CCNP Enterprise Certification

ENSDWI : 300-415

2.0 Controller Deployment

2.1 Describe controller cloud deployment

2.2 Describe Controller on-Prem Deployment

- 2.2.a Hosting platform (KVM/Hypervisor)
- 2.2.b Installing controllers
- 2.2.c Scalability and redundancy

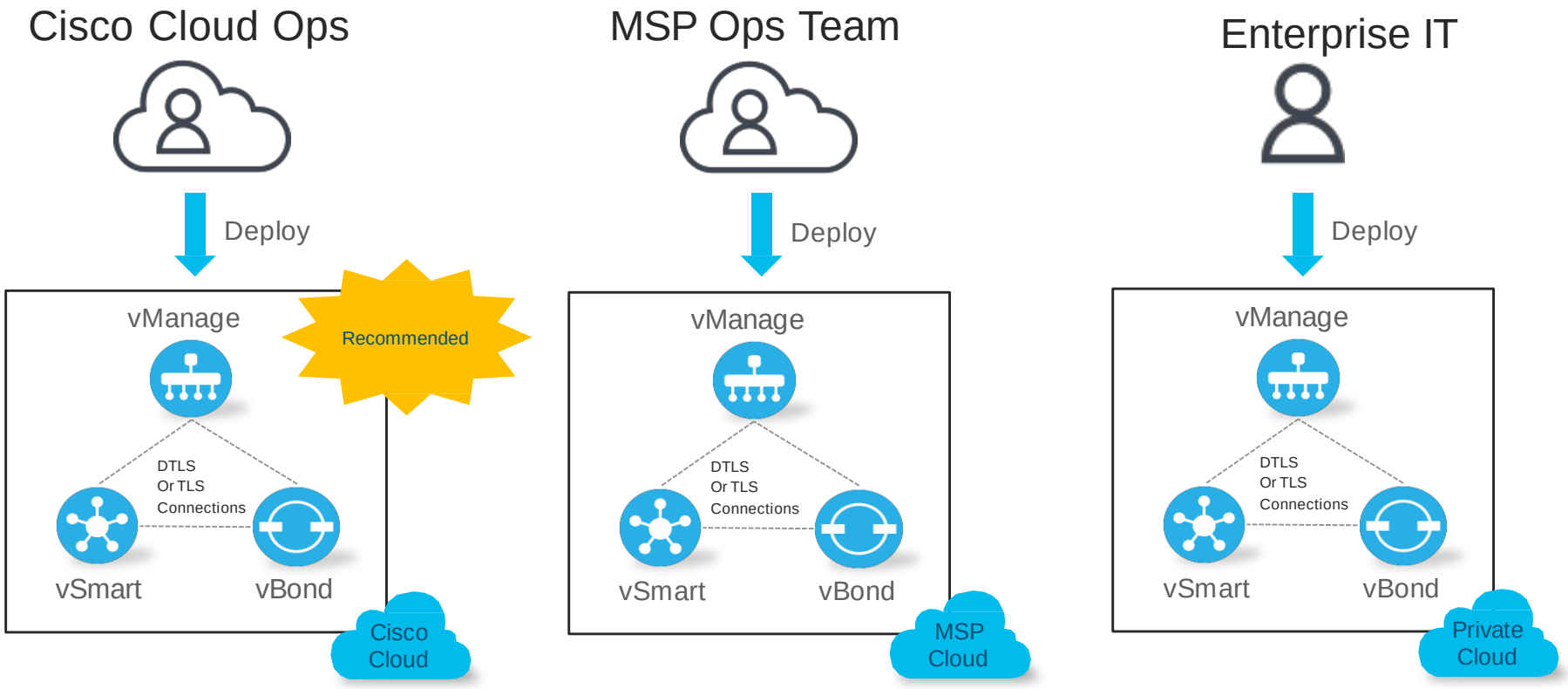
2.3 Configure and verify certificates and whitelisting

2.4 Troubleshoot control-plane connectivity between controllers

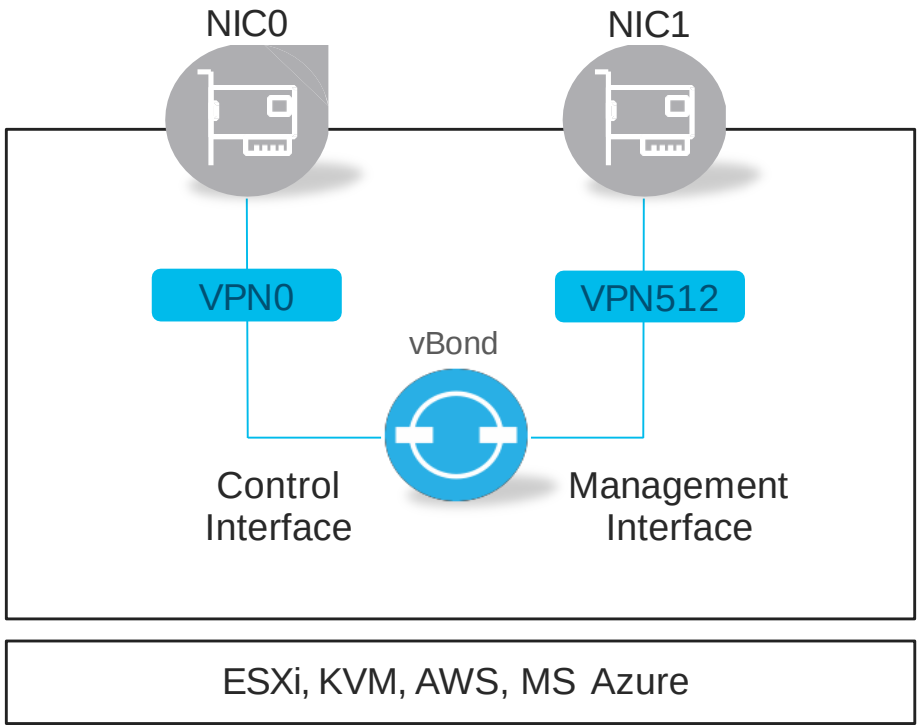
2.1 Describe controller cloud deployment

Cloud-Delivered Control

Flexible Deployment Options

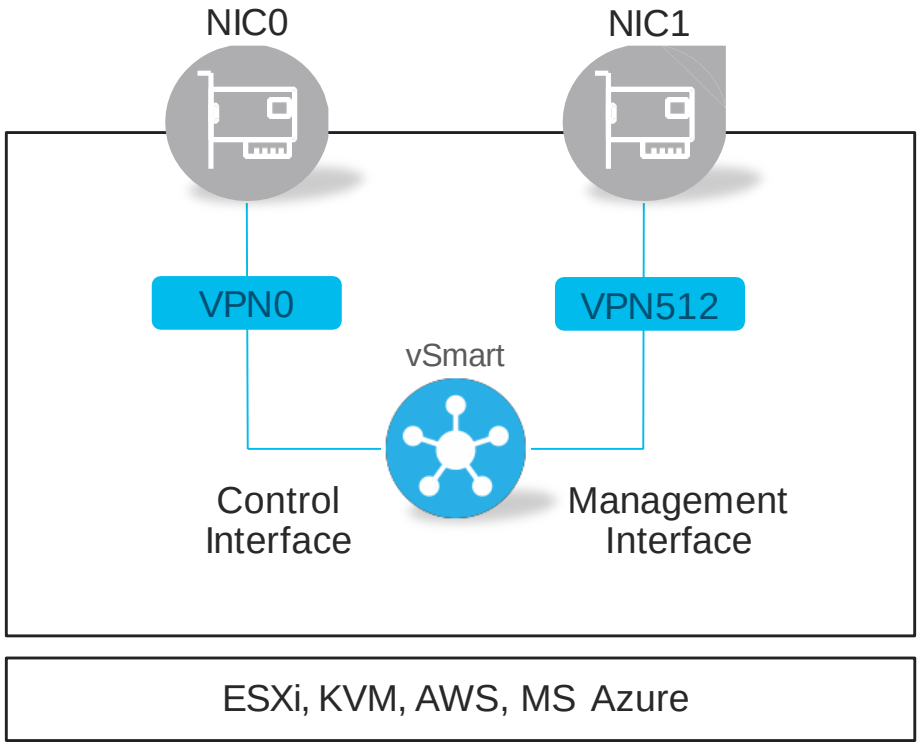


Controller Deployment



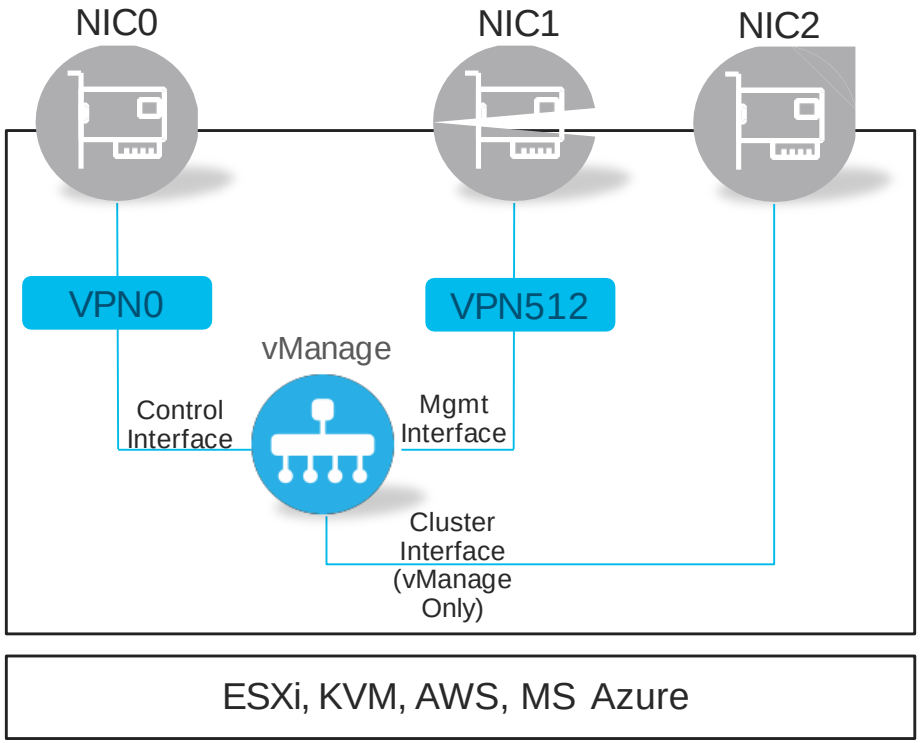
- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)

Controller Deployment



- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and Management Zone-based security
- Minimal configuration for bring-up Connectivity, System IP, Site ID, Org-Name, vBond IP

Typical Controller Deployment



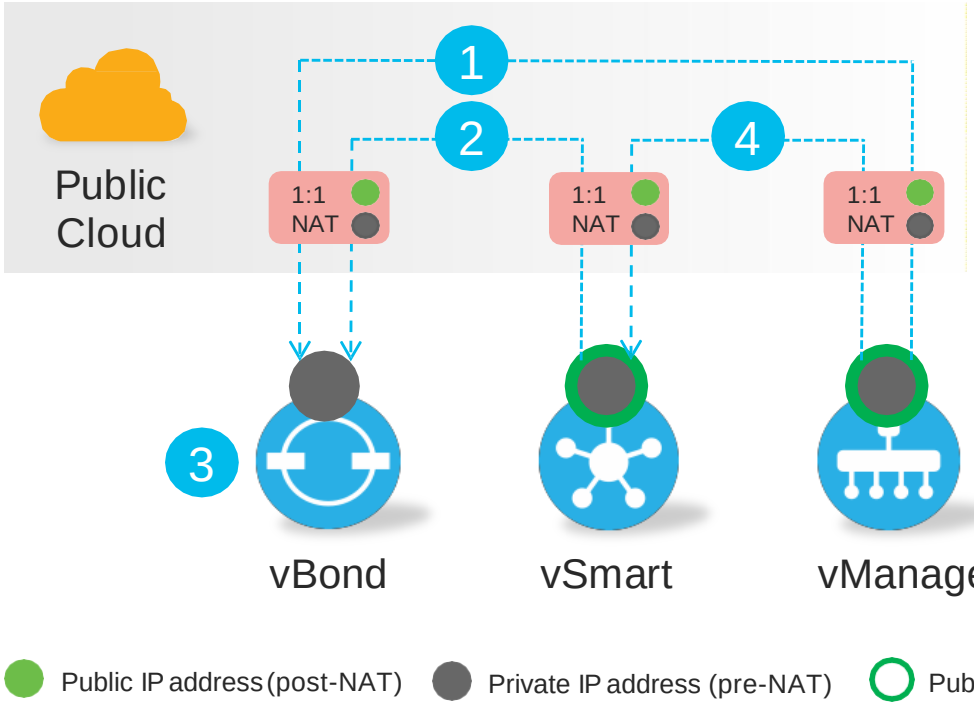
- Cloud or on premise deployment
- Separate interfaces for control and management
- Separate VPNs for control and management
  - Zone-based security
- Internal Cluster I/F for vManage instance clustering
- Minimal configuration for bring-up
  - Connectivity, System IP, Site ID, Org-Name, vBond IP (local)

Controller Communication Principles

- The vBond is a special control element because it acts as a STUN server for the network to allow vEdges to sit behind NAT devices
- To work properly, the other control elements (vManage, vSmart) need to communicate to vBond through NAT as well.
- vSmarts and vManages can communicate with each other either through NAT or un-NATed connections
- NAT must be 1:1 with no PAT
- The choice of deployment model is dependent on security posture vs network complexity tradeoff.

Controllers Public Cloud Deployment

Controllers Communication



1 2 vSmart and vManage point to the vBond IP address

- NATed public IP address

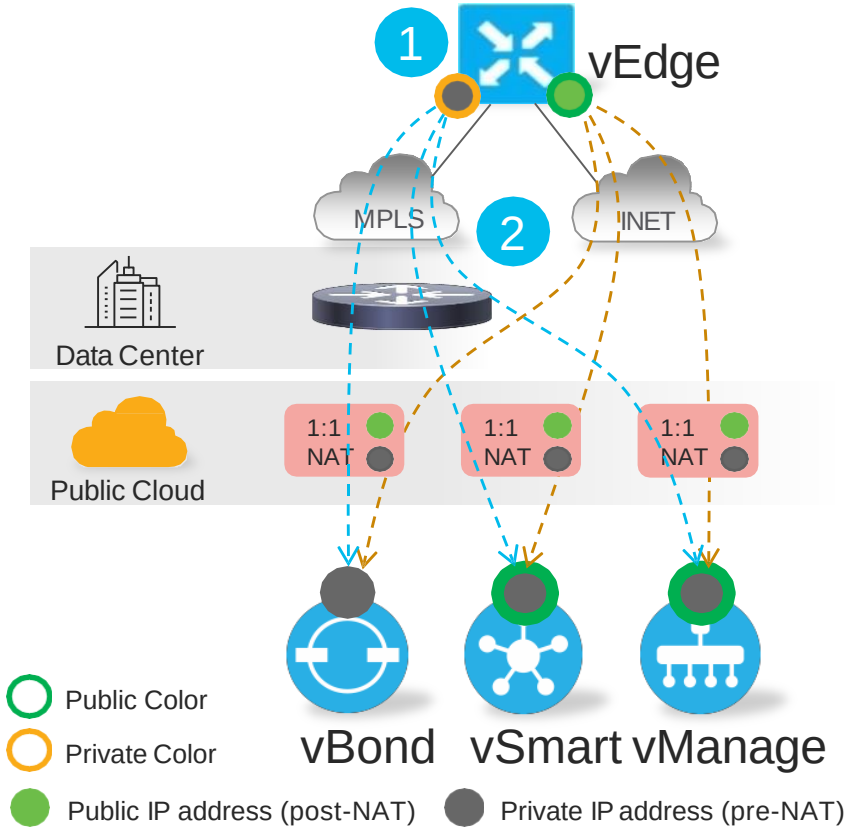
3 vBond learns interface private and NATed public IP address of vSmart and vManage

- Private is pre-NAT, public is post-NAT

4 vSmart and vManage use NATed public IP addresses for communication

- vSmart and vManage use public color (default)
- Public color to public color uses public IP address

Controllers Public Cloud Deployment



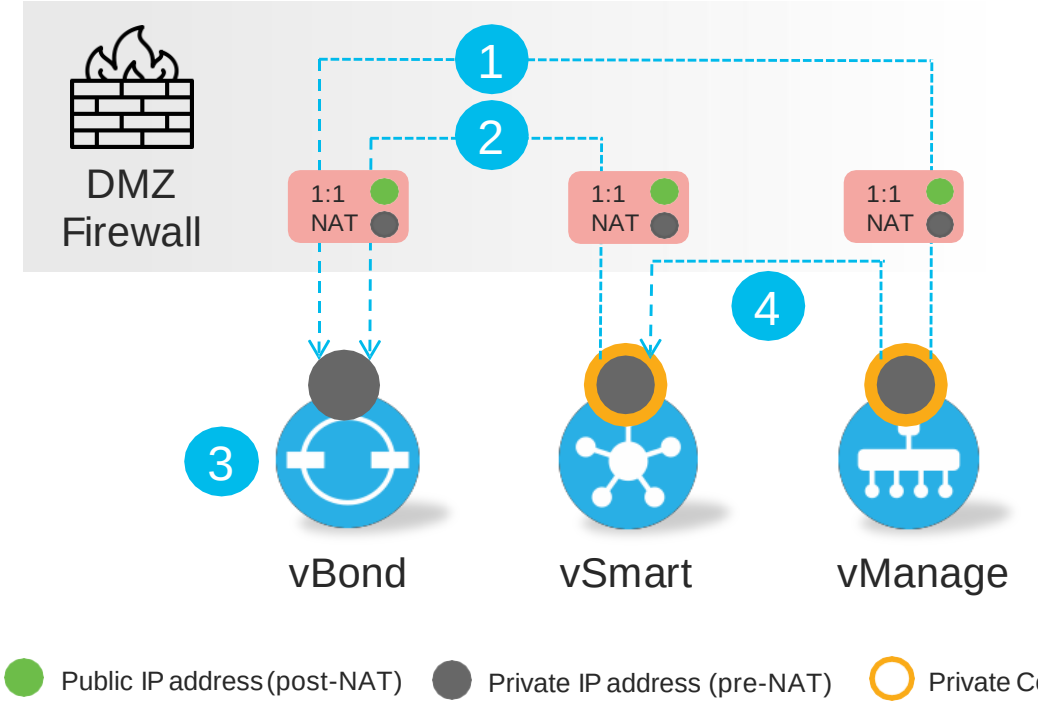
- 1 vEdge points to the vBond NATed public IP
  - vBond NATed public IP address is reachable through MPLS (direct or via Data Center) and Internet transports
- 2 vEdge communicates with vSmart and vManage using NATed public IP address
  - Private color to public color uses public IP address, public color to public color uses public IP address
  - vSmart and vManage NATed public IP addresses are reachable through MPLS (direct or via Data Center) and Internet transports

On-Prem

- 2.2 Describe Controller on-Prem Deployment
- 2.2.a Hosting platform (KVM/Hypervisor)
- 2.2.b Installing controllers
- 2.2.c Scalability and redundancy
- 2.3 Configure and verify certificates and whitelisting

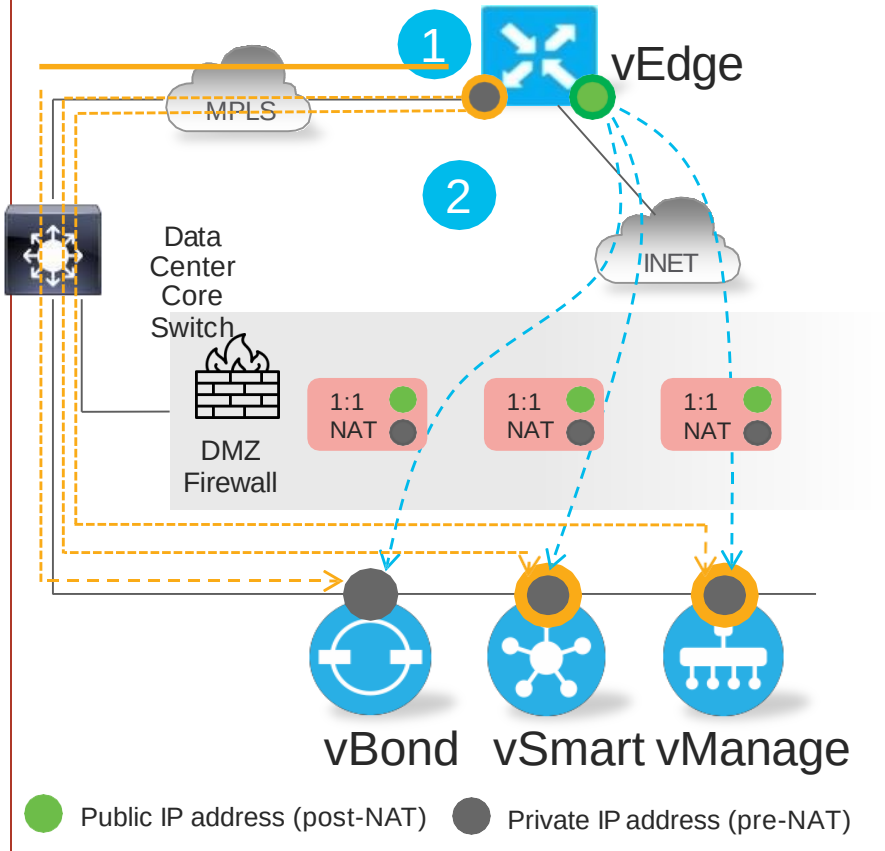
On-Prem Controllers Hybrid Deployment

Controllers Communication



- 1 2 vSmart and vManage point to the vBond IP address
  - NATed public IP address
- 3 vBond learns interface private and NATed public IP address of vSmart and vManage
  - Private is pre-NAT, public is post-NAT
- 4 vSmart and vManage use interface private IP addresses for communication
  - vSmart and vManage use private color (non-default)
  - Private color to private color uses private IP address

On-Prem Controllers Hybrid Deployment



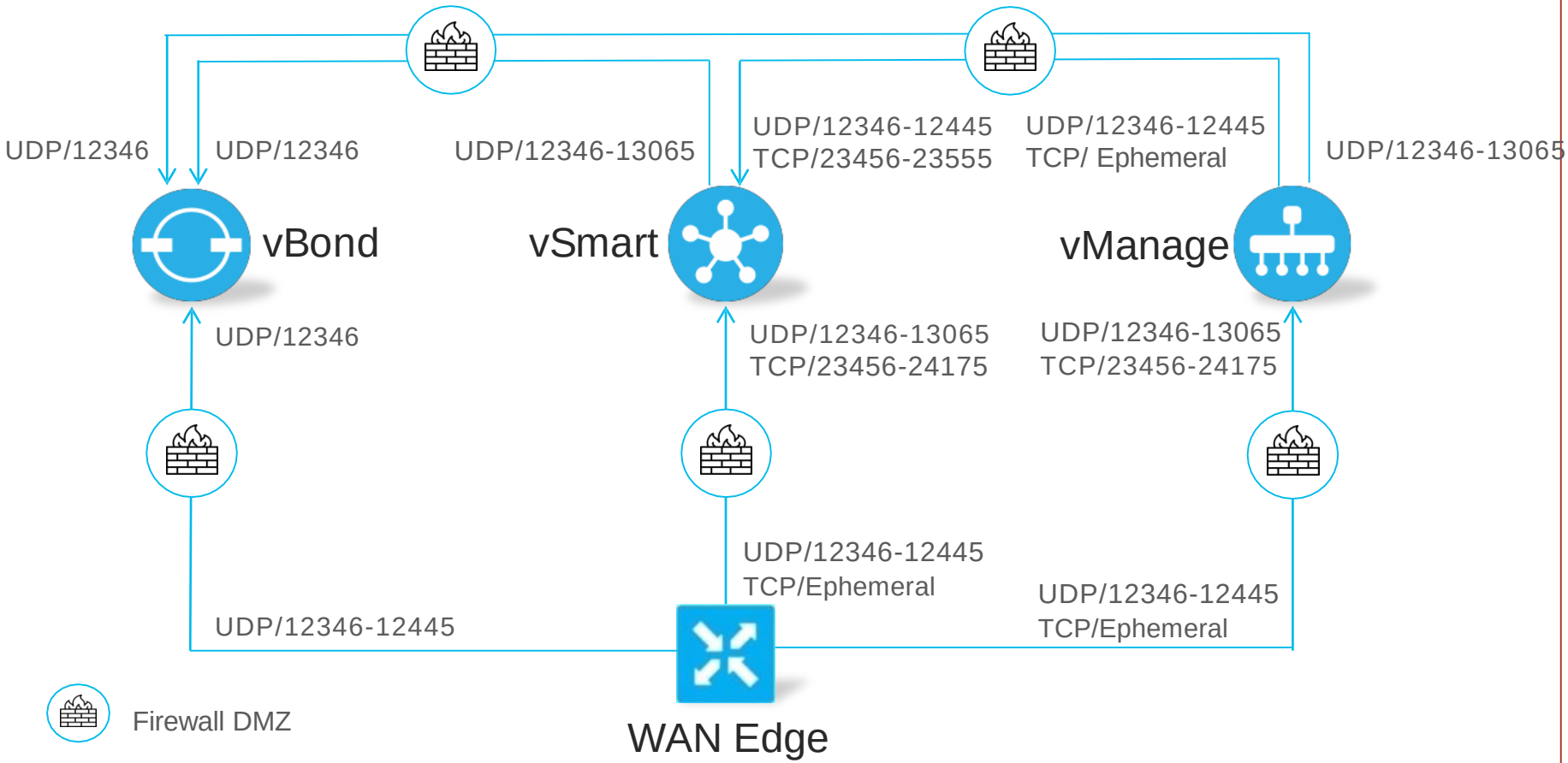
- 1 vEdge points to the vBond FQDN that resolves to both public and private IP addresses

