" <mx-net IP mask in a.b.c.d form>"
MGMT_NETWORK_IP_GATEWAY=" <mx-net gateway IP address in a.b.c.d form>"

ALL_VTFS_MODE="vhost"

# VTC/VTF Admin user/password hash
# Generate with openssl passwd -1 -salt <salt> <password>
# cisco/cisco123 PASSWORD_HASH='$1$xxx$J3aa90XAPYg6HSNUUUD2o1'
USERNAME='cisco'
PASSWORD_HASH='$1$xxx$J3aa90XAPYg6HSNUUUD2o1'


# XRVR Specific Settings (VTC only)
XRVR_USERNAME="admin"
XRVR_PASSWORD="cisco123"
XRVR_STATIC_MGMT_IP=" <XRVR's mx-net VIP address in a.b.c.d/prefixlen form>"
XRVR_STATIC_UNDERLAY_IP=" <XRVR's t-net VIP address in a.b.c.d/prefixlen form>"
XRVR_NAME=" <XRVR VM instance's hostname>"
XRVR_BGP_COMMUNITY=" <VNI range for VTS to use>"
```

Note The IOS XRv login/password is hard coded to admin/cisco123.

Step 2 Copy your IOS XRv system.cfg files to the same path where the script resides. For example:

```
admin:/opt/cisco/package/vts/bin$ ls -l
total 1432
-rwxr-xr-x 1 vts-admin vts-admin   4767 Sep 29 16:40 build_vts_config_iso.sh
-rw-r--r-- 1 root      root        1242 Sep 29 23:54 system.cfg
```

Step 3 Create the ISO file as shown below (you need to log in as root):

```
root:/opt/cisco/package/vts/bin# ./build_vts_config_iso.sh xrnc system.cfg
Validating input.
Generating ISO File.
Done!
```

Step 4 Spawn the IOS XRv VM with the ISO connected to it.

Step 5 Power on the VM.

In case you spawn a new IOS XRv VM later, it will come up with IOS XRv Day Zero configuration and get reregistered with the VTC. Use the **sync-to** option available in the Config Sync feature to synchronize the configuration with the latest VTC configuration. See the *Synchronizing Configuration* section in the *Cisco VTS User Guide* for more information on this feature.

Verifying Cisco VTS Installation in Cisco NFVI

The following procedures provide information about how to verify the Cisco VTS installation in Cisco NFVI.

Verifying VTC VM Installation

To verify VTC VM installation:

Step 1 Log into the VTC VM just created using the VTC VM console.

- If you installed the VTC VM in a VMware environment, use the VM console.
- If you installed the VTC VM in an RedHat KVM based-OpenStack environment, - telnet 0 <*console-port*> (The console port is the Telnet port in the VTC.xml file.)

Step 2 Ping the Cisco NFVI api network gateway.

If ping fails, verify the VM networking to the Cisco NFVI api network.

Step 3 For the VTC VM CLI, ping the Cisco NFVI management/provisioning (mx) network gateway.

If ping fails, verify VM networking to the mx network.

Note Underlay network gateway is the switched virtual interface (SVI) created for IOSXRv and VTF on the leaf where the controller is connected.

Step 4 After a few minutes, verify whether the VTS UI is reachable by typing in the VTS api network IP in the browser.

Verifying IOS XRv VM Installation

To verify ISO XRv VM installation:

Before you begin

Ensure the tenant network (t) gateway and management network (mx) gateway are reachable from the XRNC server.

Step 1 Log into the IOS XRv VM using the VTC VM console.

- If you installed the VTC VM in a VMware environment, use the VM console.
- If you installed the VTC VM in an RedHat KVM based-OpenStack environment, use virt-manager or VNC console to log into the VM. See Installing VTC VM - Manual Configuration using VNC, on page 11

Step 2 Ping the Cisco NFVI tenant (t) network gateway IP address.

In case ping fails, verify Cisco NFVI tenant network.

Step 3 Ping the VTC Cisco NFVI management/provisioning (mx) network IP address.

In case ping fails, verify the mx network.

Note You should be able to ping the gateway IP address for both Cisco NFVI mx and t networks, as XRv registers to the VTC using the VTC mx network IP address.

Step 4 Run **virsh list** to make sure the nested VM is running.

Step 5 Verify whether the nested IOS XRv is booting up. To do this, run:

```
telnet 0 5087
```

If the o/p command fails, verify whether nested virtualization on the host where IOSXRv is booted is turned on.

Also, verify that another Telnet session is not using this session.

Step 6 Verify whether the Virtual Forwarding Group (VFG) group is created on the VTS GUI and IOSXRv is part of the VFG group.

Step 7 On the XRv shell, run the setup command:

```
sudo /opt/cisco/package/sr/bin/setupXRNC_HA.sh 0.0.0.0
```

For HA installations, replace 0.0.0.0 with the underlay IP address of the second IOSXRv.

Troubleshooting VTF Registration

If VTF registration issues arise, you can use the following commands to find the VTF registration logs on each Cisco NFVI compute node:

```
[root@devstack-71 neutron]# docker exec -it neutron_vtf_4269 bash
[root@devstack-71 /]# cd /var/log/vpfa
[root@devstack-71 vpfa]# ls
vpfa_err.log   vpfa_med.log  vpfa_server.log        vpfa_server_frequent.log  vpfa_stdout.log

vpfa_freq.log  vpfa_reg.log  vpfa_server_errors.log  vpfa_server_slow.log
[root@devstack-71 vpfa]# tail vpfa_reg.log
2016-06-23 02:47:22,860:INFO:VTF-REG: Sent PATCH {"vtf": {"username": "admin",
"vpp-client-name": "devstack-71", "ip": "34.34.34.5", "binding-host-name": "devstack-71",
"gateway-ip": "34.34.34.1", "local-mac": "00:3a:7d:6a:13:c9"}} to
https://172.18.96.15:8888/api/running/cisco-vts/vtfs/vtf
2016-06-23 02:47:23,050:INFO:VTF-REG-ERR: Failure:400!!!
```

A successful log example is shown below:

```
[root@devstack-71 vpfa]# tail vpfa_reg.log
2016-06-23 15:27:57,338:INFO:AUTH: Successful Login - User: admin
URI:/yang-api/datastore/interfaces Host:IPv4Address(TCP, '34.34.34.5', 21345) Method:GET
2016-06-23 15:28:07,340:INFO:AUTH: Successful Login - User: admin
URI:/yang-api/datastore/interfaces Host:IPv4Address(TCP, '34.34.34.5', 21345) Method:GET
```

If a VTF registration fails, check the following:

- IP network connectivity between the compute nodes and the VTC and XRNC/XRVR VMs (Cisco NFVI tenant and management/provisioning networks)
- VTS_PARAMETERS—The VTS_USERNAME must be admin.
- The VTC and XRNC/XRVR must be up and the VTS configurations (described in Configuring Cisco VTS and XRVR After Installation, on page 17) must be applied. The XRVR must be registered with VTC.
- Check that the VTS UI shows "vtsgroup3" in Inventory->Authorization Groups.
- Check that the VTC Admin Username is admin and Device Username is what was set for XRVR_USERNAME in the XRNC config ISO.

Configuring Cisco VTS and XRVR After Installation

The following steps cover the Cisco VTS configurations you need to provision after installation.

Step 1 If you changed the Cisco VTS username/password when you configured the VTS HA configuration, continue with Step 3. If not, log into the Cisco VTS GUI using the default username/password admin/admin.

Step 2 Change the Cisco VTS password using the UI Change Password tab.

Note Before you enter the Cisco VTS password, review Cisco VTS Usernames and Passwords in Cisco NFVI, on page 4.

Step 3 Log into the Linux CLI using SSH then use the ncs_cli to set the following parameters:

```
configure
set resource-pools vni-pool vnipool range 4096 65535
set devices device <XRVR-NAME> asr9k-extension:device-info device-use leaf
set devices device <XRVR-NAME> asr9k-extension:device-info bgp-peering-info bgp-asn 23
set devices device <XRVR-NAME> asr9k-extension:device-info bgp-peering-info loopback-if-num 0
```

Step 4 After the VTF registers, add the following configurations:

```
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
devices
    device <XRVR-NAME>
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
policy-parameters
    distribution-mode decentralized-l2
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
policy-parameters
    control-plane-protocol bgp-evpn
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
policy-parameters
    arp-suppression
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
policy-parameters
    packet-replication ingress-replication
set cisco-vts infra-policy admin-domains admin-domain D1 l3-gateway-groups l3-gateway-group L3GW-0
policy-parameters
    distribution-mode decentralized-l3
set cisco-vts infra-policy admin-domains admin-domain D1 l3-gateway-groups l3-gateway-group L3GW-0
policy-parameters
    control-plane-protocol bgp-evpn
set cisco-vts infra-policy admin-domains admin-domain D1 l3-gateway-groups l3-gateway-group L3GW-0
policy-parameters
    arp-suppression
set cisco-vts infra-policy admin-domains admin-domain D1 l3-gateway-groups l3-gateway-group L3GW-0
policy-parameters
    packet-replication ingress-replication
set cisco-vts infra-policy admin-domains admin-domain D1 l2-gateway-groups l2-gateway-group L2GW-0
ad-l3-gw-parent L3GW-0
```

Step 5 Enter the BGP configuration for XRVI:

```
some IGP
outer ospf 100
router-id 18.18.18.18
address-family ipv4 unicast
area 0.0.0.0
  default-cost 10
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
  !
```

```
!
!
interface Loopback0
ipv4 address 8.8.8.8 255.255.255.255
!

router bgp 23
bgp router-id 8.8.8.8
address-family ipv4 unicast
!
address-family l2vpn evpn
  retain route-target all
!
 After you add this BGP info in the XRVR you will need to sync the devices via the ncs_cli

ncs_cli > request devices device <XRVR-NAME> sync-from
```

Installing VTS in an HA Configuration

Complete the following steps to install Cisco VTS in a Layer 2 HA configuration.

Step 1 Create two VTC VMs. (In the following steps, these will be referred to as VTC1 and VTC2.) When you create the VMs, reserve three IP addresses for each Cisco VIM network to which the VTC VM will be connected as described in Overview to Cisco VTS Installation in Cisco NFVI, on page 1.

Step 2 If you changed the initial VTC password in a previous installation step, proceed to Step 4. If not, log into the VTC GUI using the default username/password admin/admin.

Step 3 Change the VTC password using the UI Change Password tab. See Cisco VTS Usernames and Passwords in Cisco NFVI, on page 4 for information about Cisco VTS usernames and passwords.

Step 4 Edit the cluster.conf file on VTC1 and VTC2 located in /opt/cisco/package/vtc/bin/. Both VTCs must have identical information in the cluster.conf file. Parameters you will enter include:

- vip_public—VIP address used for the Cisco VIM API (a) network.
- vip_private—VIP address used for VTS on the Cisco VIM management/provisioning (mx) network. Cisco VIM uses VTFs, so this field must be entered. The vip_private field is the VIP for the VTS master private interface
- private_network_interface—The VIP interface name used for the Cisco NFVI management/provisioning network. It is the VTC1 and VTC2 secondary interface names on the same private network as XRVR. This must be completed.
- master_name—Enter the name of the VTC you want to be the primary one in the HA configuration.
- master_ip—The master VTC IP address used for the Cisco NFVI API network.
- master_network_interface—The master VTC interface name used for the Cisco NFVI API network. The master_network_interface and slave_network_interface are the interface names of VTC1 and VTC2 where the real IP addresses reside. The interface names must be identical.
- slave_name—Enter the name of the VTC you want to be the secondary one in the HA configuration.
- slave_ip—The secondary VTC IP address used for the Cisco NFVI API network.

- slave_network_interface—The secondary VTC interface name used for the Cisco NFVI API network. The master_network_interface and slave_network_interface are the interface names of VTC1 and VTC2 where the real IP addresses reside. The interface names must be identical.
- private_gateway—The Cisco VIM management/provisioning gateway IP address from setup.yaml. This will come from the Cisco VIM setup_data.yaml file after you complete the Cisco VIM installation and the Cisco VIM Configurations for Cisco VTS Installationprocedure.
- external_ip—The external IP address. This will come from the Cisco VIM setup_data.yaml file after you complete the Cisco VIM installation and the Cisco VIM Configurations for Cisco VTS Installation procedure.