	Private IP	Public IP
MPLS		
Internet		

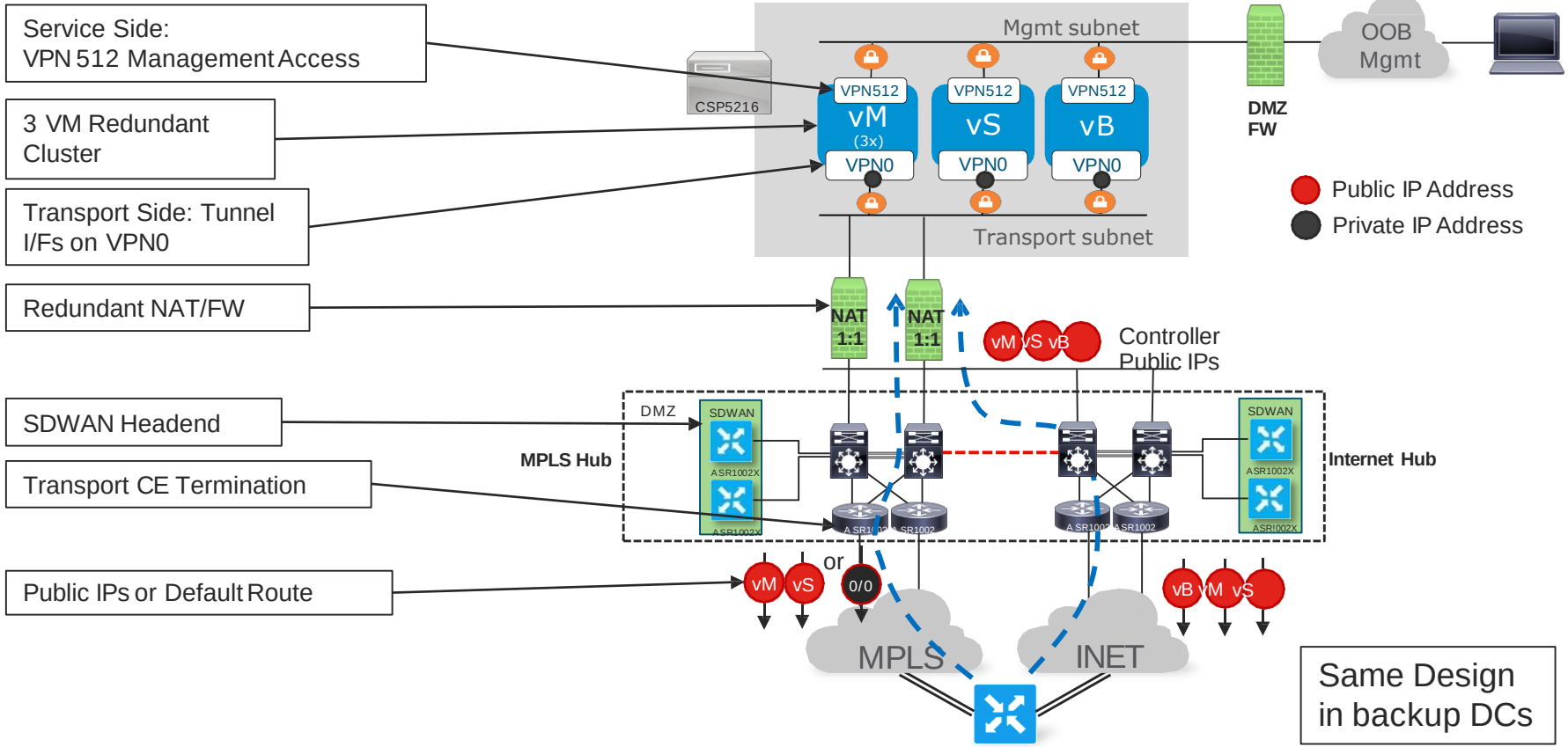
2 vEdge communicates with vSmart and vManage NATed public IP addresses over Internet and interface private IP addresses over MPLS

  - Private color to private color uses private IP address, private color to public color uses public IP address

Firewall Rules for On-Prem Controllers



Example Controller System Deployment



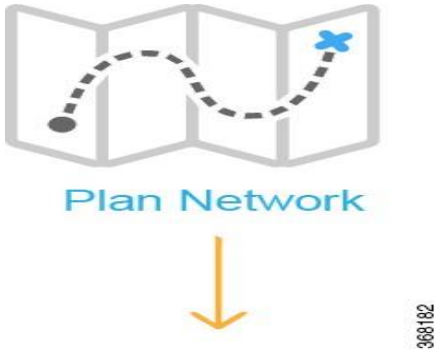
Entire system bringup process includes these steps:

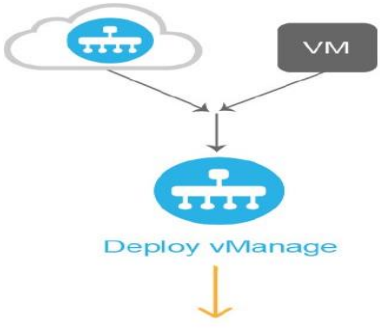
→Control Plan Bring-up steps

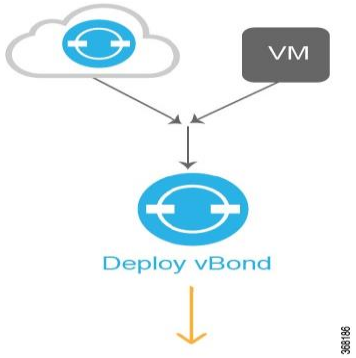
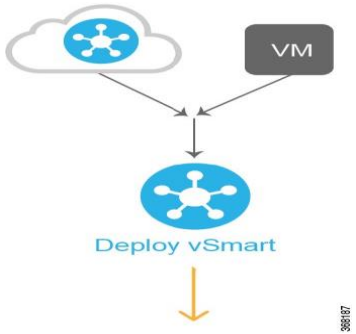
1.Install hypervisor (KVM) on the server .
2.Spin-up virtual machines on the server .
3.Install images for vManage, vBond, vSmart and vEdges on the virtual machines .
4.Create a minimal configuration for vManage (Deploy vManage).
5.Create a minimal configuration for vBond (Deploy vBond).
6.Create a minimal configuration for vSmart (Deploy vSmart).
7.Enable connectivity between Controllers (Enable Inter-Controller Connectivity).
8.Generate CSRs for each Controller (Overlay Connections).
9.Sign certificates to validate and authenticate the Controllers. (Certificate Signature).

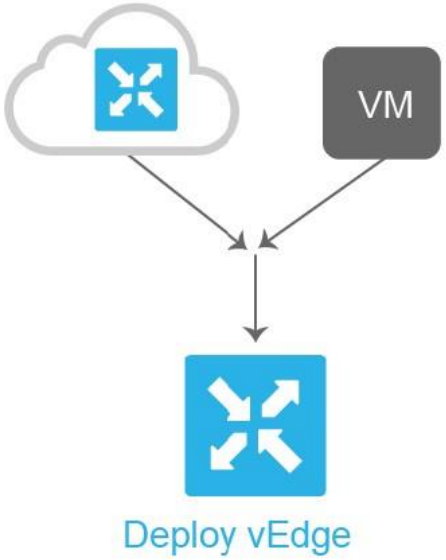
→ vEDGE Bring-up steps

1.Create a minimal configuration for vEdges and establish IP connectivity into the WAN circuits (Deploy vEdge).
2.Verify that vEdge routers are able to reach the Controllers (vEdge Connections).
3.Authenticate each vEdge router (Certify vEdges).
4.Register each vEdge router with vManage (Register vEdge).
5.Verify that the vEdge are up in the vManage dashboard (Verify SD-WAN Connectivity).

	Workflow	Procedure
1		Plan out your overlay network. See Components of the Cisco SD-WAN Solution .

	Workflow	Procedure
2		On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.
3		Download the software images.
4		Deploy the vManage NMS in the data center: 1. Create a vManage VM instance, either on an ESXi or a KVM hypervisor. 2. Create either a minimal or a full configuration for each vManage . 3. Configure certificate settings and generate a certificate for the vManage NMS. 4. Create a vManage cluster .

	Workflow	Procedure
5		Deploy the vBond orchestrator : 1. Create a vBond VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the vBond orchestrator. 3. Add the vBond orchestrator to the overlay network. During this process, you generate a certificate for the vBond orchestrator. 4. Create a full configuration for the vBond orchestrator.
6		Deploy the vSmart controller in the data center: 1. Create a vSmart VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the vSmart controller. 3. Add the vSmart controller to the overlay network. During this process, you generate a certificate for the vSmart controller. 4. Create a full configuration for the vSmart controller.

7		Deploy the vEdge routers in the overlay network: 1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor. 2. For software vEdge Cloud routers, send a certificate signing request to Symantec and then install the signed certificate on the router. 3. From the vManage NMS, send the serial numbers of all vEdge routers to the vSmart controllers and vBond orchestrators in the overlay network. 4. Create a full configuration for the vEdge routers.

2.2.a Hosting platform (KVM/Hypervisor)

Server
Recommendations

vBond Orchestrator Server Recommendations

Devices	**vCPUs**	**RAM**	**OS Volume**	**Bandwidth**	**vNICs**
1-50	2	4 GB	10 GB	1 Mbps	2 (one for tunnel interface, one for management)
51-250	2	4 GB	10 GB	2 Mbps	2 (one for tunnel interface, one for management)
251-1000	2	4 GB	10 GB	5 Mbps	2 (one for tunnel interface, one for management)
1001 or more	4	8 GB	10 GB	10 Mbps	2 (one for tunnel interface, one for management)

vManage NMS Server Recommendations for On-prem Multitenants

vCPUs	RAM	OS Volume	Database Volume	Bandwidth	vNICs
32	64 GB	20 GB	1 TB, 3072 IOPS	150 Mbps	3 network interfaces

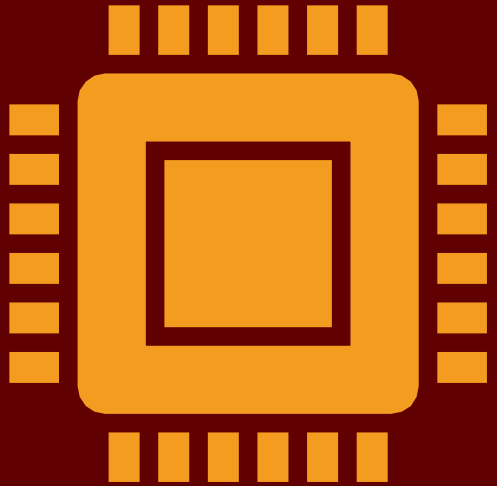
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Create_vManage_VM_Instance_on_ESXi_7835.xml

vManage NMS Server Recommendations

Devices	vCPUs	RAM	OS Volume	Database Volume	Bandwidth	vNICs
1-250	16	32 GB	20 GB	500 GB, 1500 IOPS	25 Mbps	3 (one for tunnel interface, one for management, one for the vManage cluster message bus)
251-1000	32	64 GB	20 GB	1 TB, 3072 IOPS	100 Mbps	3 (one for tunnel interface, one for management, one for the vManage cluster message bus)
1001 or more	32	64 GB	20 GB	1 TB, 3072 IOPS	150 Mbps	3 (one for tunnel interface, one for management, one for the vManage cluster message bus)

vSmart Controller Server Recommendations

Devices	vCPUs	RAM	OS Volume	Bandwidth	vNICs
1-50	2	4 GB	16 GB	2 Mbps	2 (one for tunnel interface, one for management)
51-250	4	8 GB	16 GB	5 Mbps	2 (one for tunnel interface, one for management)
251-1000	4	16 GB	16 GB	7 Mbps	2 (one for tunnel interface, one for management)
1001 or more	8	16 GB	16 GB	10 Mbps	2 (one for tunnel interface, one for management)



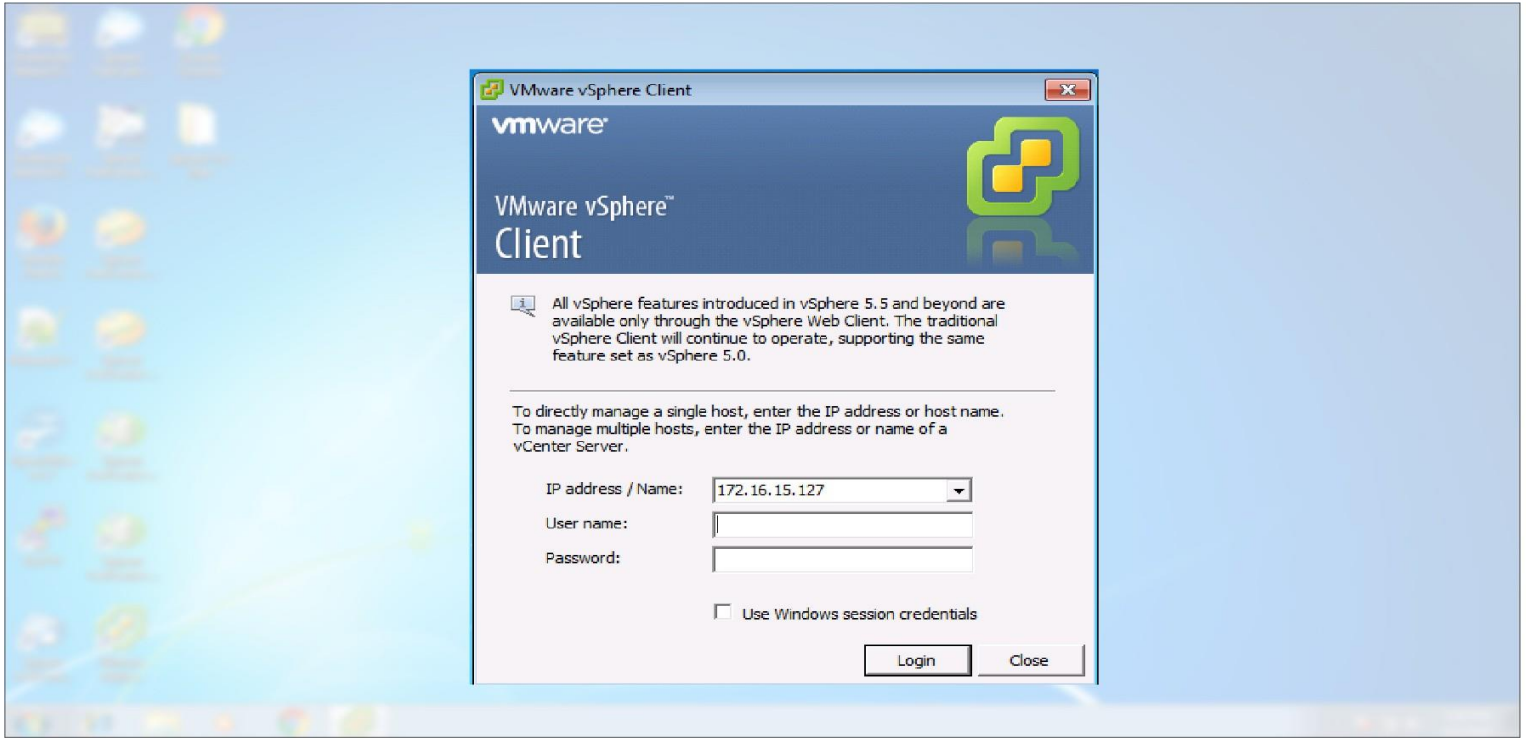
Spun up virtual machines on a server

- **vManage**: vmanage-software-release.ova
- **vBond**: vbond-software-release.ova
- **vSmart**: vsmart-software-release.ova
- **vEdge**: viptela-edge-software-release.ova

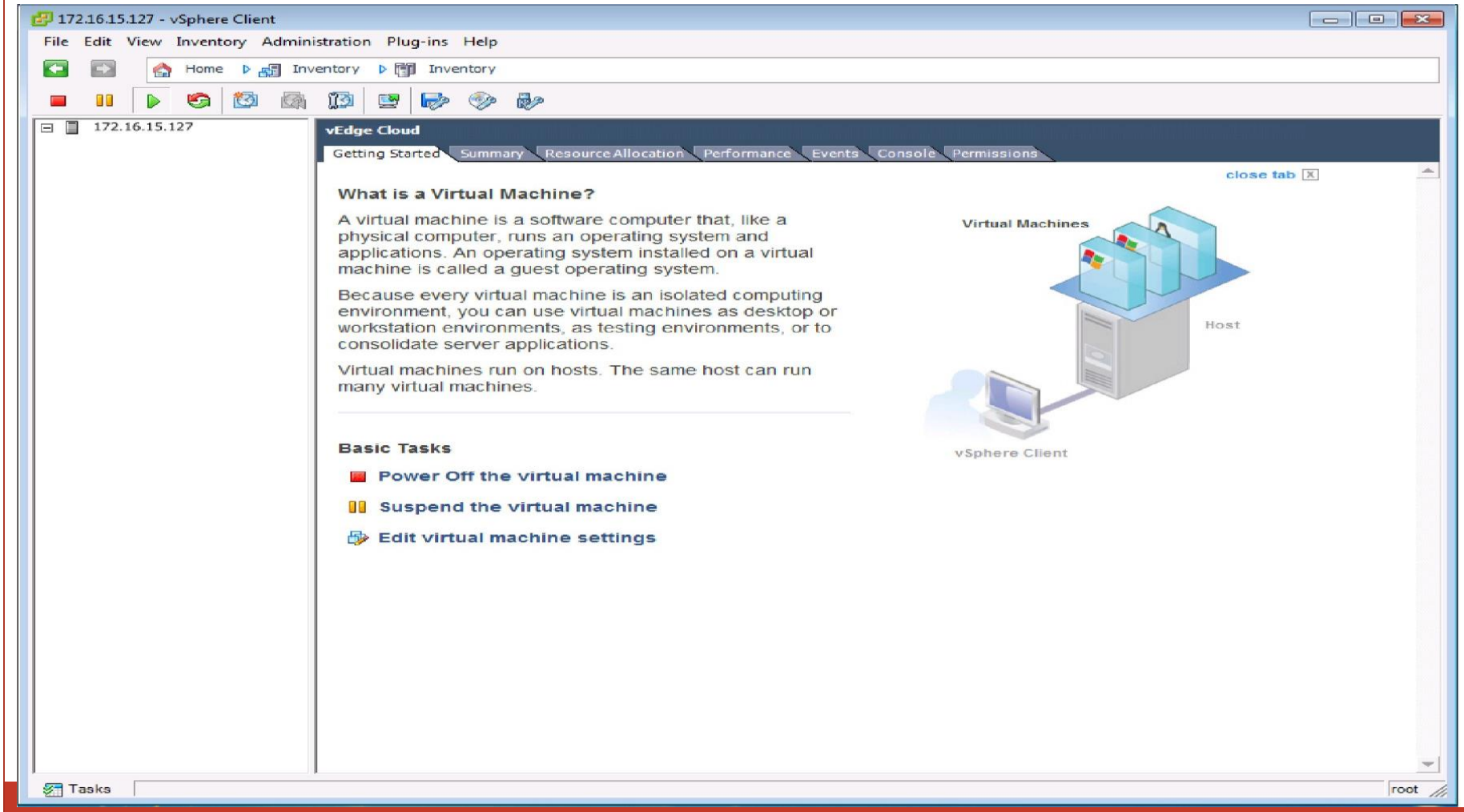
To download the Cisco SD-WAN software:

1. Go to http://viptela.com/support/ and log in.
2. Click Downloads.
3. Select the software release version.
4. Click the desired .ova software image file to download it. (Note that the .tar files are software bundles that you use only when upgrading the software. They are not required for initial software installation.)
5. Copy the software image to the desired HTTP or FTP file server in your local network.

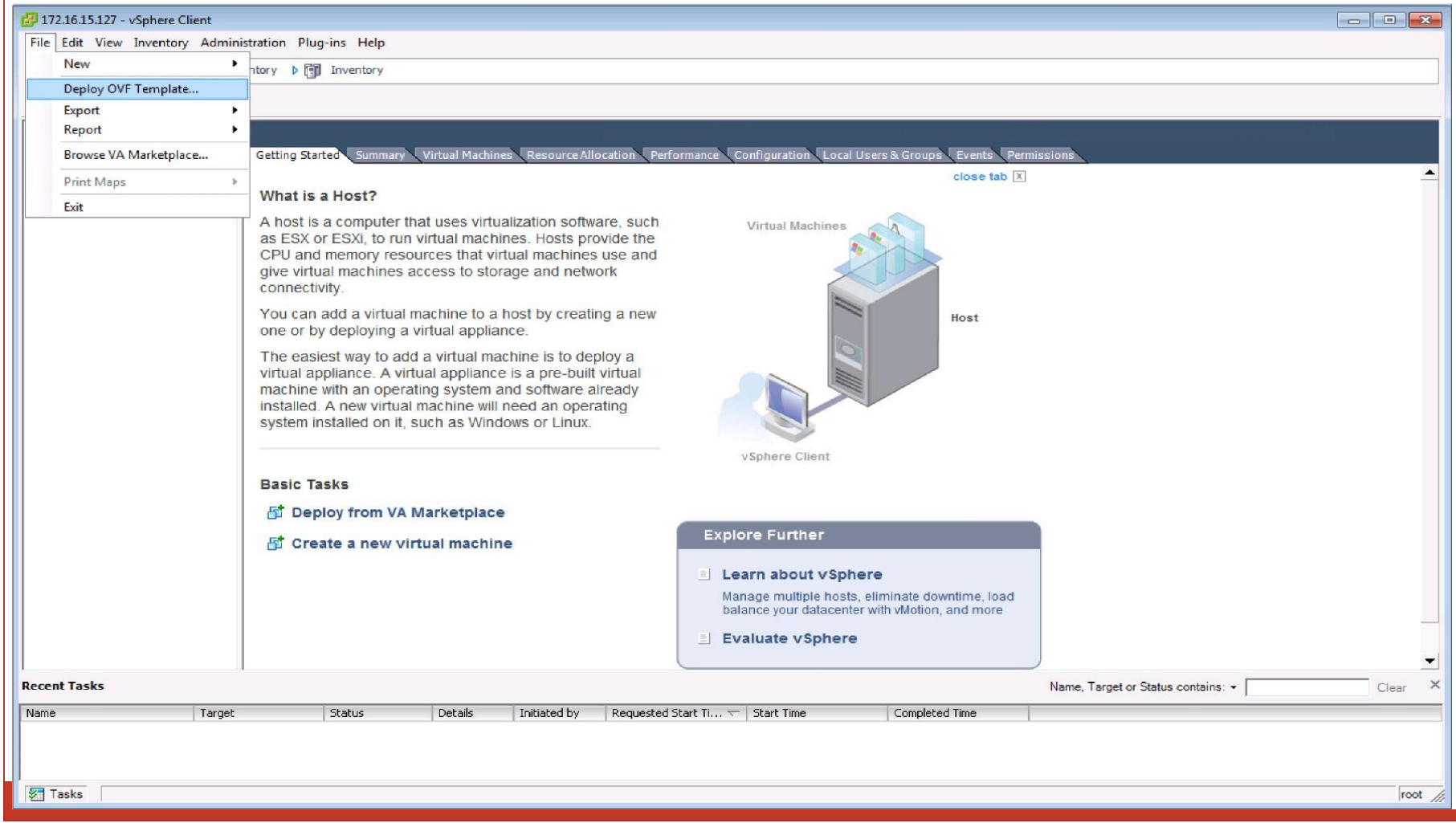
Deploy the vManage NMS



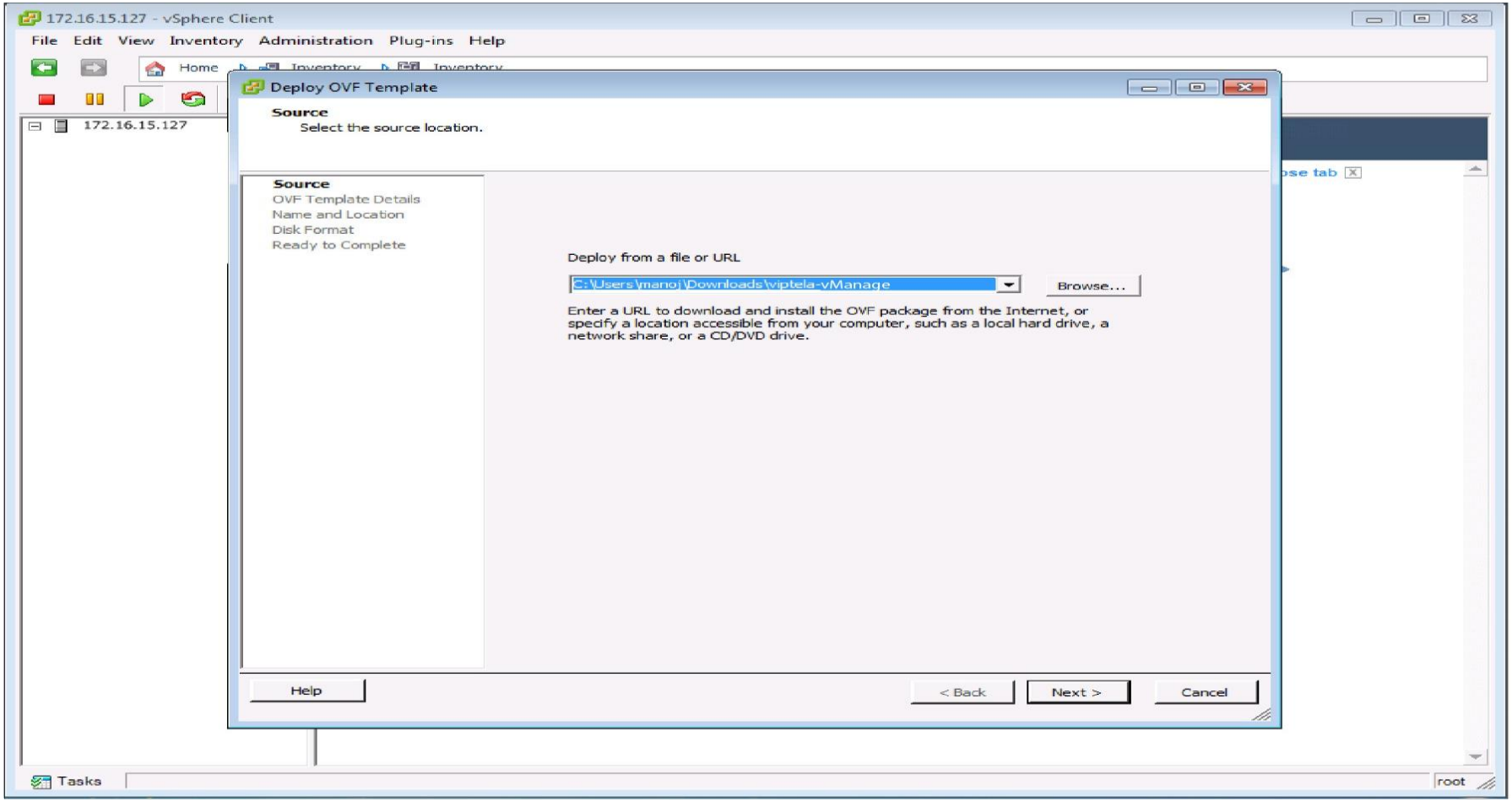
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Create_vManage_VM_Instance_on_ESXi_7835.xml


172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
172.16.15.127
vEdge Cloud
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
What is a Virtual Machine?
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.
Virtual machines run on hosts. The same host can run many virtual machines.
Virtual Machines
Host
vSphere Client
Basic Tasks
Power Off the virtual machine
Suspend the virtual machine
Edit virtual machine settings
Tasks
root

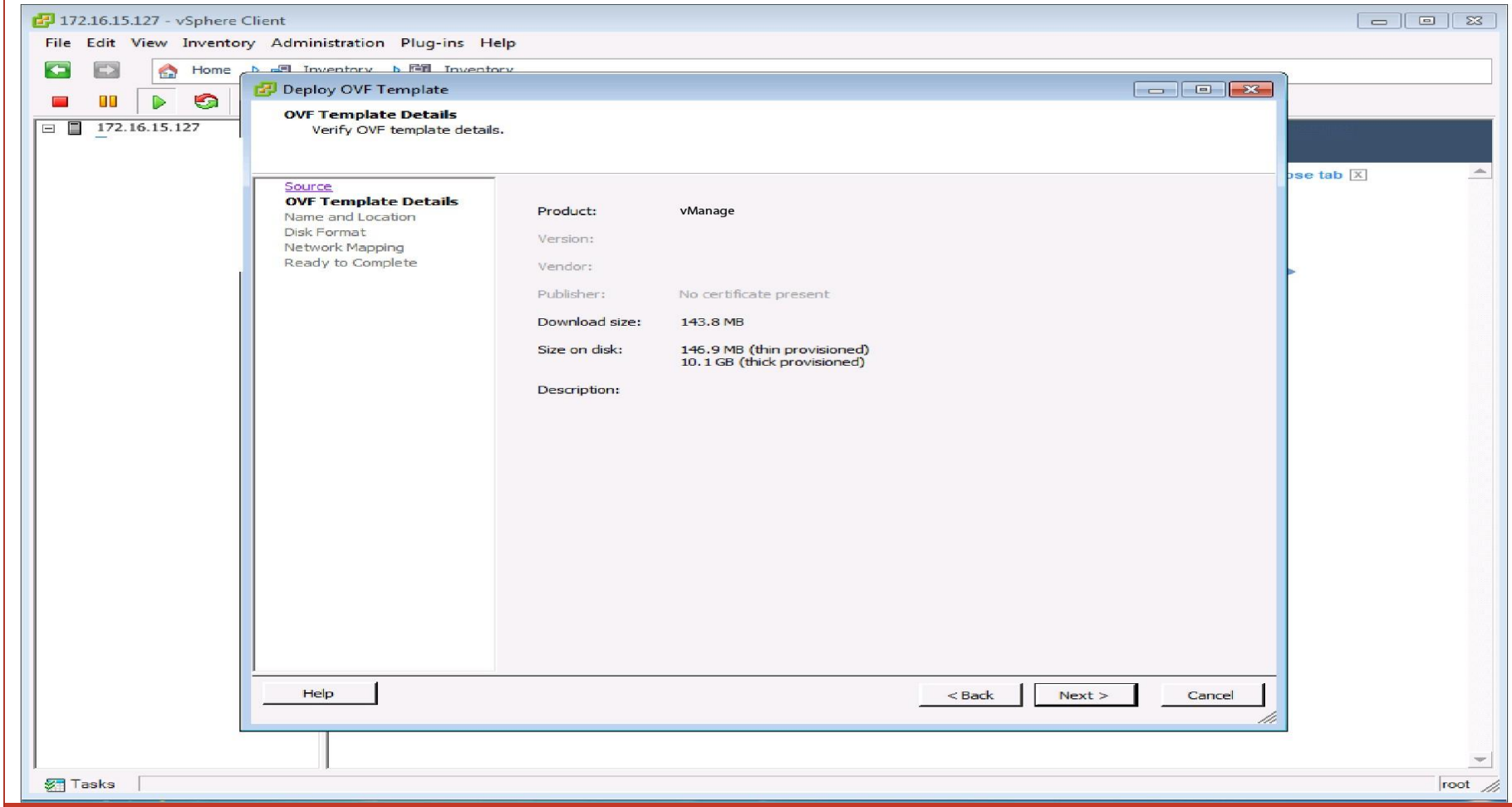
368239

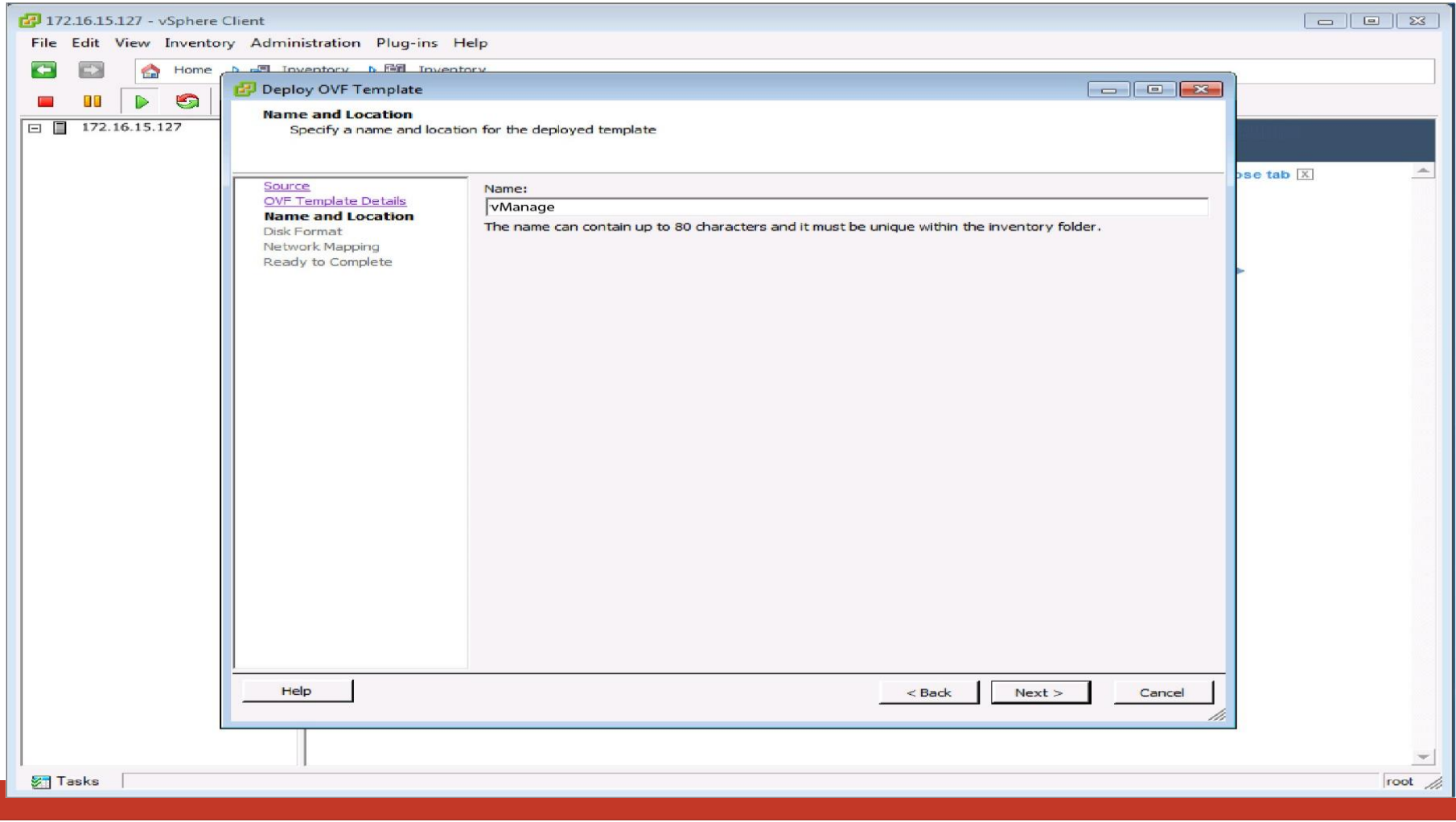

172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
New
Deploy OVF Template...
Export
Report
Browse VA Marketplace...
Print Maps
Exit
Inventory
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
close tab
What is a Host?
A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.
You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.
The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.
Virtual Machines
Host
vSphere Client
Basic Tasks
Deploy from VA Marketplace
Create a new virtual machine
Explore Further
Learn about vSphere
Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more
Evaluate vSphere
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
root

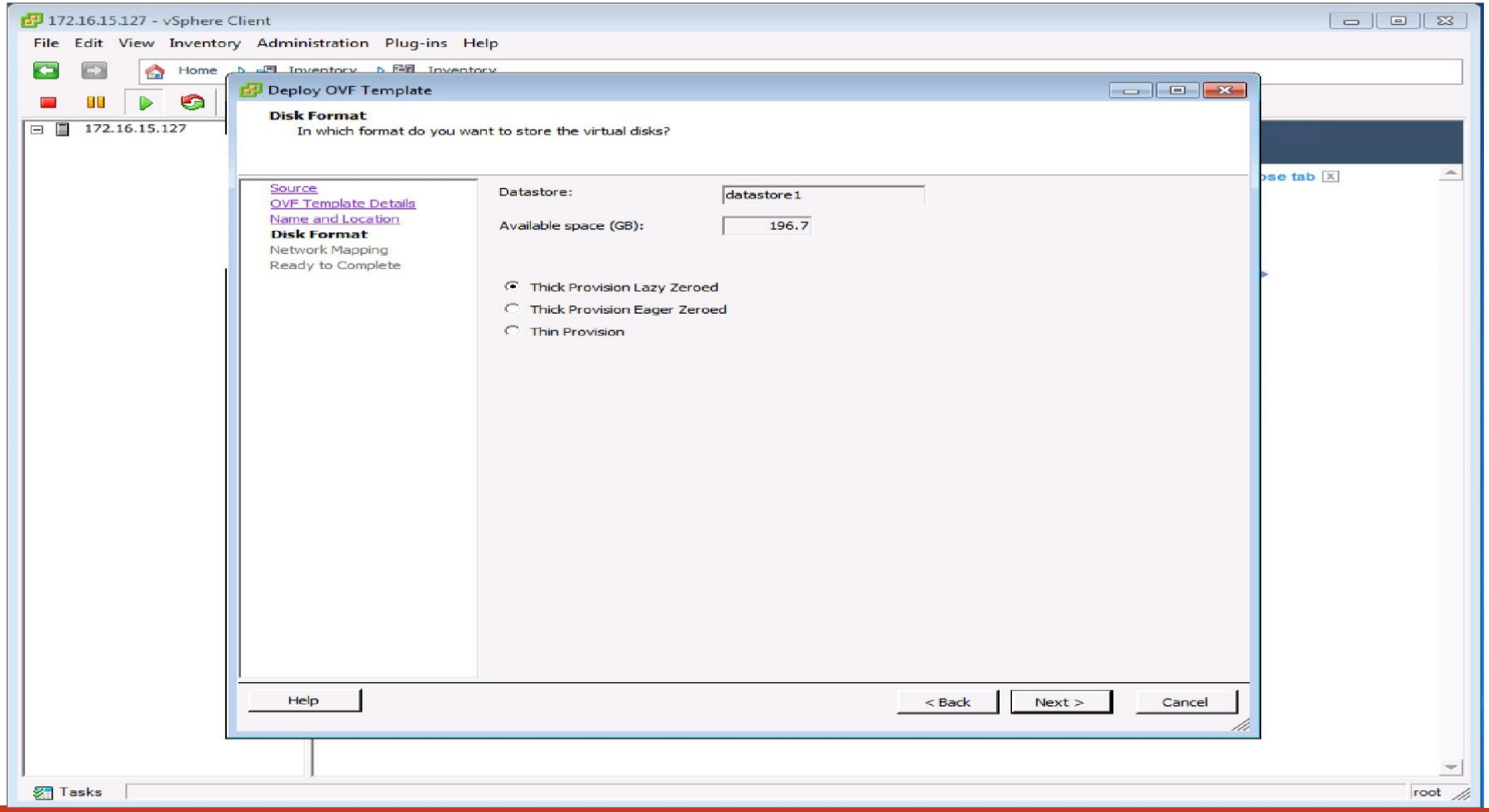
368257

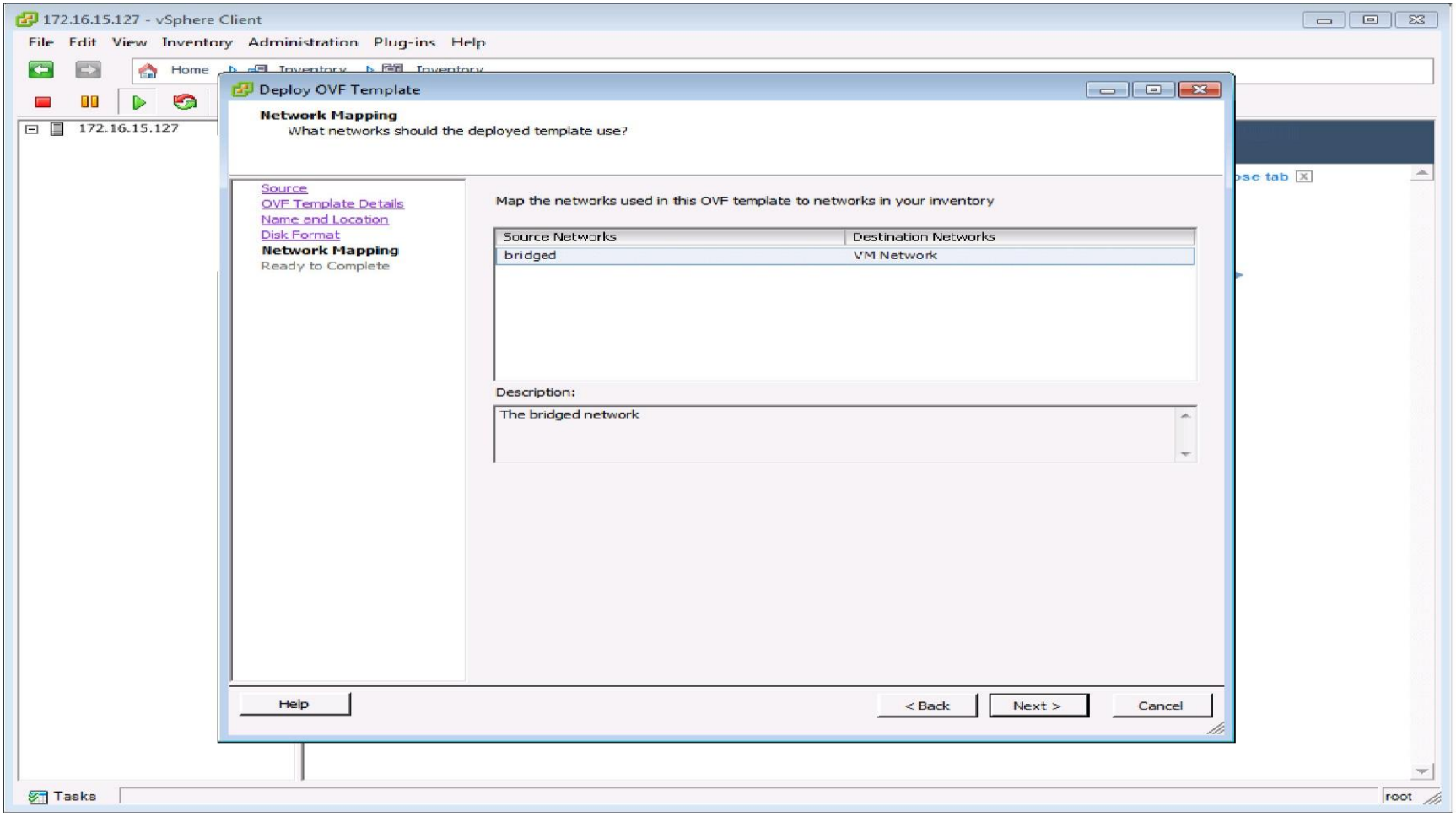

172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Source
Select the source location.
Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete
Deploy from a file or URL
C:\Users\manoj\Downloads\viptela-vManage
Browse...
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help
< Back
Next >
Cancel
Tasks
root

368344

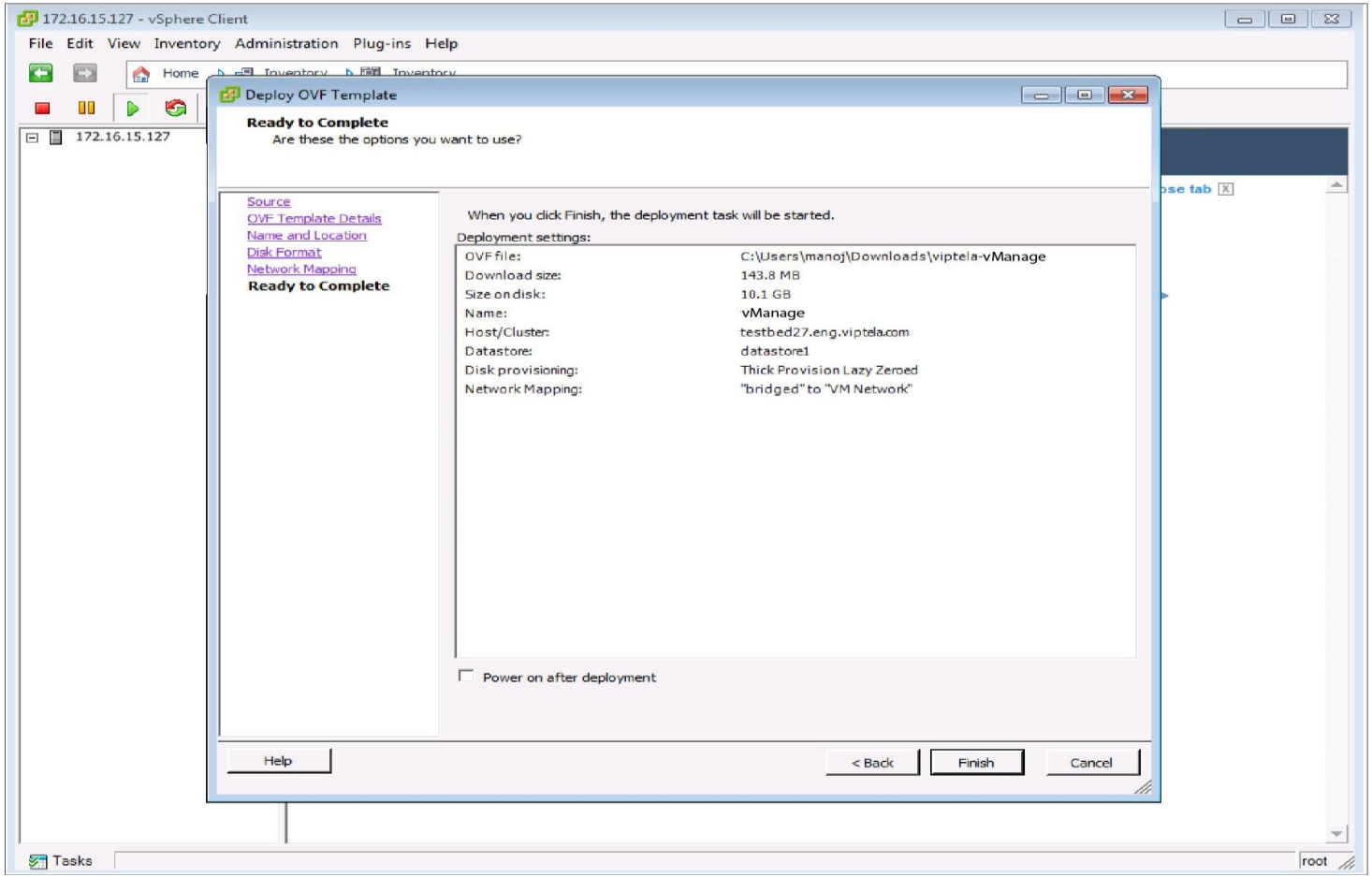

172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
OVF Template Details
Verify OVF template details.
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
Product: vManage
Version:
Vendor:
Publisher: No certificate present
Download size: 143.8 MB
Size on disk: 146.9 MB (thin provisioned)
10.1 GB (thick provisioned)
Description:
Help
< Back
Next >
Cancel
Tasks
root


172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Name and Location
Specify a name and location for the deployed template
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
Name:
vManage
The name can contain up to 80 characters and it must be unique within the inventory folder.
Help
< Back
Next >
Cancel
Tasks
root