```
###Virtual IP of VTC Master on the public interface.
# In case of Cisco VIM this is the VTC VIP on "api" network
vip_public=<VIP on a-net>

vip_private=<VIP on mx-net>
private_network_interface=eth1  # fixed value

master_name=vtc1
master_ip=<IP on a-net>
master_network_interface=eth0   # fixed value

slave_name=vtc2
slave_ip=<IP on a-net>
slave_network_interface=eth0    # fixed value


#Note this should be reachable all the time as this is used for management network VIP monitoring
private_gateway=<mx-net gateway IP from setup_data.yaml>

###In the event that a network failure occurs evenly between the two routers, the cluster needs an
outside ip to determine where the failure lies
###This can be any external ip such as your vmm ip or a dns but it is recommended to be a stable ip
 within your environment
external_ip=<external_lb_vip_address from setup_data.yaml>


#---------------------------------------------------------
# For Cisco VIM the below values should be left blank
#---------------------------------------------------------

###If you have your vtc's in different subnets, xrvr will need to be configured to route traffic and
 the below section needs to be filled in
###If you have your vtc's on the same subnet, the below section can be skipped

###Name of your vrf. Example: VTS_VIP
vrf_name=

###Ip of your first Xrvr. Example: 11.1.1.5
xrvr1_mgmt_ip=

###List of neighbors for xrvr1, separated by comma. Example: 11.1.1.1,11.1.1.2
xrvr1_bgp_neighbors=

###Ip of your second Xrvr. Example: 12.1.1.5
xrvr2_mgmt_ip=

###List of neighbors for xrvr2, separated by comma. Example: 12.1.1.1,12.1.1.2
xrvr2_bgp_neighbors=

###Credentials for Xrvr
xrvr_user=
xrvr_pass=

###Xrvr ASN information
remote_ASN=
local_ASN=

###Xrvr BGP information
bgp_keepalive=
bgp_hold=
```

Step 5 After modifying the cluster.conf files on VTC1 and VTC2 execute the 'modify_host_vtc.sh script located in /opt/cisco/package/vtc/bin'. The script will execute the following:

On VTC1

```
127.0.0.1       localhost
127.0.1.1       vtc1
11.1.1.4        vtc1
11.1.1.14       vtc2
```

On VTC2

```
127.0.0.1       localhost
127.0.1.1       vtc1
11.1.1.4        vtc1
11.1.1.14       vtc2
```

11.1.1.4 is the VTC1 real IP address, and 11.1.1.14 if the VTC2 real IP address. You might see the hostname in the prompt fail to change after running the script. The prompt will change to the hostname that is defined in cluster.conf after you log out or reboot.

Step 6 Execute the cluster installer script, cluster_install.sh, located in /opt/cisco/package/vtc/bin/ on VTC1 and VTC2. Do not run the script until have completed Steps 1-5.

```
admin@vtc1:/opt/cisco/package/vtc/bin$ sudo ./cluster_install.sh
[sudo] password for admin:
Change made to ncs.conf file. Need to restart ncs
ncs stop/waiting
ncs start/running
corosync stop/waiting
corosync start/running, process 5220
HA cluster is installed
```

Step 7 Execute the master_node_install.sh script located in /opt/cisco/package/vtc/bin/, on the VTC that you want to be the master. Run this script only on the master VTC. Do not run it on the slave VTS.