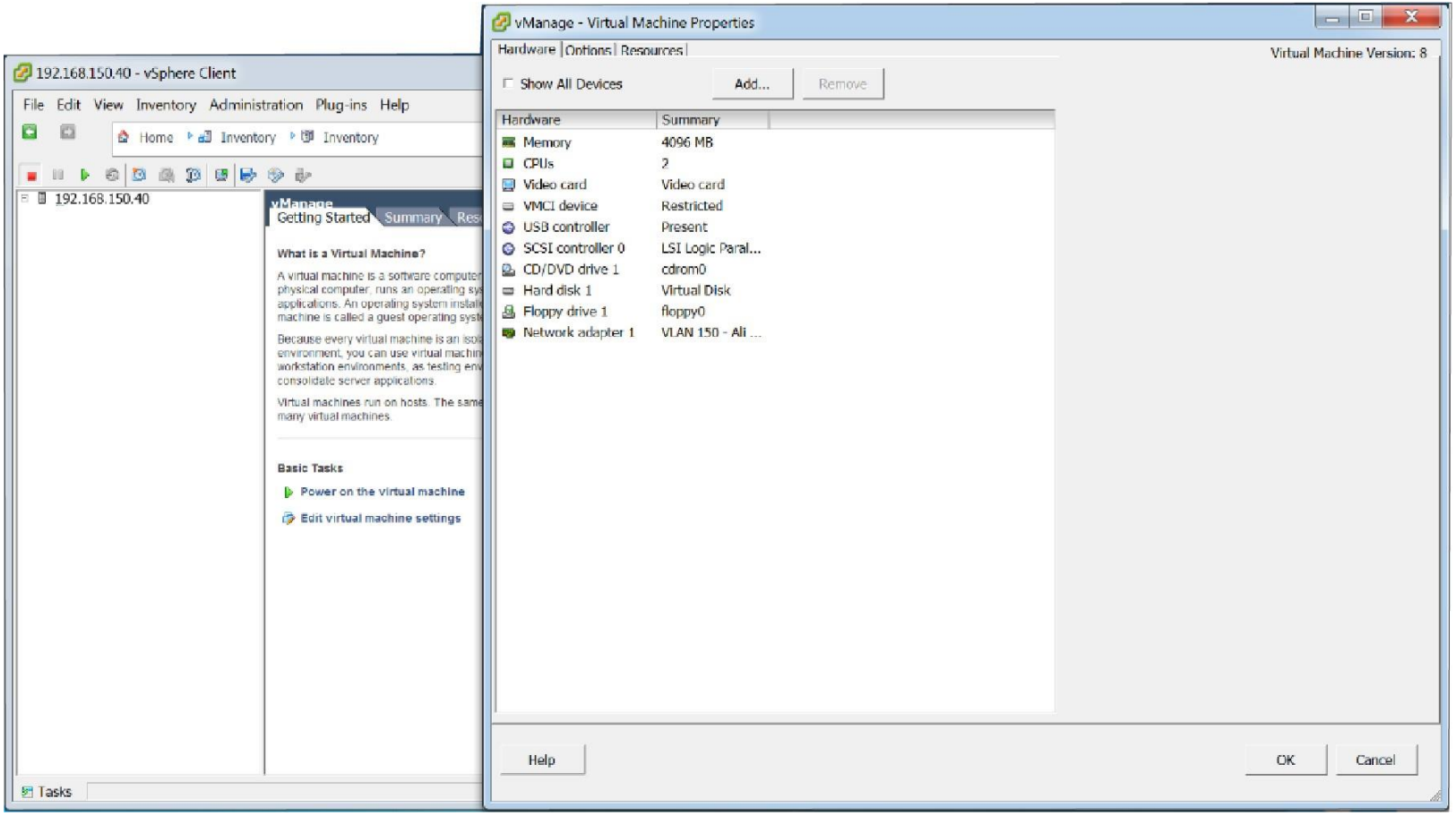

172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Disk Format
In which format do you want to store the virtual disks?
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
Datastore:
datastore1
Available space (GB):
196.7
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Help
< Back
Next >
Cancel
Tasks
root


172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
bridged
VM Network
Description:
The bridged network
Help
< Back
Next >
Cancel
Tasks
root

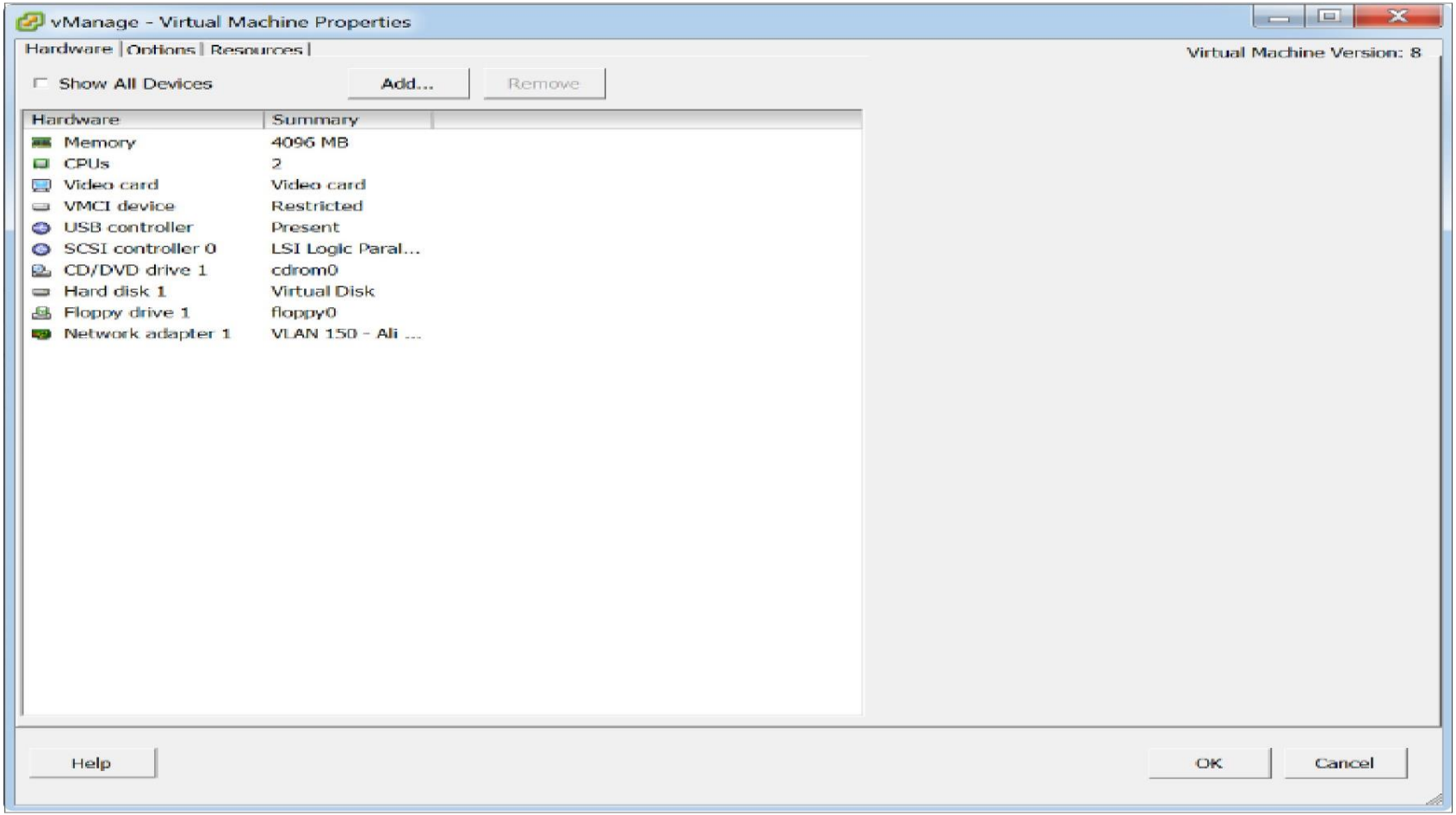
368246


172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Ready to Complete
Are these the options you want to use?
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
When you click Finish, the deployment task will be started.
Deployment settings:
OVF file: C:\Users\manoj\Downloads\viptela-vManage
Download size: 143.8 MB
Size on disk: 10.1 GB
Name: vManage
Host/Cluster: testbed27.eng.viptela.com
Datastore: datastore1
Disk provisioning: Thick Provision Lazy Zeroed
Network Mapping: "bridged" to "VM Network"
Power on after deployment
Help
< Back
Finish
Cancel
Tasks
root

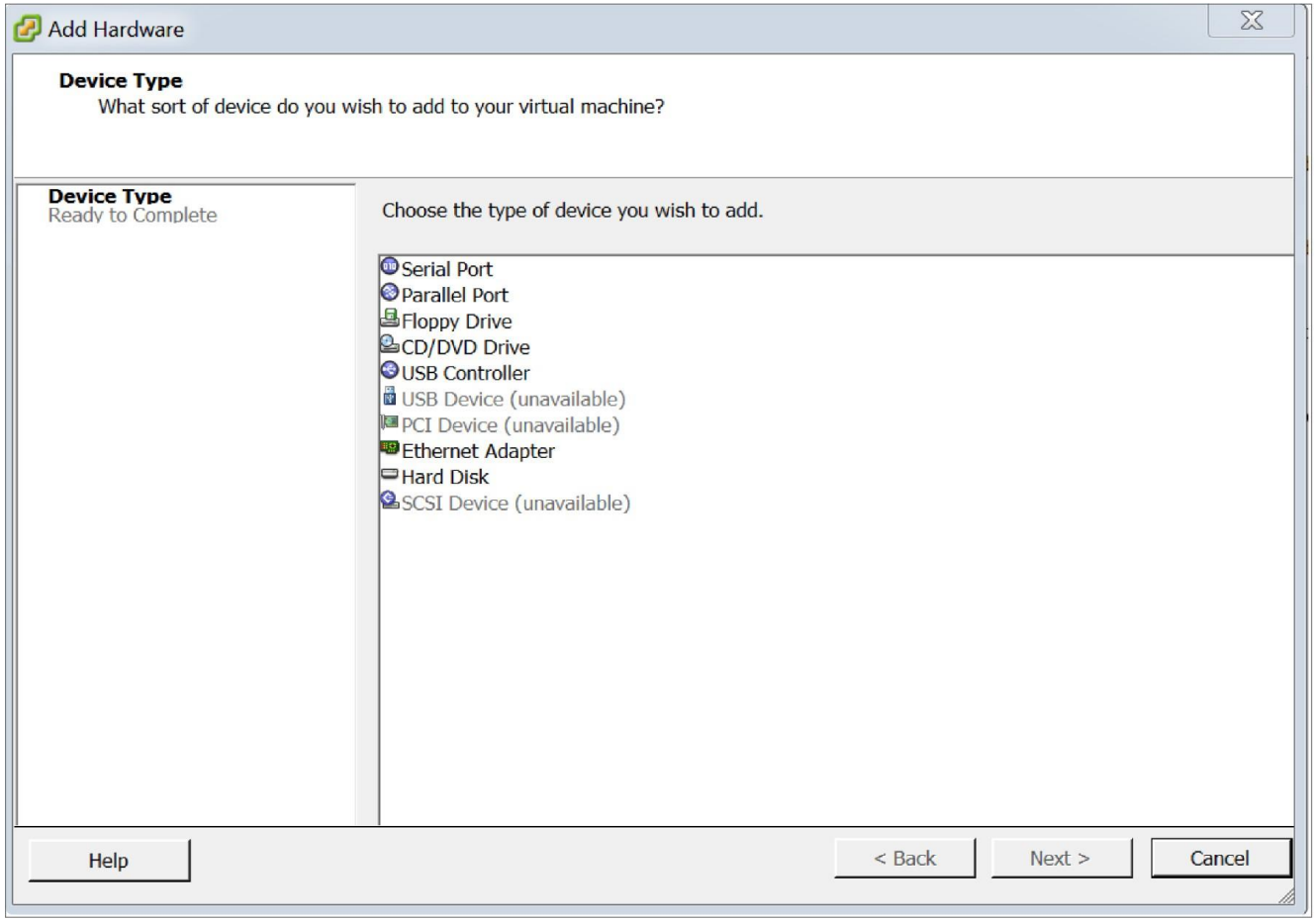
368347


192.168.150.40 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.150.40
vManage
Getting Started Summary
What is a Virtual Machine?
Basic Tasks
Power on the virtual machine
Edit virtual machine settings
Tasks
vManage - Virtual Machine Properties
Hardware Options Resources
Virtual Machine Version: 8
Show All Devices
Add...
Remove
Hardware Summary
Memory 4096 MB
CPUs 2
Video card Video card
VMCI device Restricted
USB controller Present
SCSI controller 0 LSI Logic Paral...
CD/DVD drive 1 cdrom0
Hard disk 1 Virtual Disk
Floppy drive 1 floppy0
Network adapter 1 VLAN 150 - Ali ...
Help
OK
Cancel

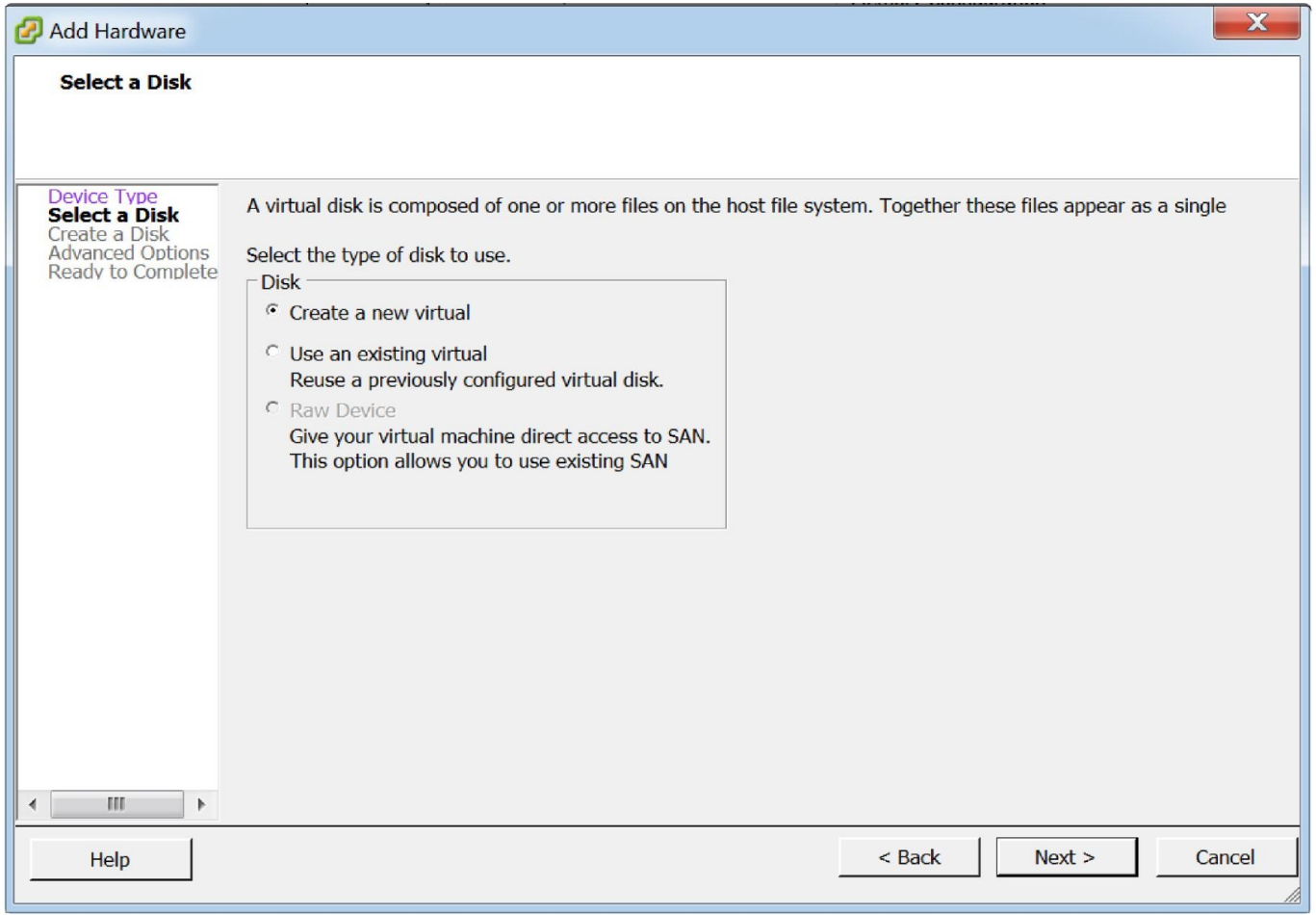
368337


vManage - Virtual Machine Properties
Hardware | Options | Resources |
Virtual Machine Version: 8
Show All Devices
Add...
Remove
Hardware
Summary
Memory
4096 MB
CPUs
2
Video card
Video card
VMCI device
Restricted
USB controller
Present
SCSI controller 0
LSI Logic Paral...
CD/DVD drive 1
cdrom0
Hard disk 1
Virtual Disk
Floppy drive 1
floppy0
Network adapter 1
VLAN 150 - Ali ...
Help
OK
Cancel

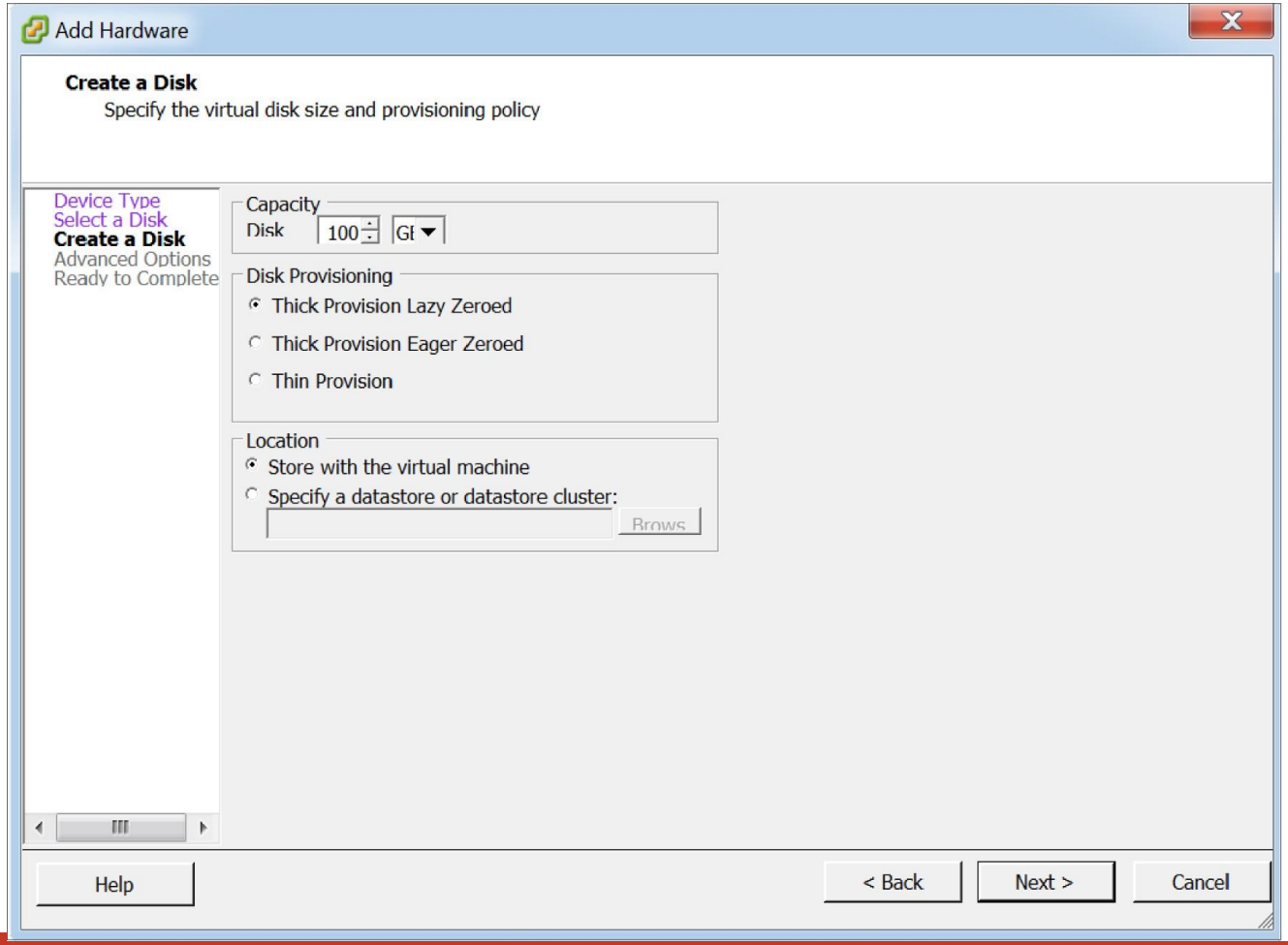
368336


Add Hardware
Device Type
What sort of device do you wish to add to your virtual machine?
Device Type
Ready to Complete
Choose the type of device you wish to add.
Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device (unavailable)
Help
< Back
Next >
Cancel

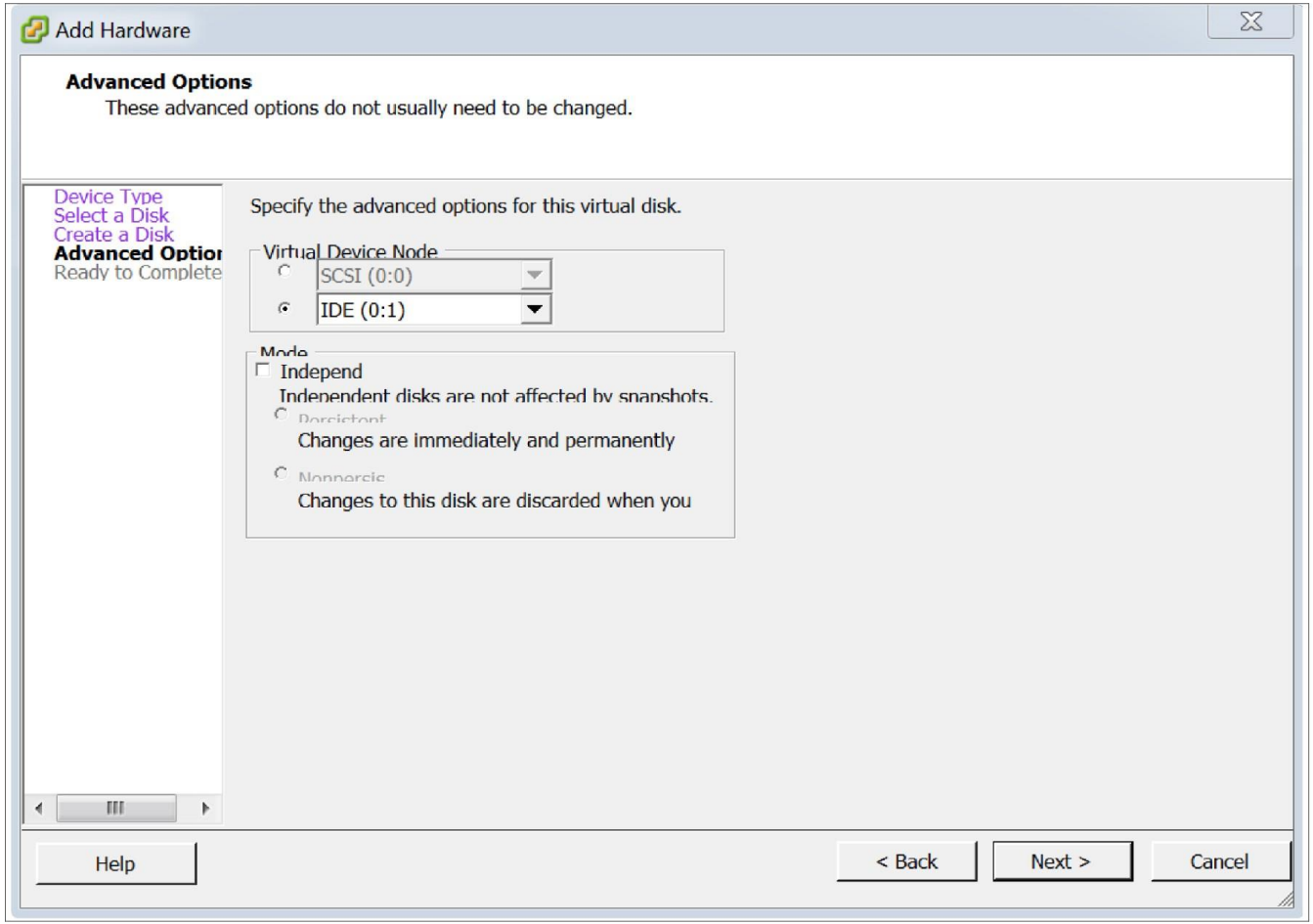
368341


Add Hardware
Select a Disk
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
A virtual disk is composed of one or more files on the host file system. Together these files appear as a single
Select the type of disk to use.
Disk
Create a new virtual
Use an existing virtual
Reuse a previously configured virtual disk.
Raw Device
Give your virtual machine direct access to SAN.
This option allows you to use existing SAN
Help
< Back
Next >
Cancel

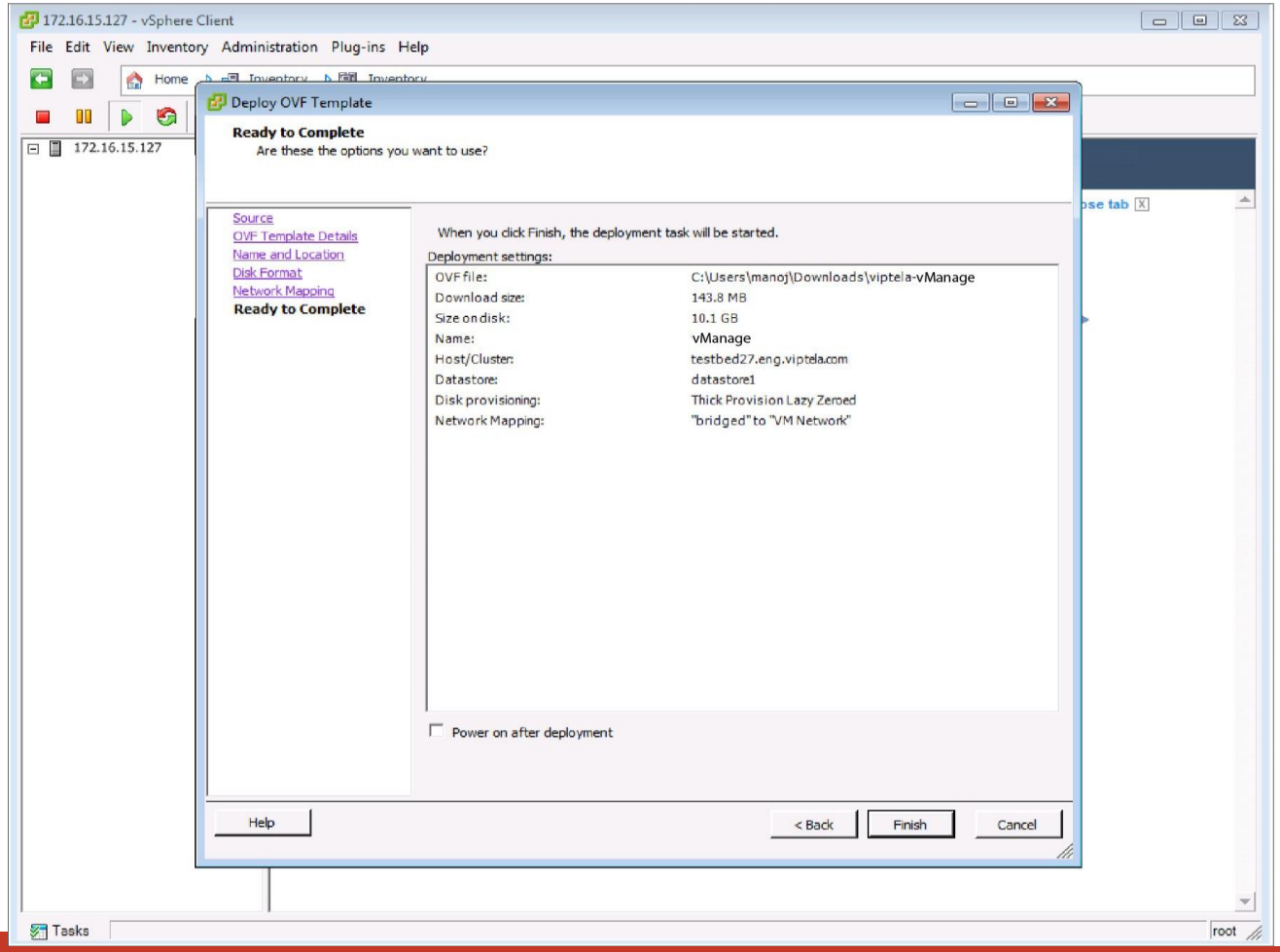
368339

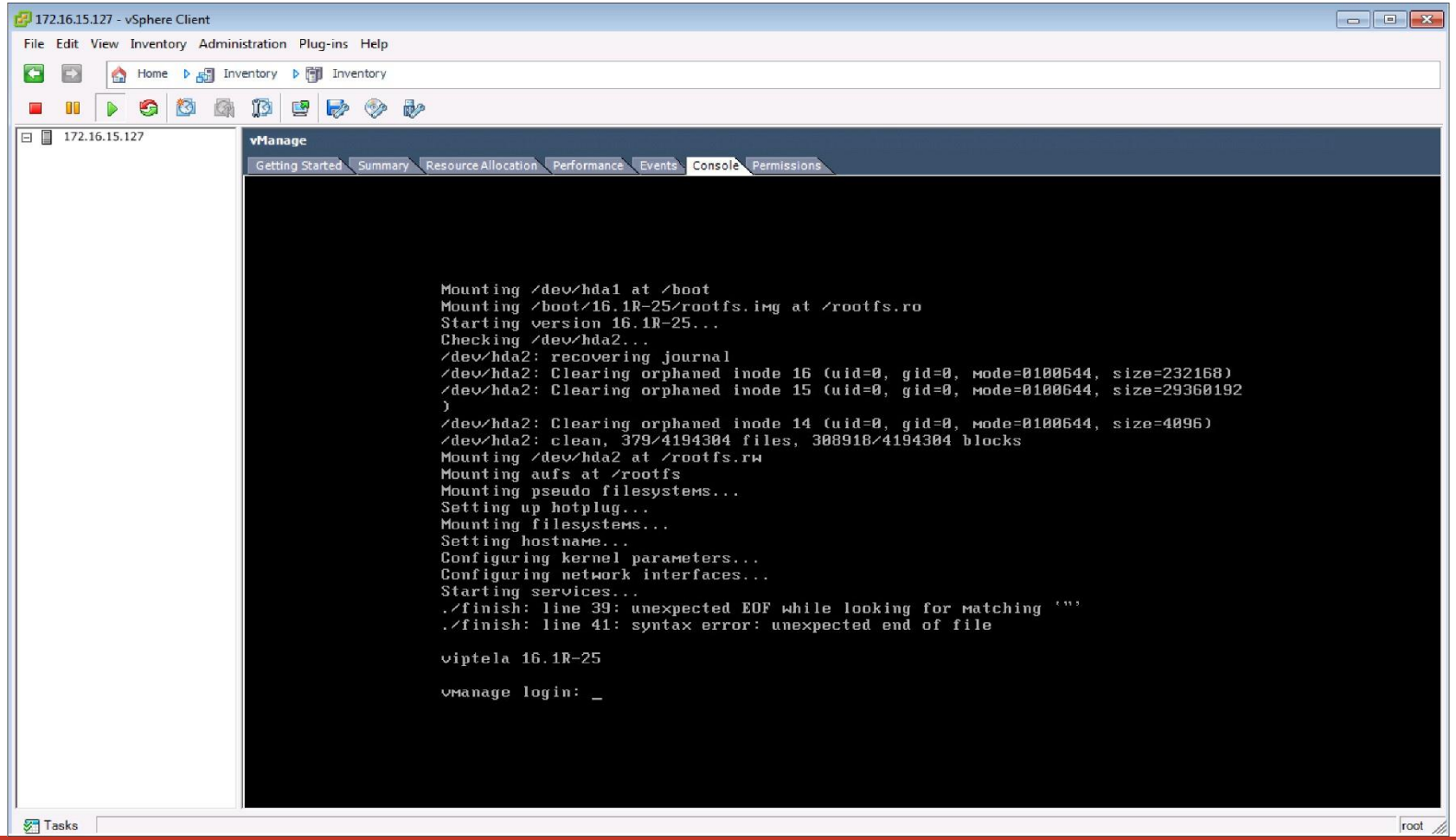

Add Hardware
Create a Disk
Specify the virtual disk size and provisioning policy
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Capacity
Disk
100
GI
Disk Provisioning
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Location
Store with the virtual machine
Specify a datastore or datastore cluster:
Brows
Help
< Back
Next >
Cancel

368340

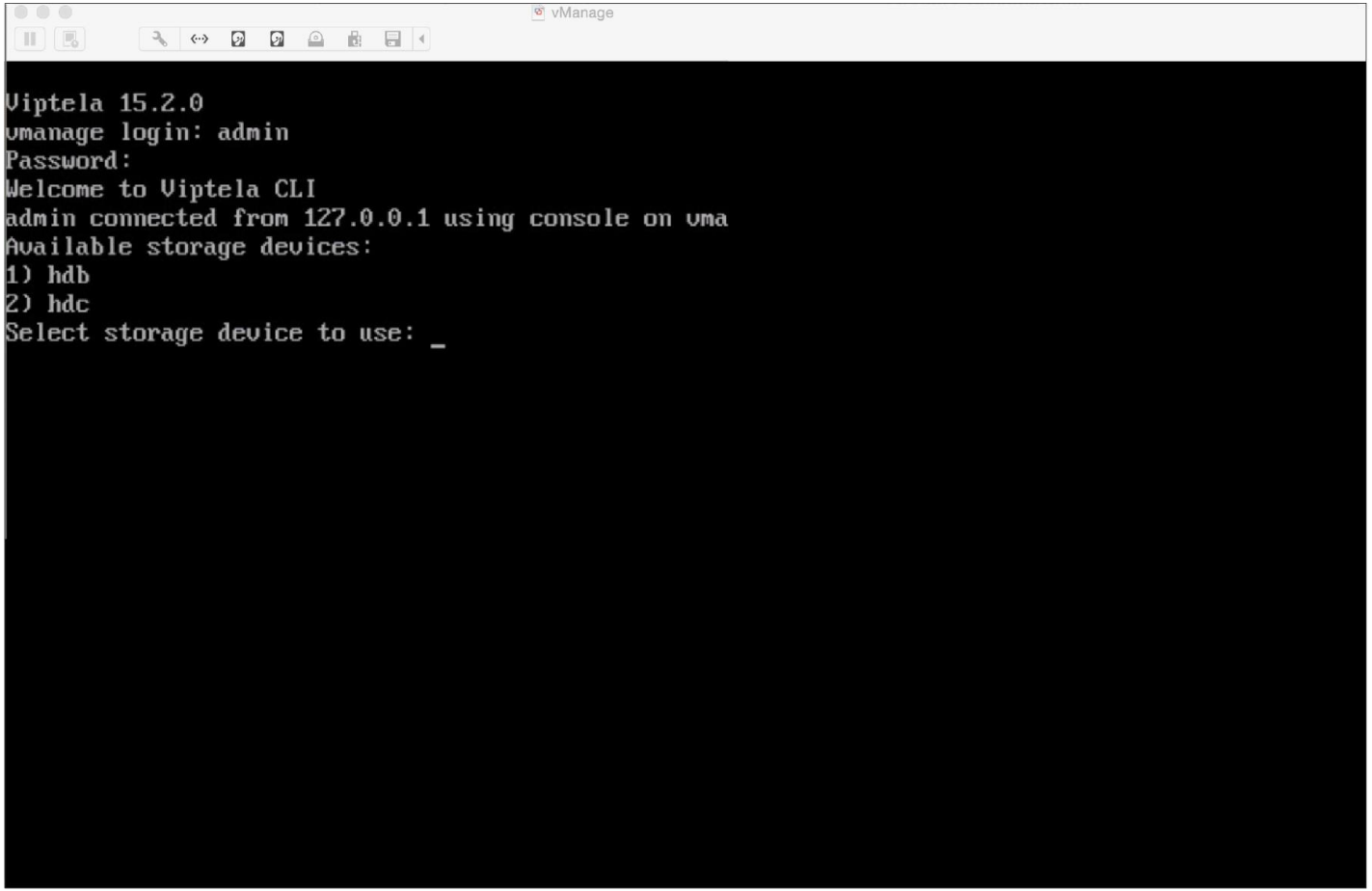

Add Hardware
Advanced Options
These advanced options do not usually need to be changed.
Device Type
Select a Disk
Create a Disk
Advanced Optior
Ready to Complete
Specify the advanced options for this virtual disk.
Virtual Device Node
SCSI (0:0)
IDE (0:1)
Mode
Independ
Independent disks are not affected by snapshots.
Persistent
Changes are immediately and permanently
Nonpersis
Changes to this disk are discarded when you
Help
< Back
Next >
Cancel

368338

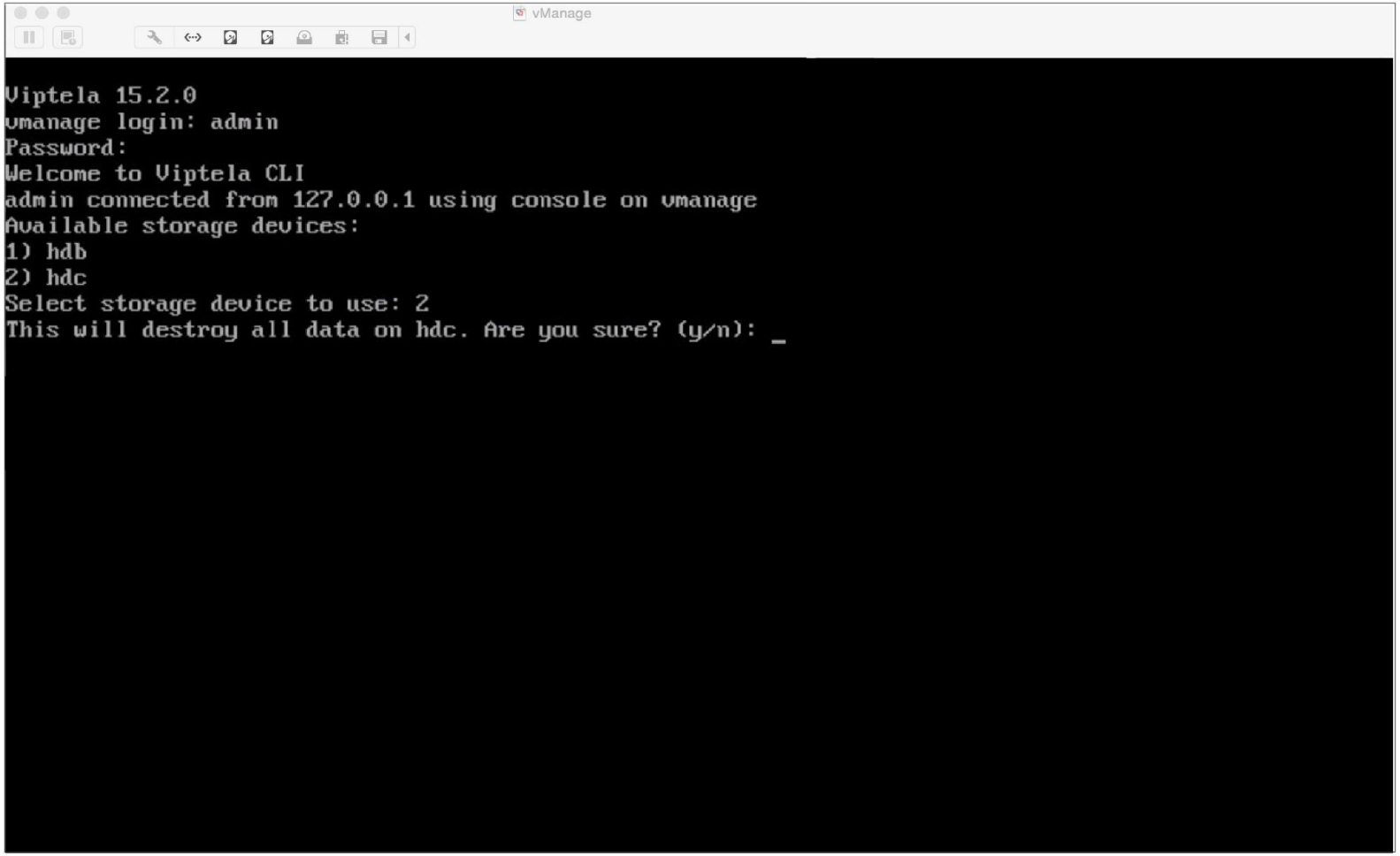

172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.15.127
Deploy OVF Template
Ready to Complete
Are these the options you want to use?
Source
OVF Template Details
Name and Location
Disk Format
Network Mapping
Ready to Complete
When you click Finish, the deployment task will be started.
Deployment settings:
OVF file: C:\Users\manoj\Downloads\viptela-vManage
Download size: 143.8 MB
Size on disk: 10.1 GB
Name: vManage
Host/Cluster: testbed27.eng.viptela.com
Datastore: datastore1
Disk provisioning: Thick Provision Lazy Zeroed
Network Mapping: "bridged" to "VM Network"
Power on after deployment
Help
< Back
Finish
Cancel
Tasks
root


172.16.15.127 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
172.16.15.127
vManage
Getting Started Summary Resource Allocation Performance Events Console Permissions
Mounting /dev/hda1 at /boot
Mounting /boot/16.1R-25/rootfs.img at /rootfs.ro
Starting version 16.1R-25...
Checking /dev/hda2...
/dev/hda2: recovering journal
/dev/hda2: Clearing orphaned inode 16 (uid=0, gid=0, mode=0100644, size=232168)
/dev/hda2: Clearing orphaned inode 15 (uid=0, gid=0, mode=0100644, size=29360192
)
/dev/hda2: Clearing orphaned inode 14 (uid=0, gid=0, mode=0100644, size=4096)
/dev/hda2: clean, 379/4194304 files, 308918/4194304 blocks
Mounting /dev/hda2 at /rootfs.rw
Mounting aufs at /rootfs
Mounting pseudo filesystems...
Setting up hotplug...
Mounting filesystems...
Setting hostname...
Configuring kernel parameters...
Configuring network interfaces...
Starting services...
./finish: line 39: unexpected EOF while looking for matching `"'
./finish: line 41: syntax error: unexpected end of file
viptela 16.1R-25
vmanage login: _
Tasks
root

368352


vManage
Viptela 15.2.0
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vma
Available storage devices:
1) hdb
2) hdc
Select storage device to use: _

368334


vManage
Viptela 15.2.0
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
Available storage devices:
1) hdb
2) hdc
Select storage device to use: 2
This will destroy all data on hdc. Are you sure? (y/n): _

368335

a. Log in with the default username and password:

```
Login: admin  password:
admin  #
```

b. In the management VPN, VPN 512, configure an IP address on interface eth0. Specify an IP address that is reachable on your network. If necessary, add a default route:

```
# config
(config)# vpn 512
(config)# ip route prefix/length next-hop-ip-address
(config-vpn-512)# interface eth0
(config-interface-eth0)# ip address ip-address
(config-interface-eth0)# no shutdown
(config-interface-eth0)# commit and-quit
#
```

7. To connect to the vManage instance, type the following string in the URL:

   https:// *ip-address* **:8443/**

8. Log in with the username **admin** and the password **admin**.

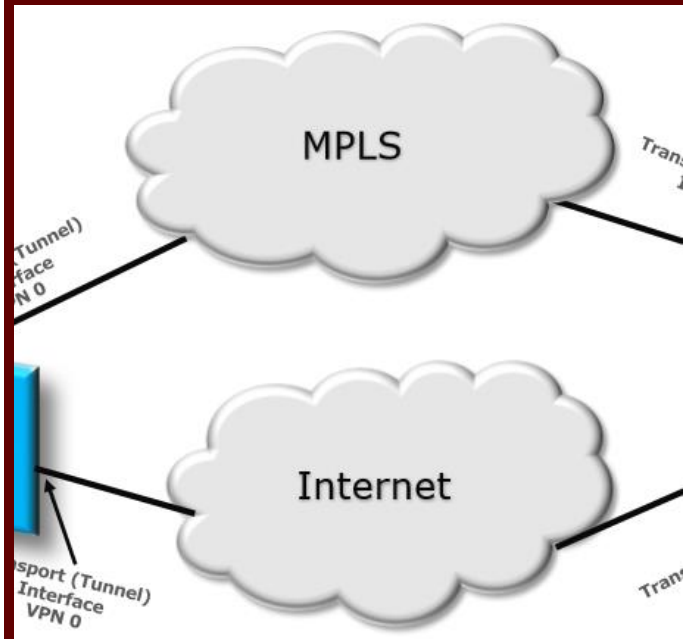
System bring & Demo Lab

System bring up process includes these steps:

1.Install hypervisor (KVM) on the server (preconfigured).
2.Spin-up virtual machines on the server (preconfigured).
3.Install images for vManage, vBond, vSmart and vEdges on the virtual machines (preconfigured).
4.Create a minimal configuration for vManage (Deploy vManage section).
5.Create a minimal configuration for vBond (Deploy vBond section).
6.Create a minimal configuration for vSmart (Deploy vSmart section).
7.Enable connectivity between Controllers (Enable Inter-Controller Connectivity section).
8.Generate CSRs for each Controller (Overlay Connections section).
9.Sign certificates to validate and authenticate the Controllers. (Certificate Signature section).

Configuration Elements in a Device

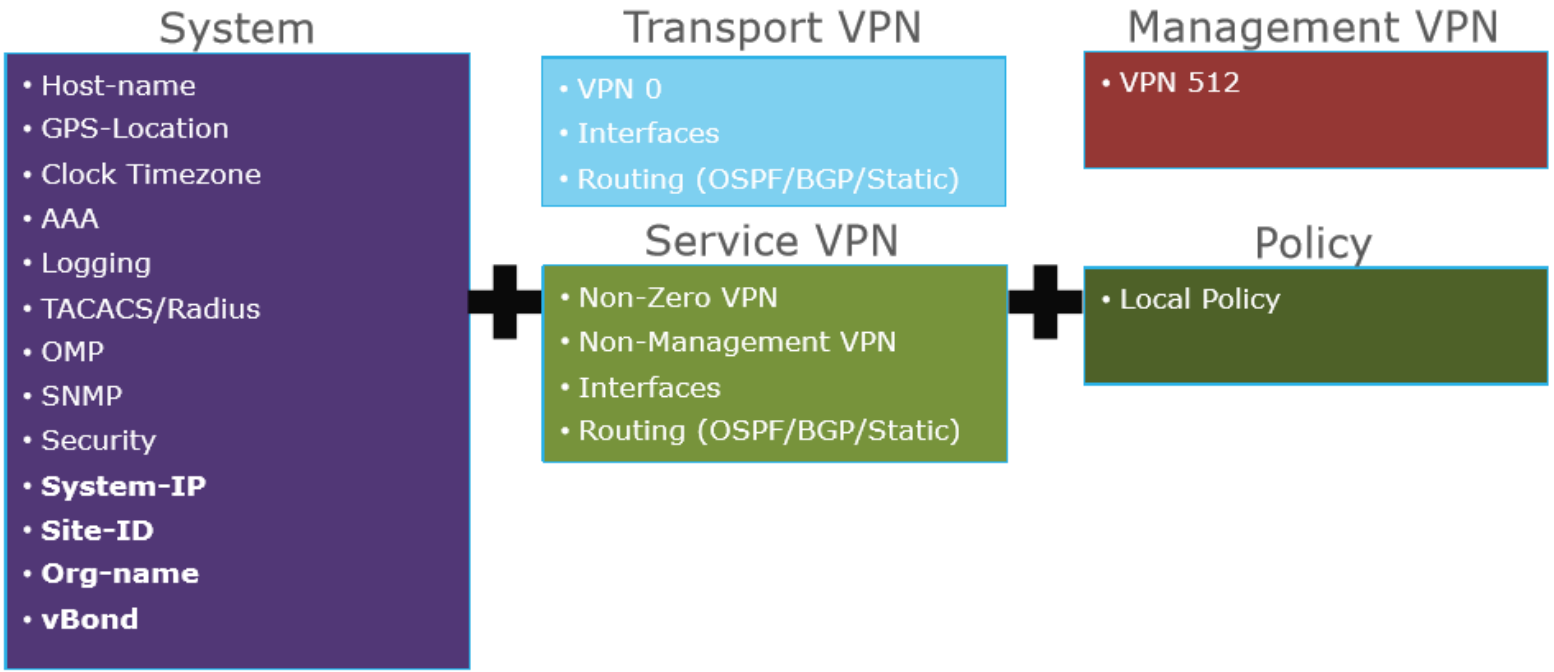
- **System Configuration**
- • System ip address (Unique)
- • Site-id
- • System Organization name
- (This needs to be the same for all)
- • vBond ip address
- • Host-name (Unique)
- **Device Specific configuration**
- (Interface level)
- • Tunnel-interface
- VPN 0
- • Management Interface
- VPN 512
- • Service Interface
- VPN 1 – 511 , VPN 513 - 65530



CLI Configuration Example for vSmart

vSmart# Config t (Start the configuration mode)
vSmart(config)#
(system ready to accept configuration commands)
vSmart(config)# system
(starting System Mode)
vSmart(config-system)#system-ip 12.12.12.12
 (Assign system-ip- it should be a unique value)
vSmart(config-system)# site-id 10
(Site-id’s can be shared with other devices on site
vSmart(config-system)# commit
(write the configuration changes to device Memory)
Commit complete (system wrote all changes to memory)

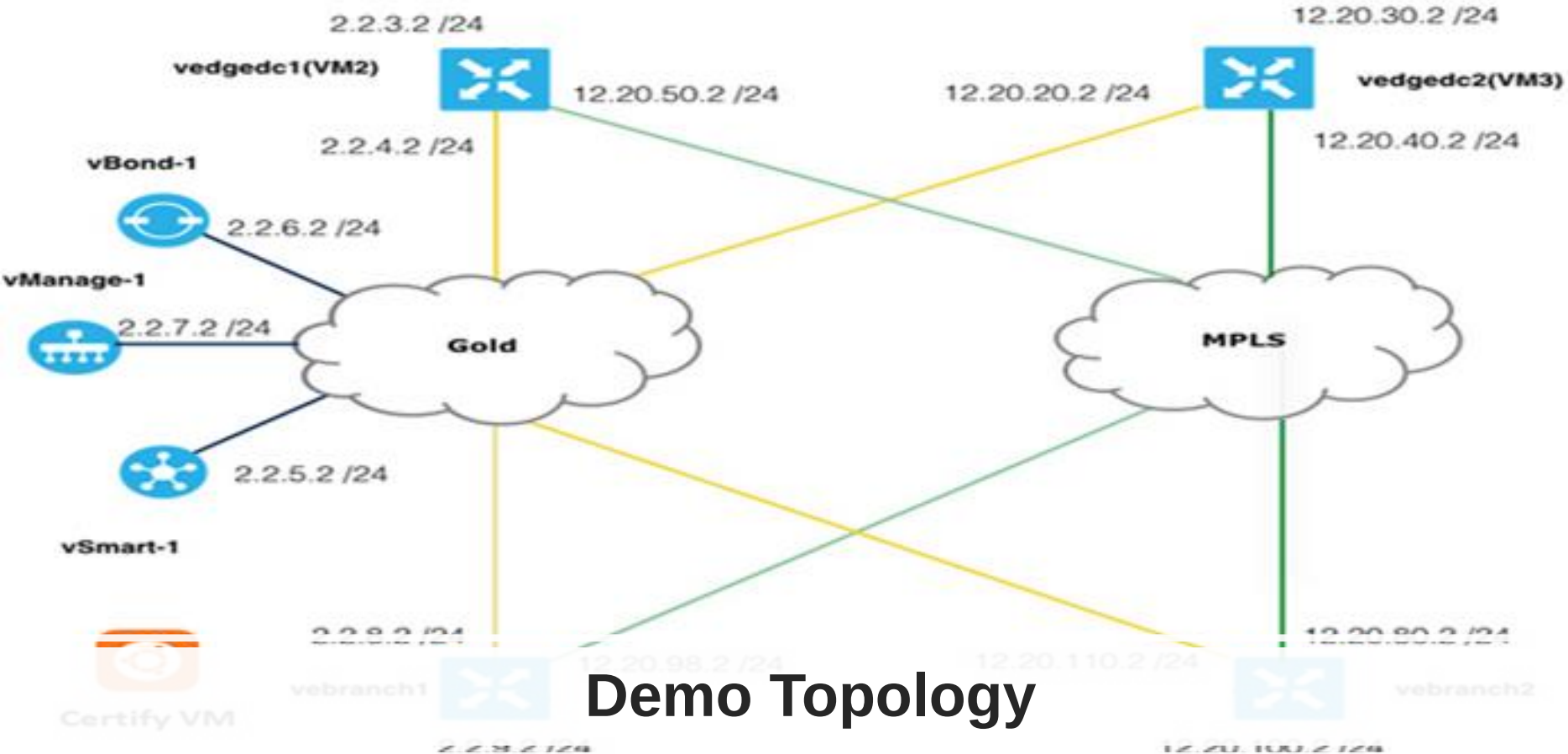
vEdge Configuration Components



Transport Parameters	Details
VPN0	Carries control traffic between vSmart and vEdge. Also between vSmart and vBond orchestrators. It also carries all securely encrypted data traffic between sites.
Tunnel Interface	Configure DTLS or TLS WAN transport connection. Configuring transport tunnel enables the flow of control and data traffic on the interface.
Service VPN (Non Zero VPN)	VPN other than 0 and 512
VPN 512	Management VPN, carries out-of-band network management traffic among the Viptela devices in the network. It is not a routable VPN.