```
admin@vtc1:/opt/cisco/package/vtc/bin$ sudo ./master_node_install.sh
Master node install finished
```

When the master_node_install script finishes, you can use the **ip addr** command to see the public and private VIPs. If you use VTF, with the VIP up, both XRVRs automatically complete their auto-registration.

Step 8 Verify the HA Status:

```
admin@vtc1:/opt/cisco/package/vtc/bin$ sudo crm status
Last updated: Wed May  4 00:00:28 2016
Last change: Wed May  4 00:00:10 2016 via crm_attribute on vtc2
Stack: corosync
Current DC: vtc2 (739533872) - partition with quorum
Version: 1.1.10-42f2063
2 Nodes configured
4 Resources configured
```

```
Online: [ vtc1 vtc2 ]

ClusterIP      (ocf::heartbeat:IPaddr2):       Started vtc1
Master/Slave Set: ms_vtc_ha [vtc_ha]
     Masters: [ vtc1 ]
     Slaves: [ vtc2 ]
ClusterIP2     (ocf::heartbeat:IPaddr2):       Started vtc1

admin@vtc1:/opt/cisco/package/vtc/bin$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

    link/ether 52:54:00:00:bd:0f brd ff:ff:ff:ff:ff:ff
    inet 11.1.1.4/24 brd 11.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
  inet 11.1.1.2/32 brd 11.1.1.2 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:420:10e:2010:5054:ff:fe00:bd0f/64 scope global dynamic
       valid_lft 2591955sec preferred_lft 604755sec
    inet6 fe80::5054:ff:fe00:bd0f/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

    link/ether 52:54:00:4c:11:13 brd ff:ff:ff:ff:ff:ff
    inet 15.15.15.4/24 brd 11.1.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 15.15.15.20/32 brd 11.1.1.20 scope global eth1
```

Completing the XRNC HA Configuration

Complete the following steps to set up the XRNC HA configuration:

Before you begin

Ensure the tenant network (t) gateway and management network (mx) gateway are reachable from the XRNC server.

Step 1 log into each DL and navigate to /opt/cisco/package/sr/bin, using SSH.

Step 2 Edit the DL hostnames as XRDL1 and XRDL2.

Step 3 Run the following commands to set up the XRNC HA:

On the active XRNC:

```
sudo /opt/cisco/package/sr/bin/setupXRNC_HA.sh < IP address of br-underlay XRNC2>
```

On the standby XRNC:

```
sudo /opt/cisco/package/sr/bin/setupXRNC_HA.sh -s < IP address of br-underlay XRNC1>
```

Uninstalling VTC HA

To move VTC back to it's original pre-HA state, run the following script on both the active and standby nodes.

```
sudo /opt/cisco/package/vtc/bin/uninstallHA.sh
```

Sample Cisco VTS Configurations for Cisco NFVI

Sample VTC VM libvert Domain Configuration

```
<domain type='kvm' id='254'>
  <name>VTC</name>
  <uuid>5789b2c3-df39-4154-a1d3-e38cefc856a3</uuid>
  <memory unit='KiB'>8388608</memory>
  <currentMemory unit='KiB'>8388608</currentMemory>
  <vcpu placement='static'>8</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
    <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
    <boot dev='hd'/>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
  <cpu mode='custom' match='exact'>
    <model fallback='allow'>Westmere</model>
    <feature policy='require' name='vmx'/>
  </cpu>
  <clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='none'/>
      <source file='/opt/neutron-vts/vtc/vtc.qcow2'/>
      <backingStore/>
      <target dev='vda' bus='virtio'/>
      <alias name='virtio-disk0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
    </disk>
    <disk type='file' device='cdrom'>
      <driver name='qemu' type='raw'/>
      <source file='/opt/neutron-vts/config.iso'/>
      <backingStore/>
      <target dev='hdc' bus='ide'/>
      <readonly/>
      <alias name='ide0-1-0'/>
      <address type='drive' controller='0' bus='1' target='0' unit='0'/>
    </disk>
    <controller type='usb' index='0'>
      <alias name='usb'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
    </controller>
    <controller type='pci' index='0' model='pci-root'>
      <alias name='pci.0'/>
    </controller>
    <controller type='virtio-serial' index='0'>
      <alias name='virtio-serial0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
    </controller>
    <controller type='ide' index='0'>
      <alias name='ide'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
    </controller>
    <interface type='bridge'>
      <source bridge='br_api'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </interface>
    <interface type='bridge'>
      <source bridge='br_mgmt'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x0b' function='0x0'/>
    </interface>
    <serial type='tcp'>
      <source mode='bind' host='127.0.0.1' service='4799'/>
      <protocol type='telnet'/>
      <target port='0'/>
      <alias name='serial0'/>
    </serial>
    <console type='tcp'>
      <source mode='bind' host='127.0.0.1' service='4799'/>
      <protocol type='telnet'/>
      <target type='serial' port='0'/>
      <alias name='serial0'/>
    </console>
    <channel type='spicevmc'>
      <target type='virtio' name='com.redhat.spice.0' state='disconnected'/>
      <alias name='channel0'/>
      <address type='virtio-serial' controller='0' bus='0' port='1'/>
    </channel>
    <input type='mouse' bus='ps2'/>
    <input type='keyboard' bus='ps2'/>
    <graphics type='vnc' port='5900' autoport='yes' listen='0.0.0.0'>
      <listen type='address' address='0.0.0.0'/>
    </graphics>
    <sound model='ich6'>
      <alias name='sound0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
    </sound>
    <video>
      <model type='qxl' ram='65536' vram='65536' vgamem='16384' heads='1'/>
      <alias name='video0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
    </video>
    <memballoon model='virtio'>
      <alias name='balloon0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
    </memballoon>
  </devices>
</domain>
```

Sample XRNC VM libvirt Domain Configuration