Series of Viptela Fabric Bring up labs

- Controllers System wide Configuration
- vManage VPN & Static Rotue Configuration
- vSmart & vBond VPN & Static Rotue Configuration
- Add Controllers to vManage Dashboard
- Add CSR to Root CA Server
- Permanent certificates & install certificates to controllers



Demo Topology

```
conf t
system
     host-name              vManage-1
     system-ip              172.27.0.5
     site-id                1002
     organization-name
     vbond 2.2.6.2
 !
commit and-quit
```

```
conf t
 vpn 0
    no int eth0
    vpn 512
    int eth0
     ip dhcp-client
   no shut
 commit and-quit
```

3. Configure a tunnel interface on eth1. IP address will be 2.2.7.2/24. Use the following configuration commands:

```
conf t
  vpn 0
 interface eth1
        ip address 2.2.7.2/24
        tunnel-interface
        allow-service all
    !
    mtu  1400
    no shutdown
  !
    ip route 0.0.0.0/0 2.2.7.1
    !
    commit and-quit
```

```
conf t
system
    host-name                   vBond-1
    system-ip                   172.27.0.4
    site-id                     1001
    no route-consistency-check
    organization-name
    vbond 2.2.6.2 local
 !
commit and-quit
```

Deploy vBond

```
conf t
system
 host-name          vSmart-1
 system-ip          172.27.0.6
 site-id            1000
 organization-name "
 vbond 2.2.6.2
!
commit and-quit
```

Deploy vSmart

To configure a tunnel interface:

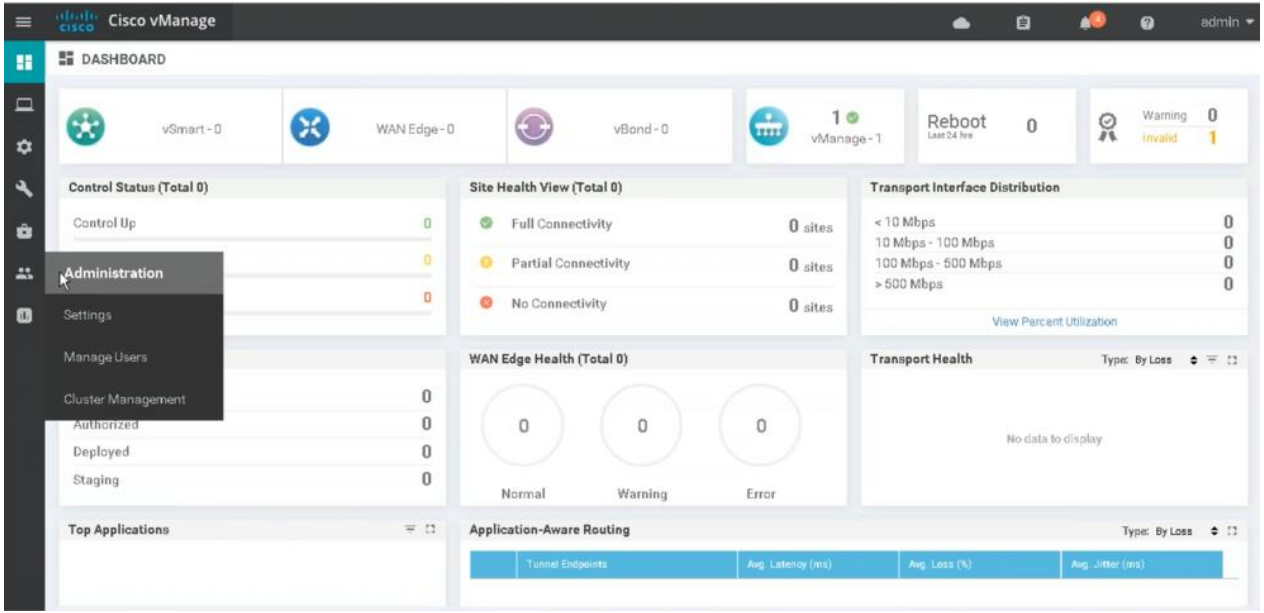
1. Use previously launched vSmart SSH session.
2. By default, the management interface **eth0** is placed in **VPN0**. Let's move it to from **VPN0** to **VPN512**.

```
conf t
 vpn 0
  no int eth0
 vpn 512
  int eth0
   ip dhcp-client
  no shut
commit and-quit
```

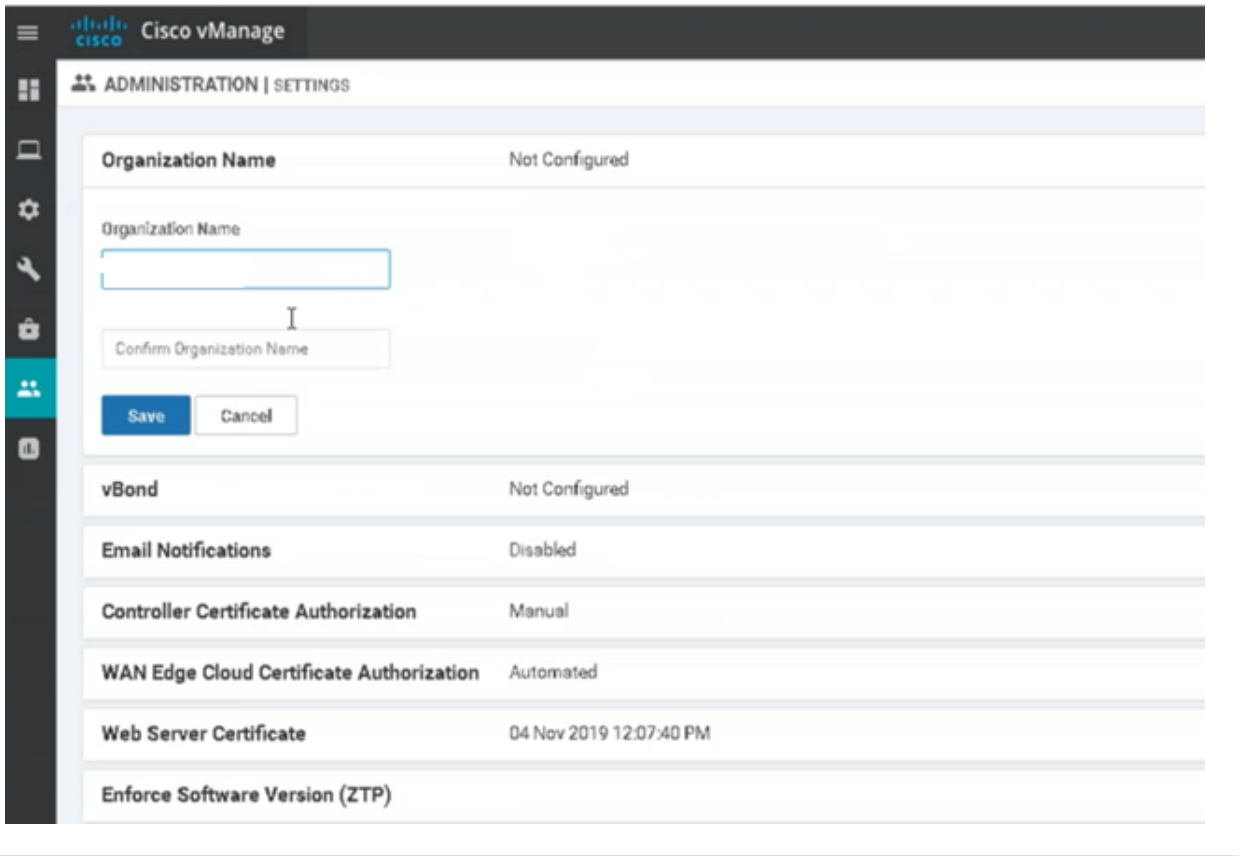
3. Configure tunnel interface on eth1. IP address will be 2.2.5.2/24. Use the following configuration commands:

```
conf t
vpn 0
 interface eth1
    ip address 2.2.5.2/24
    tunnel-interface
        allow-service all
    !
    no shutdown
```

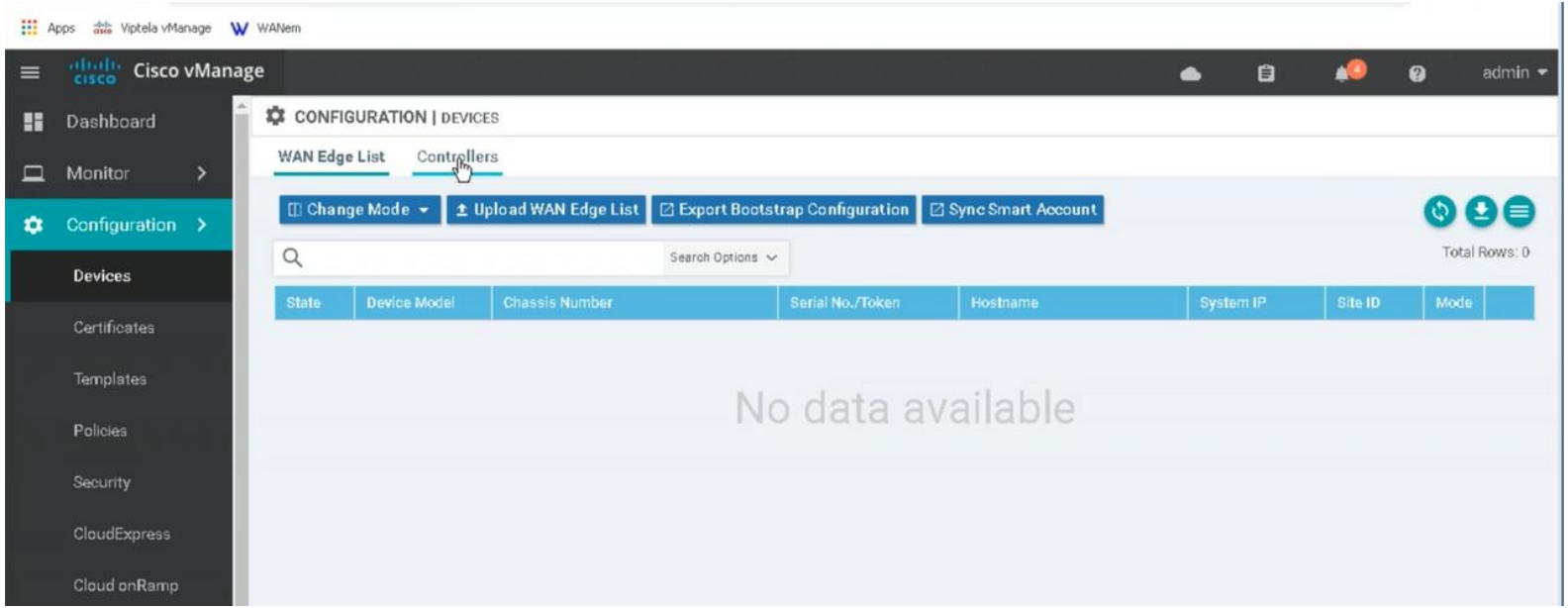
Add vBond ip & organization name to the Dashboard settings



Go to Administration & Settings



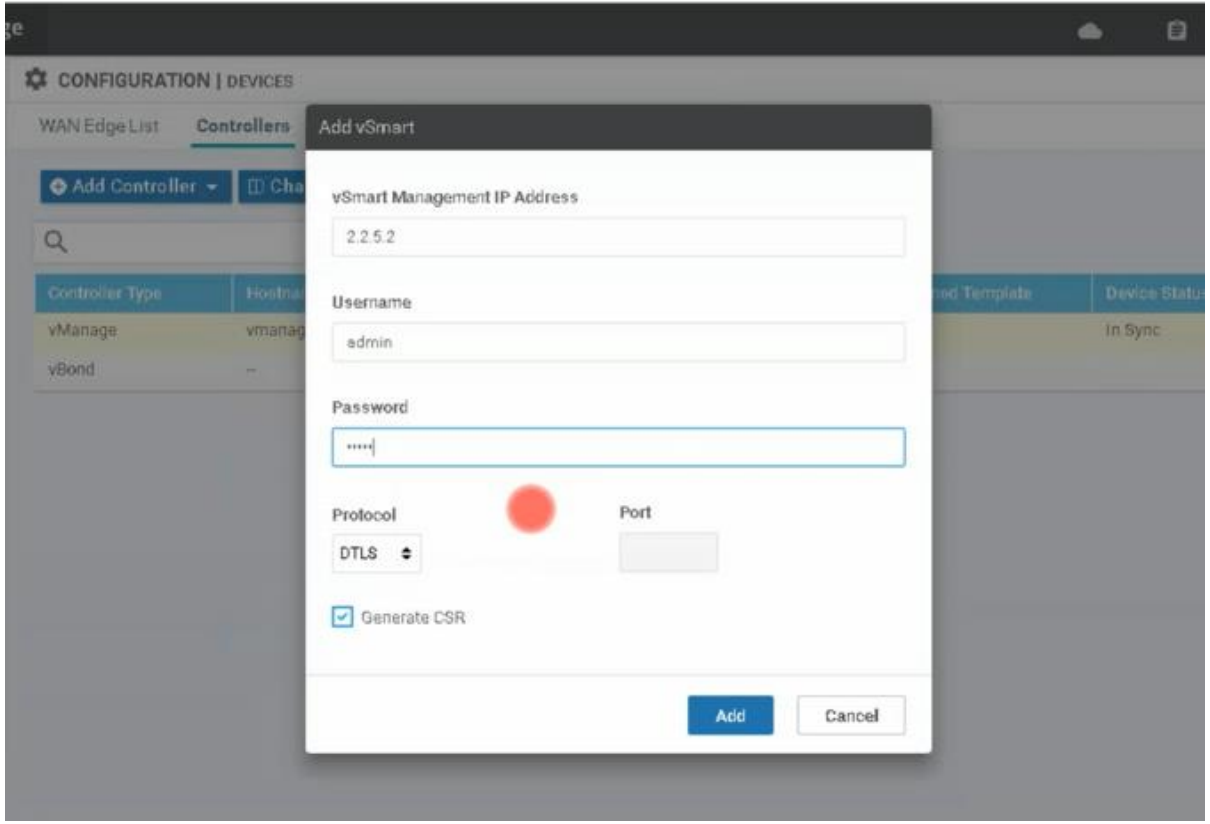
Give the Organization Name



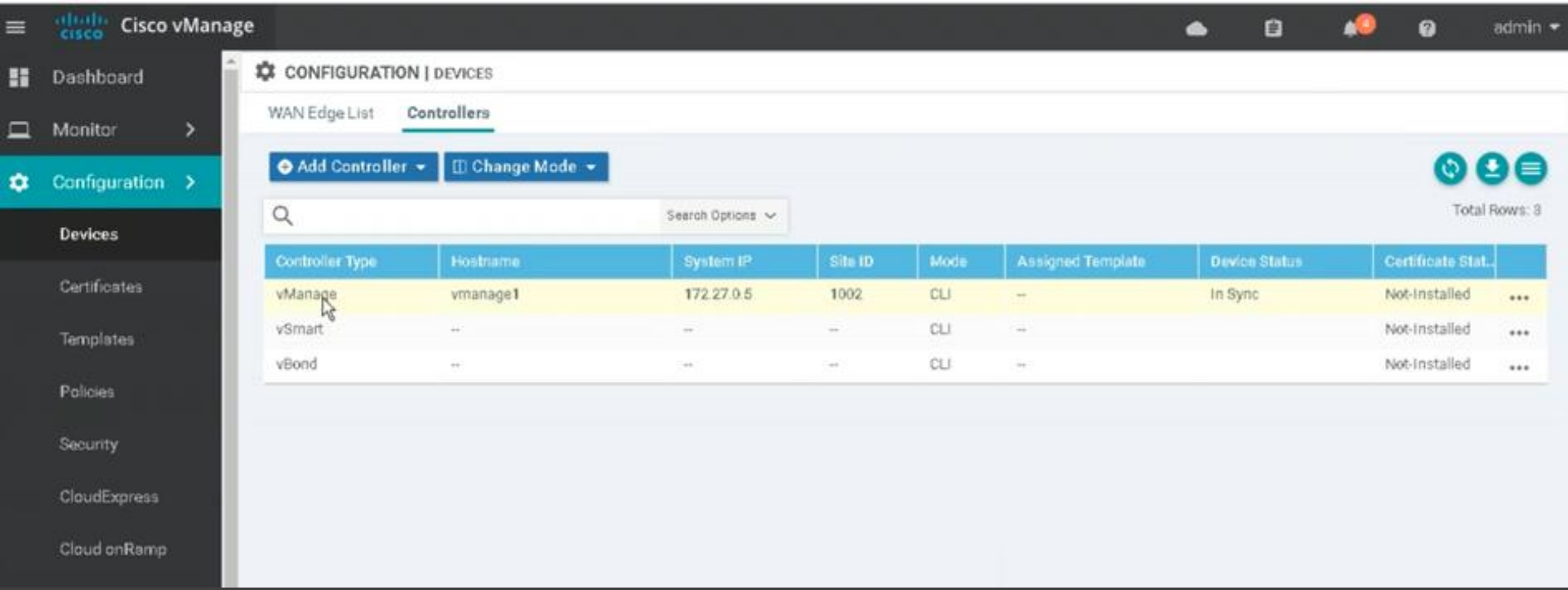
Go to Controllers

Configuration > Controllers

Add Controllers to the Dashboard

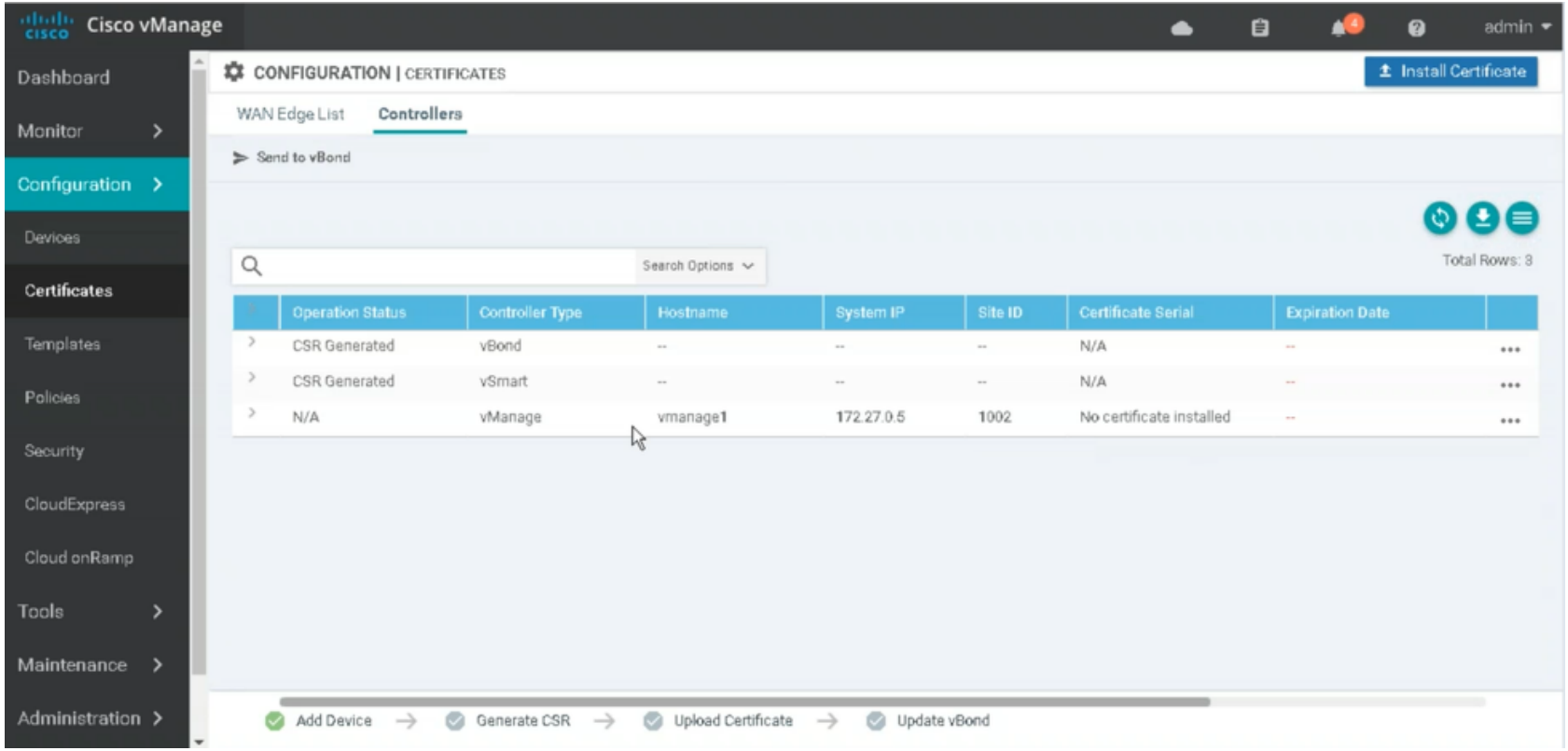

CONFIGURATION | DEVICES
WAN Edge List
Controllers
Add vSmart
Add Controller
Controller Type
vManage
vBond
In Sync
vSmart Management IP Address
2.2.5.2
Username
admin
Password
Protocol
DTLS
Port
Generate CSR
Add
Cancel

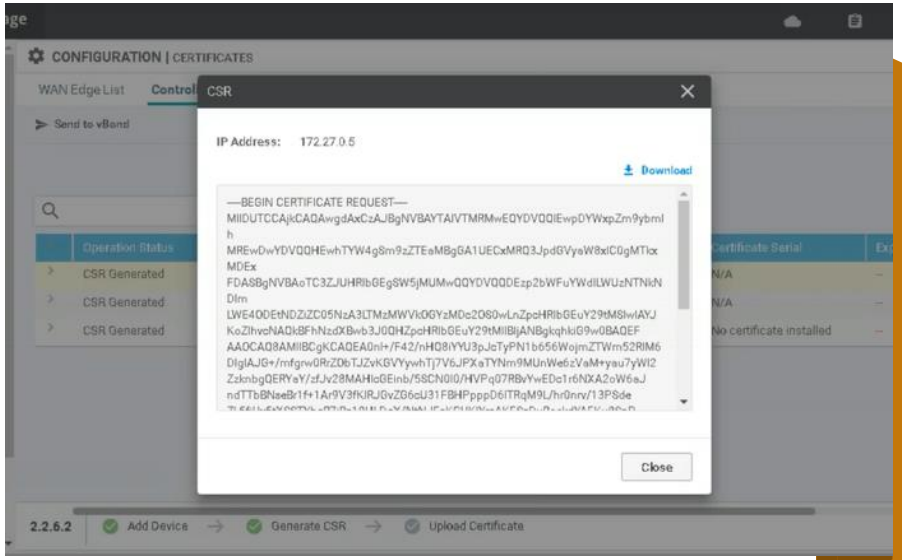
Add vSmart



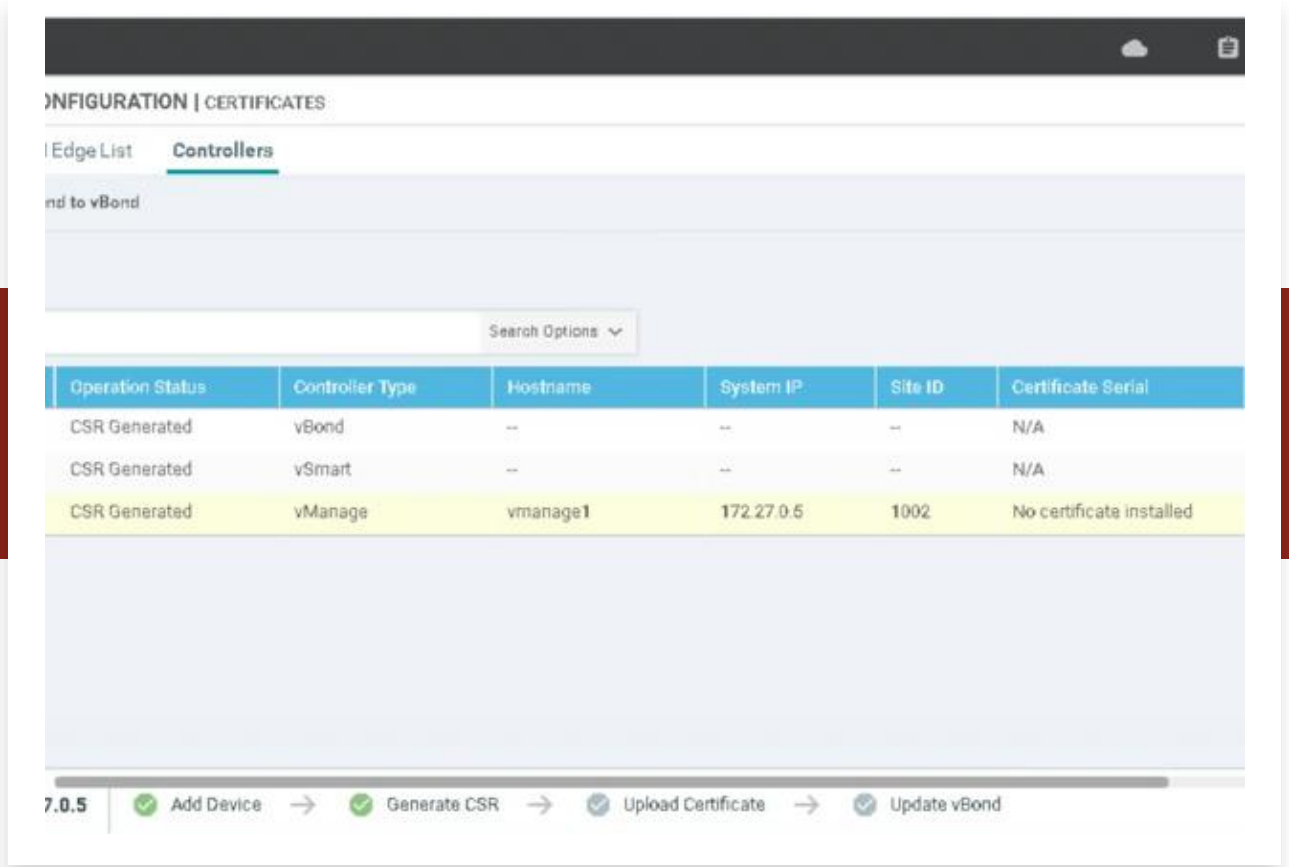
All Controllers added ☺

Generate RSA

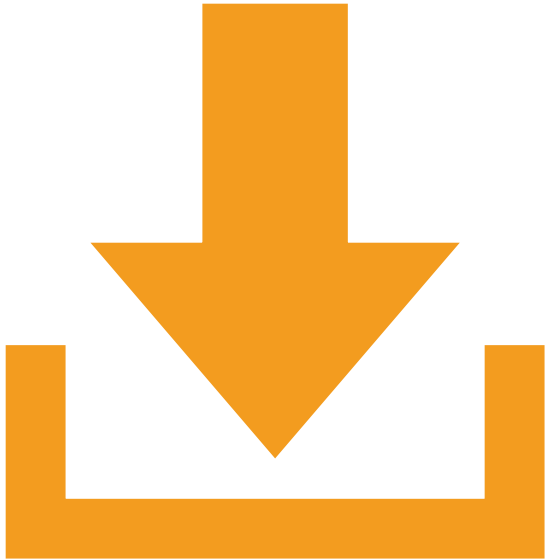

Cisco vManage
admin
Dashboard
Monitor
Configuration
Devices
Certificates
Templates
Policies
Security
CloudExpress
Cloud onRamp
Tools
Maintenance
Administration
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
Search Options
Total Rows: 3
Operation Status
Controller Type
Hostname
System IP
Site ID
Certificate Serial
Expiration Date
CSR Generated
vBond
CSR Generated
vSmart
N/A
vManage
vmanage1
172.27.0.5
1002
No certificate installed
Add Device
Generate CSR
Upload Certificate
Update vBond



Download the CSR

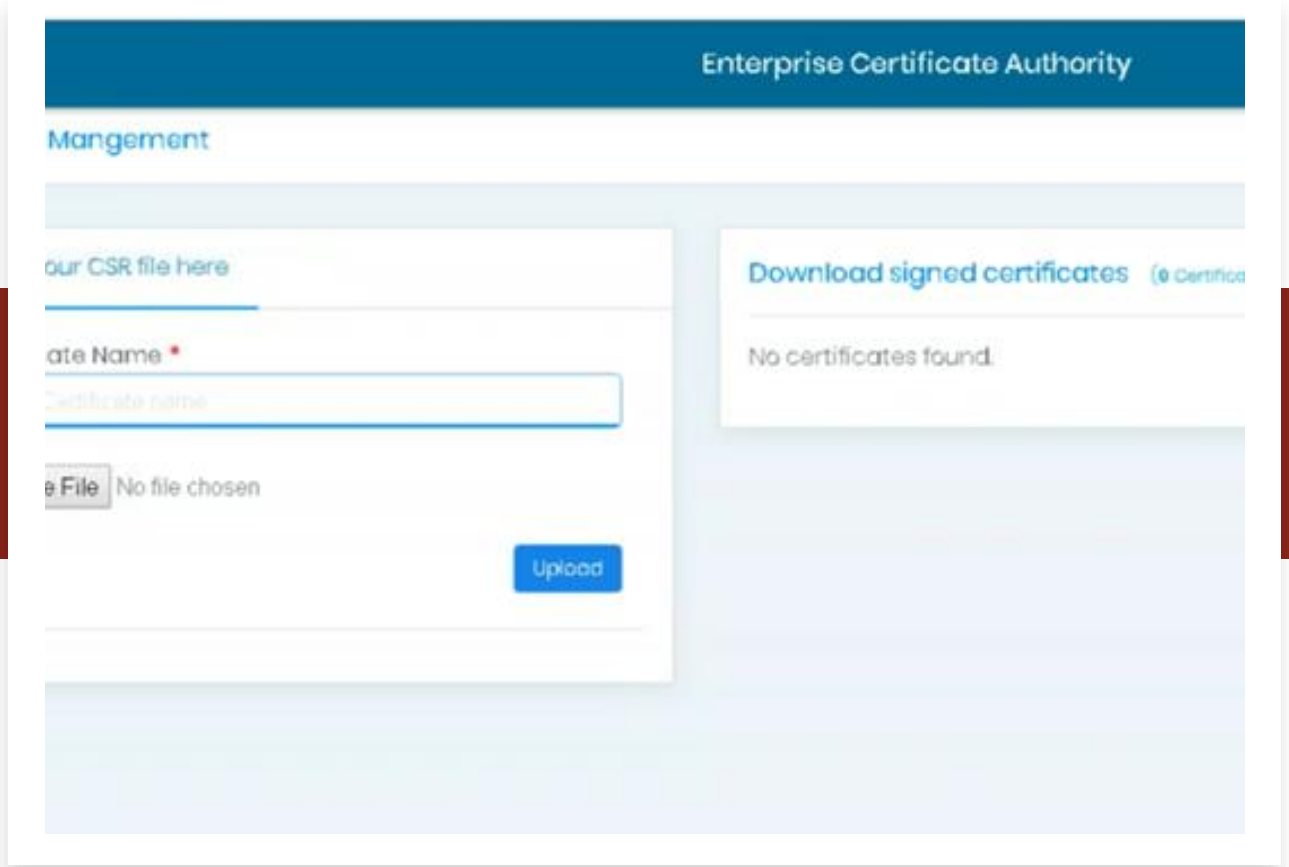


Downlaod csr for all the devices

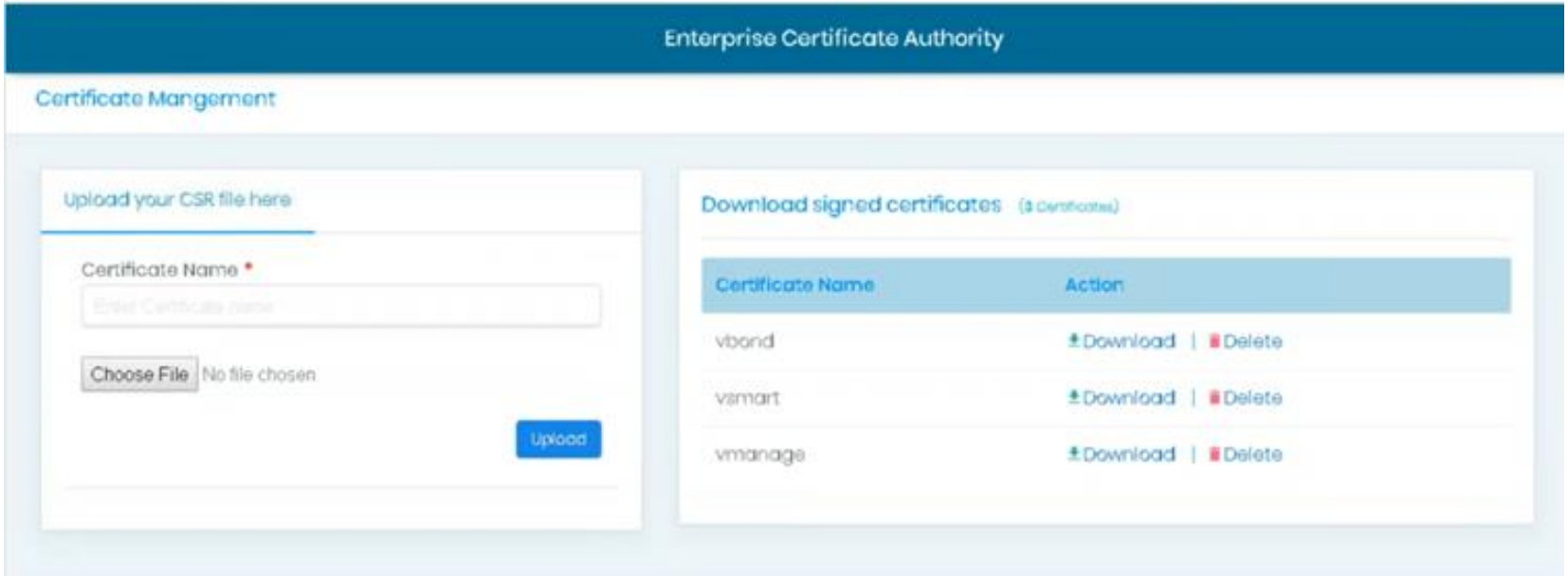


Download the CSR

From CSR generate PEM



From CSR generate PEM



Download all the PEM

Install root certificate to controllers, Control Plan authentication

Install root certificate on vManage

To open a ssh session to vManage , click on the below **Launch** button in this exercise.

Launch

Install the Root Certificate with this command:

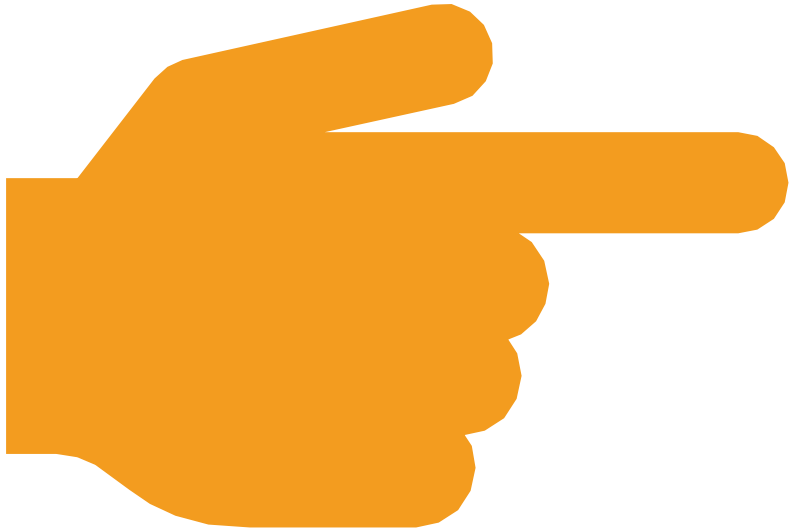
```
request root-cert-chain install scp://ubuntu@192.168.122.84:/home/ubuntu/cert
y/root-ca vpn 512
```

NOTE:

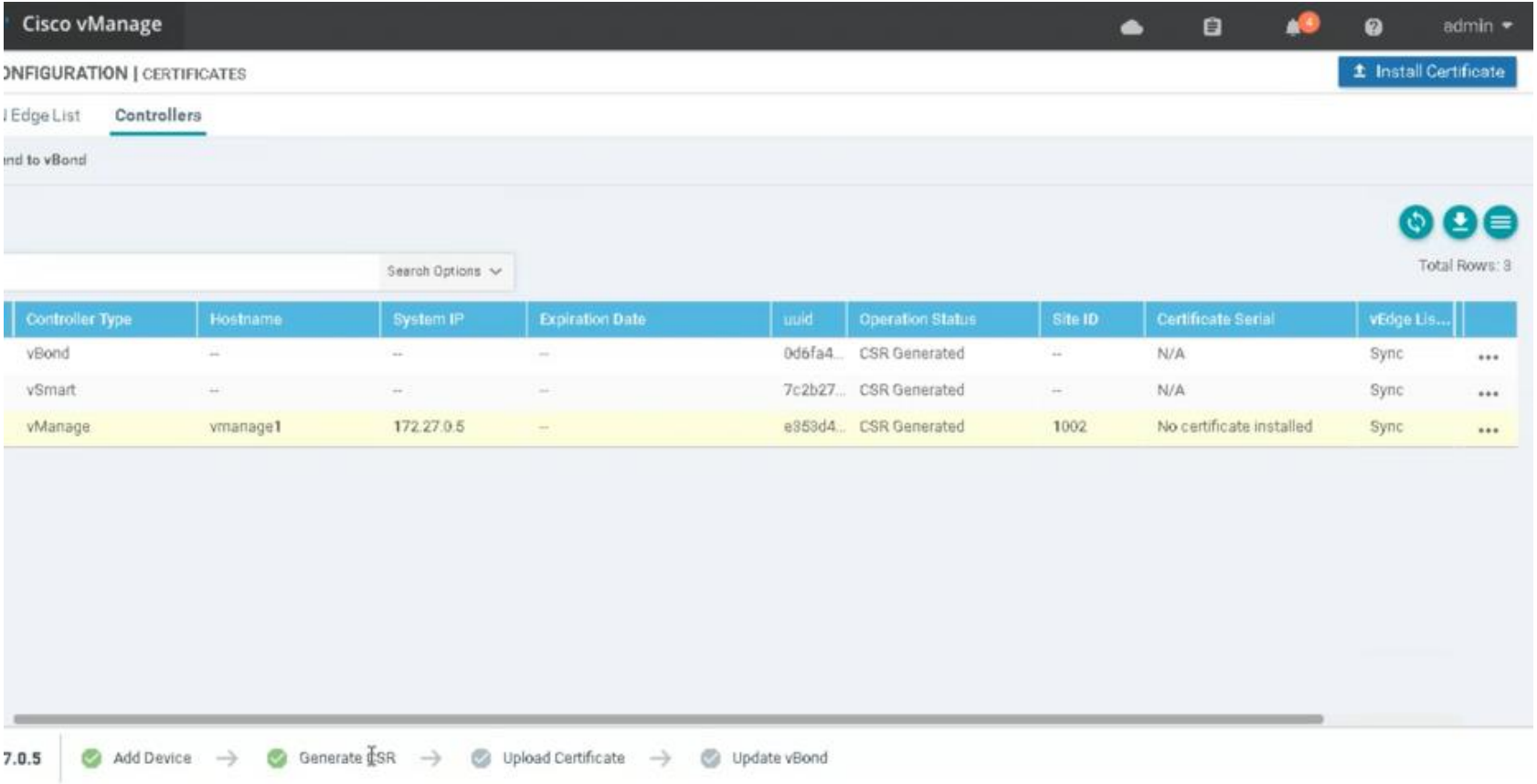
- 192.168.122.84 is the IP address of certify-vm in the lab setup that contains root-ca file
- SCP will prompt for the password to fetch the root-ca file.
  Enter password :

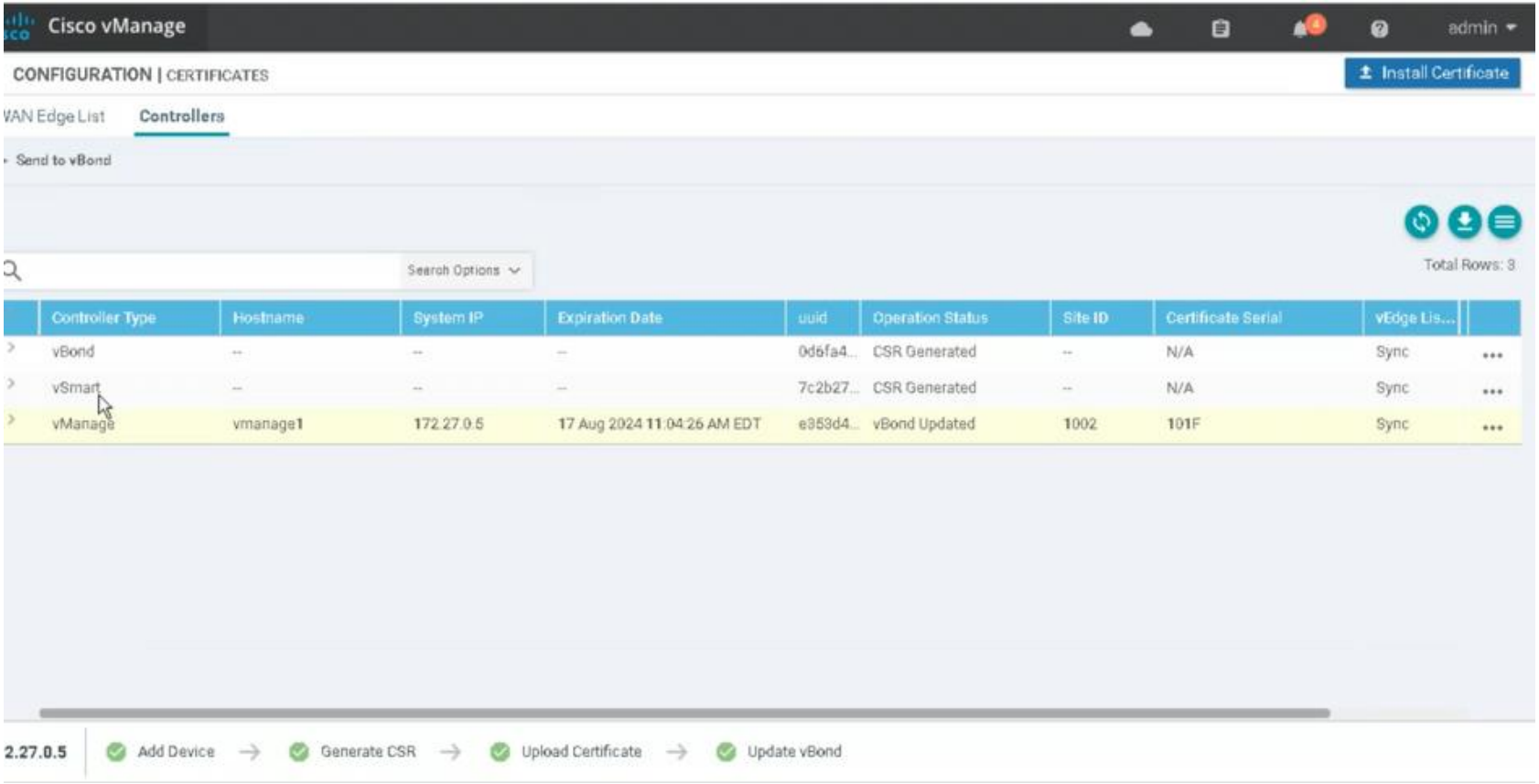
Here is an example for Root Certificate installation on vManage:

```
vManage-1# request root-cert-chain install scp://ubuntu@192.168.122.84:/home/ubuntu/certify/root-ca vpn 512
Uploading root-ca-cert-chain via VPN 512
Copying ... ubuntu@192.168.122.84:/home/ubuntu/certify/root-ca via VPN 512
Warning: Permanently added '192.168.122.84' (ECDSA) to the list of known hosts.
ubuntu@192.168.122.84's password:
root-ca                                       100% 2061   827.5KB/s   00:00
Updating the root certificate chain..
Successfully installed the root certificate chain
```



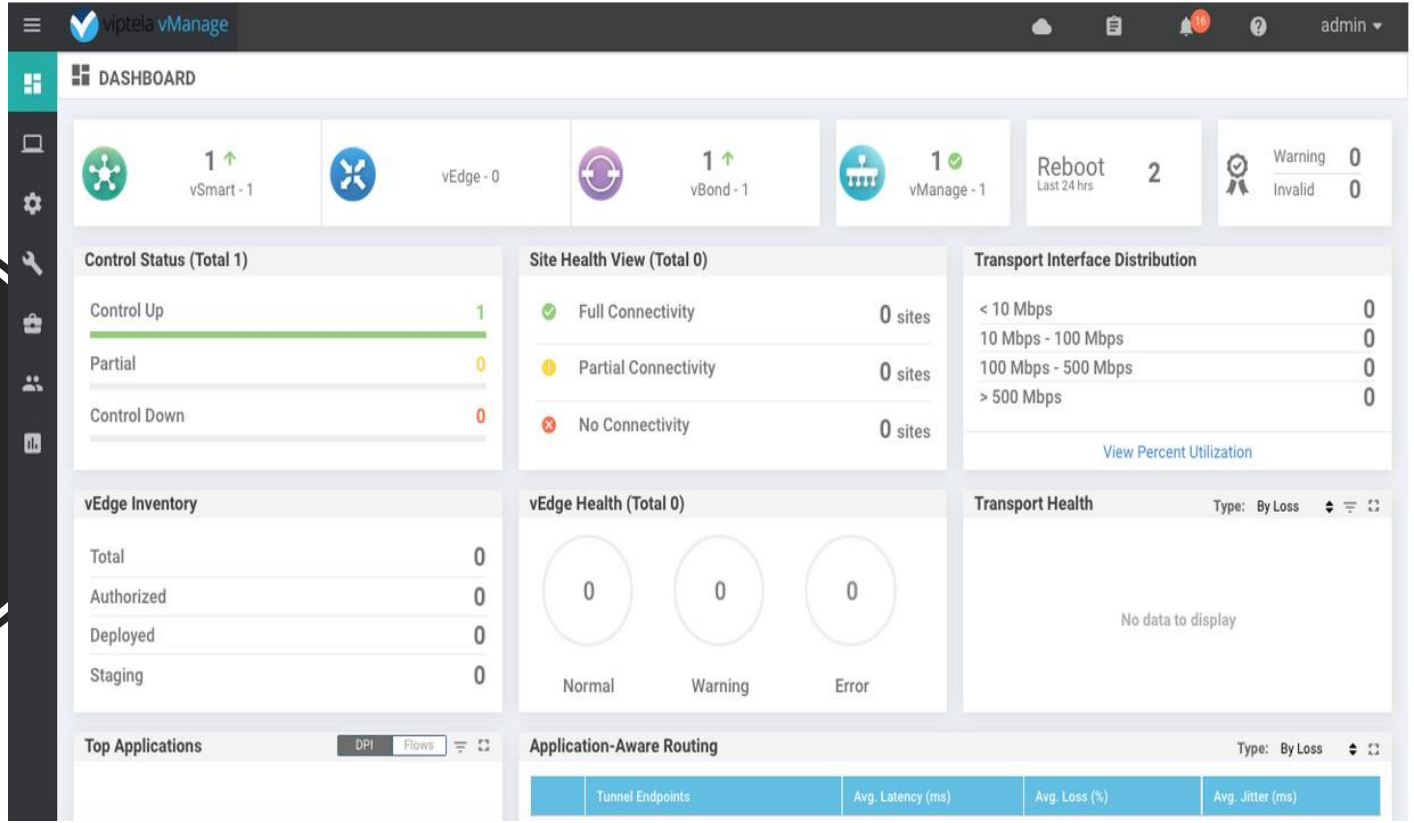
Install PEM to Controller


Cisco vManage
admin
ONFIGURATION | CERTIFICATES
Install Certificate
l Edge List
Controllers
nd to vBond
Search Options
Total Rows: 3
Controller Type
Hostname
System IP
Expiration Date
uuid
Operation Status
Site ID
Certificate Serial
vEdge Lis...
vBond
vSmart
vManage
vmanage1
172.27.0.5
0d6fa4...
7c2b27...
e853d4...
CSR Generated
1002
N/A
No certificate installed
Sync
7.0.5
Add Device
Generate CSR
Upload Certificate
Update vBond