```
<domain type='kvm'>
  <name>XRVR</name>
  <uuid>0b84e257-61bc-4e6e-8721-8528487e4d69</uuid>
  <memory unit='KiB'>32389120</memory>
  <currentMemory unit='KiB'>32388608</currentMemory>
```

```
<vcpu placement='static'>6</vcpu>
<resource>
  <partition>/machine</partition>
</resource>
<os>
  <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
  <boot dev='hd'/>
</os>
<features>
  <acpi/>
  <apic/>
  <pae/>
</features>
<cpu mode='custom' match='exact'>
  <model fallback='allow'>Westmere</model>
  <feature policy='require' name='vmx'/>
</cpu>
<clock offset='utc'/>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
  <emulator>/usr/libexec/qemu-kvm</emulator>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' cache='none'/>
    <source file='/opt/neutron-vts/xrnc/xrnc.qcow2'/>
    <target dev='vda' bus='virtio'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0'/>
  </disk>
  <disk type='file' device='cdrom'>
    <driver name='qemu' type='raw'/>
    <source file='/opt/neutron-vts/xrnc_cfg.iso'/>
    <target dev='hdc' bus='ide'/>
    <readonly/>
    <address type='drive' controller='0' bus='1' target='0' unit='0'/>
  </disk>
  <controller type='usb' index='0'>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
  </controller>
  <controller type='pci' index='0' model='pci-root'/>
  <controller type='virtio-serial' index='0'>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
  </controller>
  <controller type='ide' index='0'>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
  </controller>
  <interface type='bridge'>
    <source bridge='br_mgmt'/>
    <model type='virtio'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x0c' function='0x0'/>
  </interface>
  <interface type='bridge'>
    <source bridge='br_tenant'/>
    <model type='virtio'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
  </interface>
  <serial type='tcp'>
    <source mode='bind' host='127.0.0.1' service='9099'/>
    <protocol type='telnet'/>
    <target port='0'/>
  </serial>
  <console type='tcp'>
    <source mode='bind' host='127.0.0.1' service='9099'/>
    <protocol type='telnet'/>
```

```
      <target type='serial' port='0'/>
    </console>
    <graphics type='vnc' port='5901' autoport='yes' listen='0.0.0.0'>
     <listen type='address' address='0.0.0.0'/>
    </graphics>
    <input type='mouse' bus='ps2'/>
    <input type='keyboard' bus='ps2'/>
    <sound model='ich6'>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
    </sound>
    <video>
      <model type='vga' vram='16384' heads='1'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0'/>
    </video>
    <memballoon model='virtio'>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
    </memballoon>
  </devices>
</domain>
```