Cisco vManage
admin
CONFIGURATION | CERTIFICATES
Install Certificate
WAN Edge List
Controllers
Send to vBond
Search Options
Total Rows: 3
Controller Type
Hostname
System IP
Expiration Date
uuid
Operation Status
Site ID
Certificate Serial
vEdge Lis...
vBond -- -- -- 0d6fa4... CSR Generated -- N/A Sync
vSmart -- -- -- 7c2b27... CSR Generated -- N/A Sync
vManage vmanage1 172.27.0.5 17 Aug 2024 11:04:26 AM EDT e353d4... vBond Updated 1002 101F Sync
2.27.0.5
Add Device
Generate CSR
Upload Certificate
Update vBond

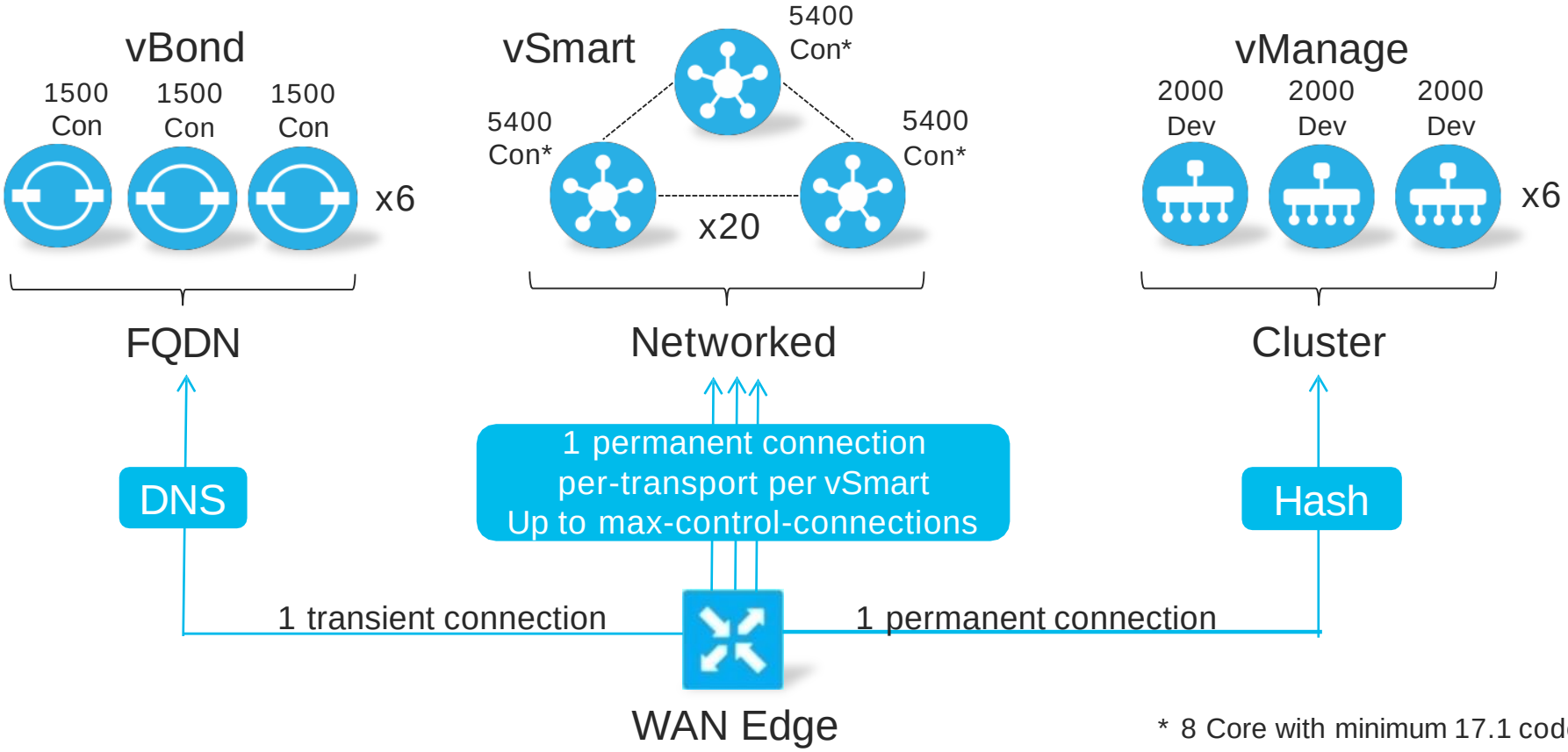
Once Done

End Result!


viptela vManage
admin
DASHBOARD
1
vSmart - 1
vEdge - 0
1
vBond - 1
1
vManage - 1
Reboot
Last 24 hrs
2
Warning 0
Invalid 0
Control Status (Total 1)
Control Up 1
Partial 0
Control Down 0
Site Health View (Total 0)
Full Connectivity 0 sites
Partial Connectivity 0 sites
No Connectivity 0 sites
Transport Interface Distribution
< 10 Mbps 0
10 Mbps - 100 Mbps 0
100 Mbps - 500 Mbps 0
> 500 Mbps 0
View Percent Utilization
vEdge Inventory
Total 0
Authorized 0
Deployed 0
Staging 0
vEdge Health (Total 0)
0
0
0
Normal
Warning
Error
Transport Health
Type: By Loss
No data to display
Top Applications
DPI
Flows
Application-Aware Routing
Type: By Loss
Tunnel Endpoints
Avg. Latency (ms)
Avg. Loss (%)
Avg. Jitter (ms)

2.2.c Scalability and redundancy

Controllers Connectivity and Scale



* 8 Core with minimum 17.1 code

Robust Network Design

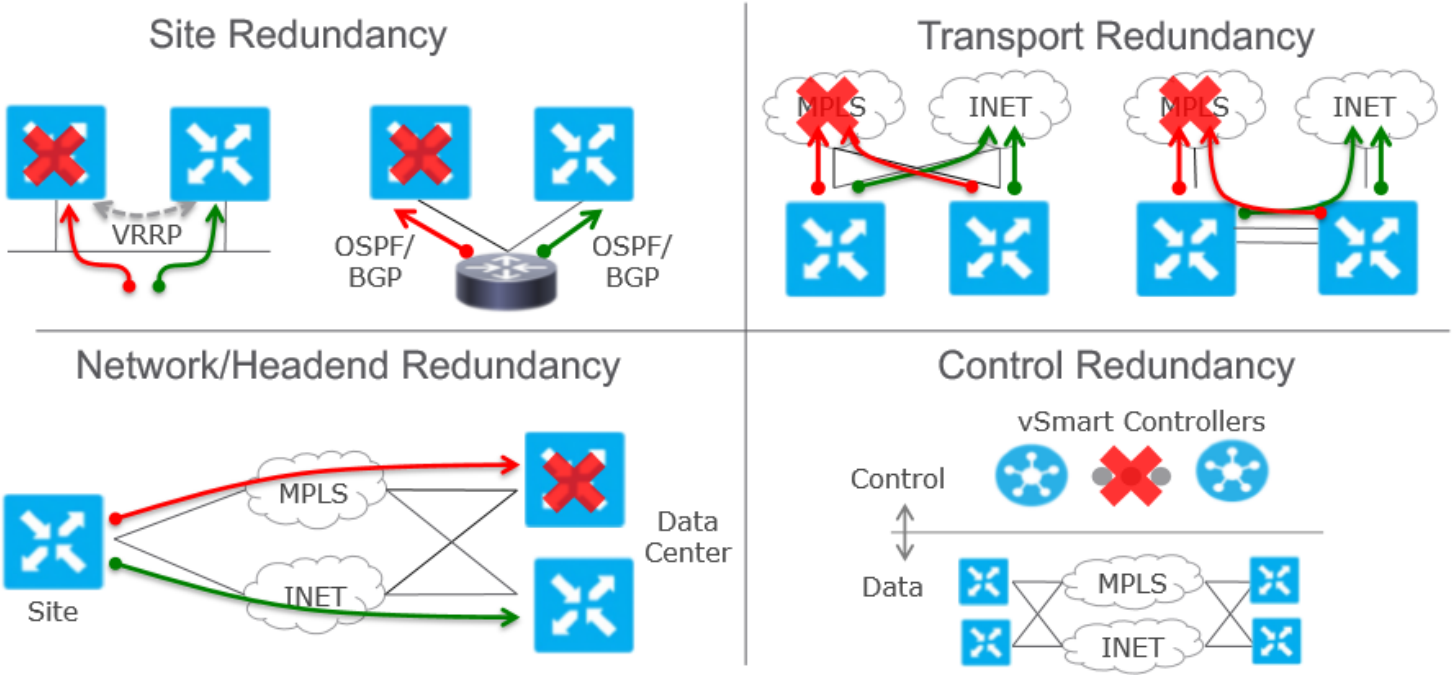
Design practices include situating :

- ❑ Redundant vBond orchestrators
- ❑ Redundant vSmart controllers
- ❑ Redundant vManage Cluster
- ❑ Dispersed geographical locations
- ❑ Connecting them to different transport networks.

Similarly, the vEdge routes at a local site can connect to

- ❑ Different transport networks
- ❑ Can reach these networks through different NATs and DMZs.

Example vEdge Redundancy



Software Support of High Availability

- The Viptela software support for high availability and resiliency in the face of failure is provided both in the control plane, using the

- standard DTLS protocol
- the proprietary Viptela Overlay Management Protocol (OMP)

- And in the data plane, using the industry-standard protocols

- BFD
- BGP
- OSPF
- VRRP

Control Plane Software Support of High Availability

The exchange of control plane information over OMP peering sessions is a key piece in the Viptela high availability solution:

1. **vSmart controllers** quickly and automatically learn when a vBond orchestrator or a vEdge router joins or leaves the network.

2. They can then rapidly make the necessary modifications in the route information that they send to the vEdge routers
3. vSmart controllers learn about the presence of other vSmart controllers, and they all automatically synchronize their route tables.

4. If one vSmart controller fails, the remaining systems take over management of the control plane, simply and automatically, and all vEdge routers in the network continue to receive current, consistent routing and TLOC updates from the remaining vSmart controllers

1. **vBond orchestrators** quickly and automatically learn when a device joins the network and when a vSmart controller leaves the network.

2. They can then rapidly make the necessary changes to the list of vSmart controller IP addresses that they send to vEdge routers joining the network.

3. vBond orchestrators learn when a domain has multiple vSmart controllers and can then provide multiple vSmart controller addresses to vEdge routers joining the network.

Redundancy

vBond Orchestrator Redundancy

vSmart Orchestrator Redundancy

vManage Orchestrator Redundancy

vBond Orchestrator Redundancy

- The vBond orchestrator performs two key functions in the Viptela overlay network:

- Authenticates and validates all vSmart controllers and vEdge routers that attempt to join the Viptela network.

- Orchestrates the control plane connections between the vSmart controllers and the vEdge routers, thus enabling vSmart controllers and vEdge routers to connect to each other in the Viptela network.

Configuration of Redundant vBond Orchestrators

- When the network has two or more vBond orchestrators and they must all be reachable, you should use the name of a DNS server.

- if your Viptela network has only a single vBond orchestrator, it is recommended as a best practice that you **specify a DNS name** rather than an IP address in the system vbond configuration command, because this results in a scalable configuration.

- Then, if you add additional vBond orchestrators to your network, you do not need to change the configurations on any of the vEdge routers or vSmart controllers in your network.

vManage NMS Redundancy

- A highly available Viptela network contains three or more vManage NMSs in each domain.
- This scenario is referred to as a cluster of vManage NMSs, and each vManage NMS in a cluster is referred to as a vManage instance.

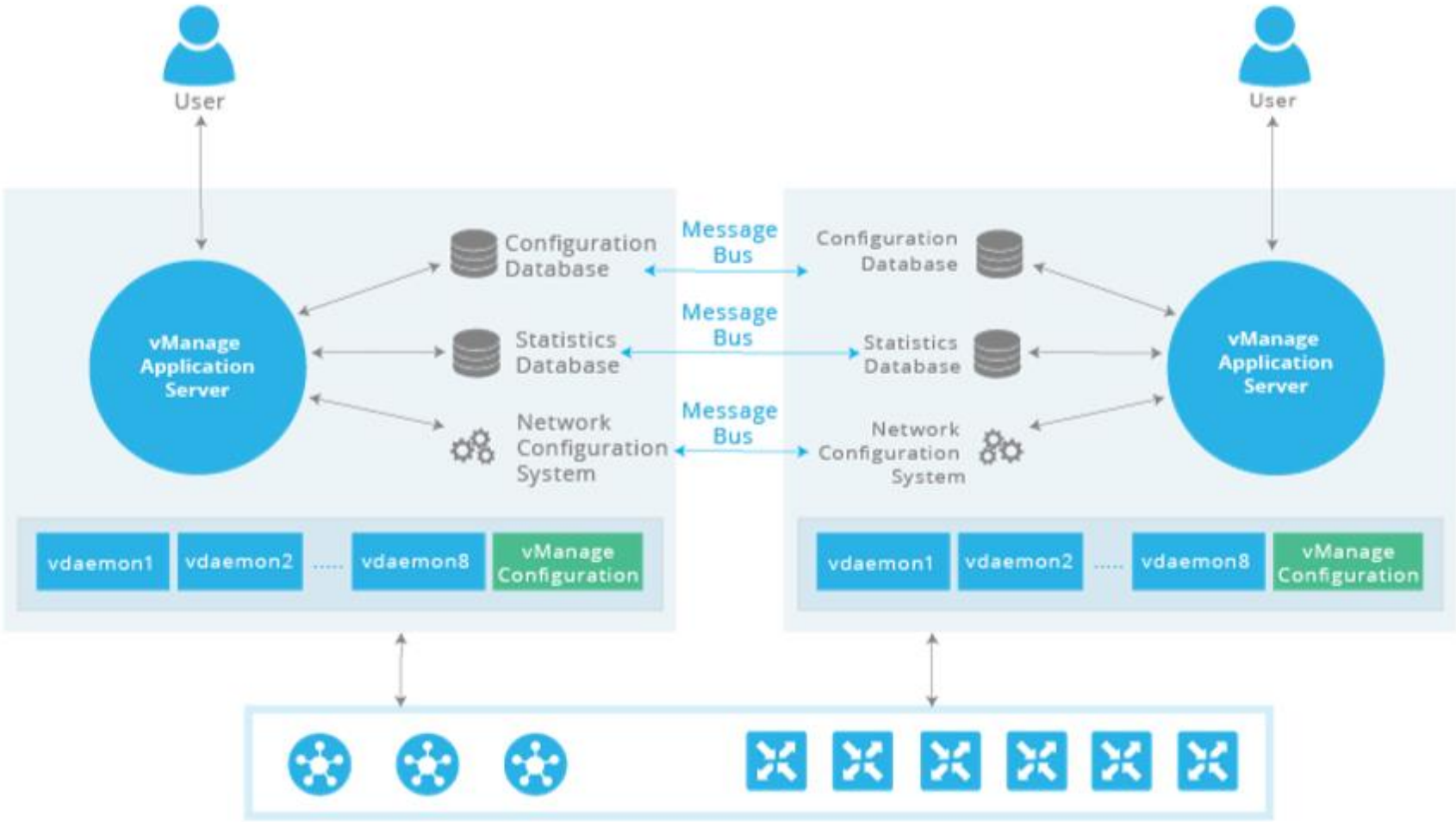
A vManage cluster consists of the following architectural components

- **Application server**—This provides a web server for user sessions. Through these sessions, a logged-in user can view a high-level dashboard summary of networks events and status, and can drill down to view details of these events.
- A user can also manage network serial number files, certificates, software upgrades, device reboots, and configuration of the vManage cluster itself from the vManage application server.
- **Configuration database**—Stores the inventory and state and the configurations for all Viptela devices.

• **Network configuration system**—Provides the mechanism for pushing configurations from the vManage NMS to the Viptela devices and for retrieving the running configurations from these devices.

• **Statistics database**—Stores the statistics information collected from all Viptela devices in the overlay network.

• **Message bus**—Communication bus among the different vManage instances. This bus is used to share data and coordinate operations among the vManage instances in the cluster.


User
User
Configuration Database
Message Bus
Configuration Database
Statistics Database
Message Bus
Statistics Database
vManage Application Server
vManage Application Server
Network Configuration System
Message Bus
Network Configuration System
vdaemon1
vdaemon2
.....
vdaemon8
vManage Configuration
vdaemon1
vdaemon2
.....
vdaemon8
vManage Configuration

Design considerations for a vManage cluster

- A vManage cluster should consist of a minimum of three vManage instances.

- The application server and message bus should run on all vManage instances.

- Within a cluster, a maximum of three instances of the configuration database and three instances of the statistics database can run. Note, however, that any individual vManage instance can run both, one, or none of these two databases.

- To provide the greatest availability, it is recommended that you run the configuration and statistics databases on three vManage instances.

vEdge Router Redundancy

vEdge routers are commonly used in two ways in the Viptela network:

- to be the Viptela routers at a branch site
- to create a hub site that branch vEdge routers connect to.

A branch site can have two vEdge routers in a branch site for redundancy. Each of the router maintains:

- A secure control plane connection, via a DTLS connection, with each vSmart controller in its domain

- A secure data plane connection with the other vEdge routers at the site

Because both vEdge routers receive the same routing information from the vSmart controllers, each one is able to continue to route traffic if one should fail, even if they are connected to different transport providers.

Recovering from a Failure in the Control & Data Plane

Recovering from a vSmart Controller Failure

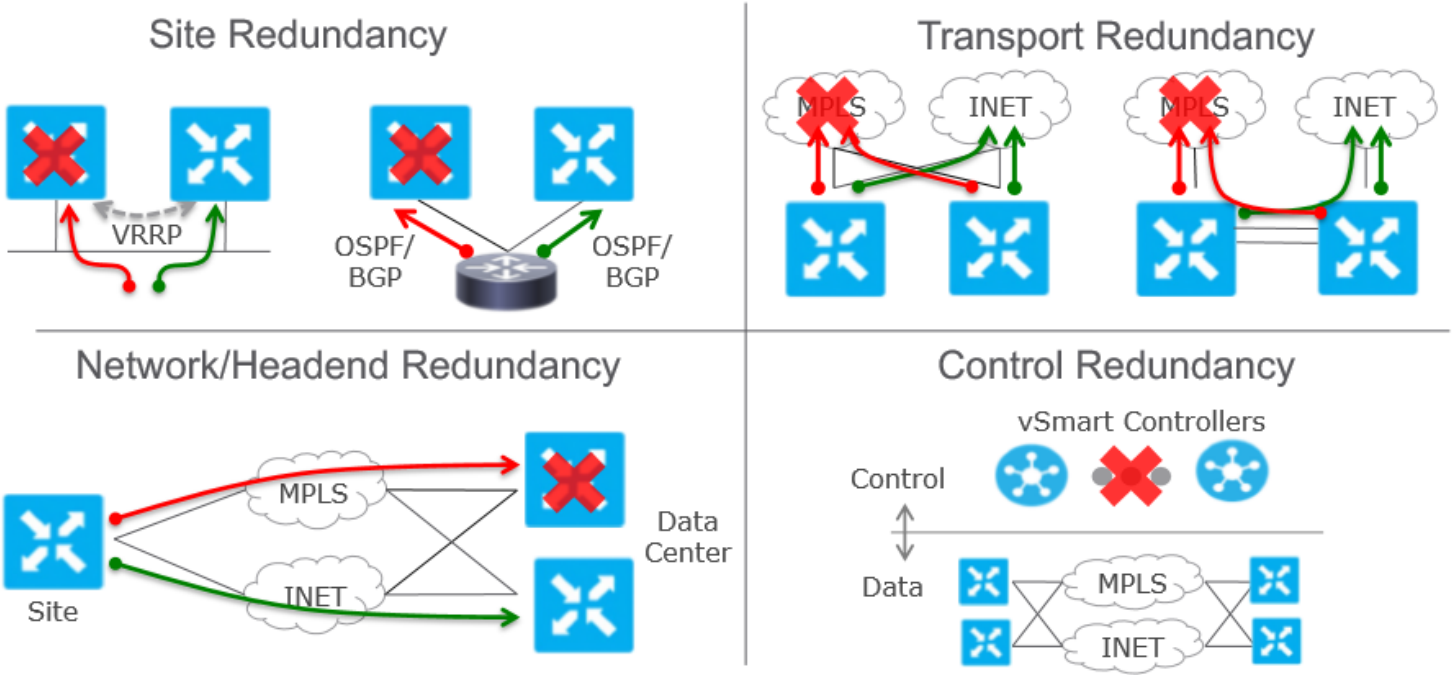
- There is a full mesh of OMP sessions among the vSmart controllers.
- Each vSmart controller has a permanent DTLS connection to each vBond orchestrator.
- The vSmart controllers have permanent DTLS connections to the vEdge routers.
- If one of the vSmart controllers fails, the other vSmart controllers seamlessly take over handling control of the network.

- The remaining vSmart controllers are able to work with vEdge routers joining the network and are able to continue sending route updates to the vEdge routers. **As long as one vSmart** controller is present and operating in the domain, the Viptela network can continue operating without interruption.

Recovering from a vBond Orchestrator Failure

- In a network with multiple vBond orchestrators, if one of them fails, the other vBond orchestrators simply continue operating and are able to handle all requests by Viptela devices to join the network.
- From a control plane point of view, each vBond orchestrator maintains a permanent DTLS connections to each of the vSmart controllers in the network.
- As long as one vBond orchestrator is present in the domain, the Viptela network is able to continue operating without interruption, because vSmart controllers and vEdge routers are still able to locate each other and join the network.
- Because vBond orchestrators never participate in the data plane of the overlay network, the failure of any vBond orchestrator has no impact on data traffic.

Recovering from a vEdge Router Failure



Data Plane Software Support for High Availability

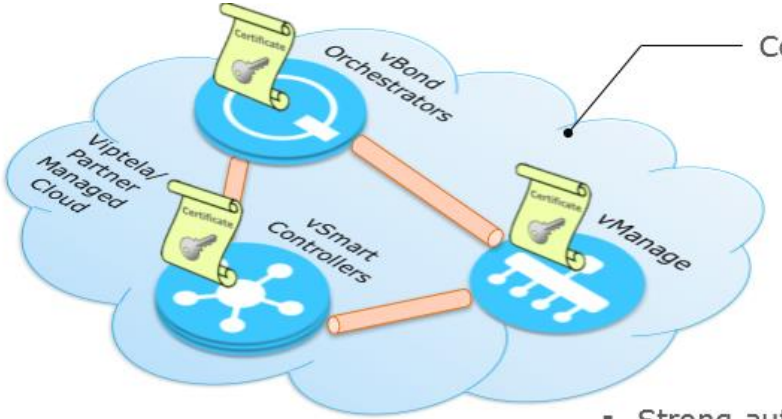
- For data plane resiliency, the Viptela software implements the standard BFD protocol, which runs automatically on the secure IPsec connections between vEdge routers.
- BFD is used to detect connection failures between the routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection. BFD is enabled, by default .

- BFD sends Hello packets periodically (by default, every 1 second) to determine whether the session is still operational. If a certain number of the Hello packets are not received, BFD considers that the link has failed and brings the BFD session down (the default dead time is 3 seconds).

- When a BFD sessions goes down, any route that points to a next hop over that IPsec tunnel is removed from the forwarding table (FIB), but it is still present in the route table (RIB)

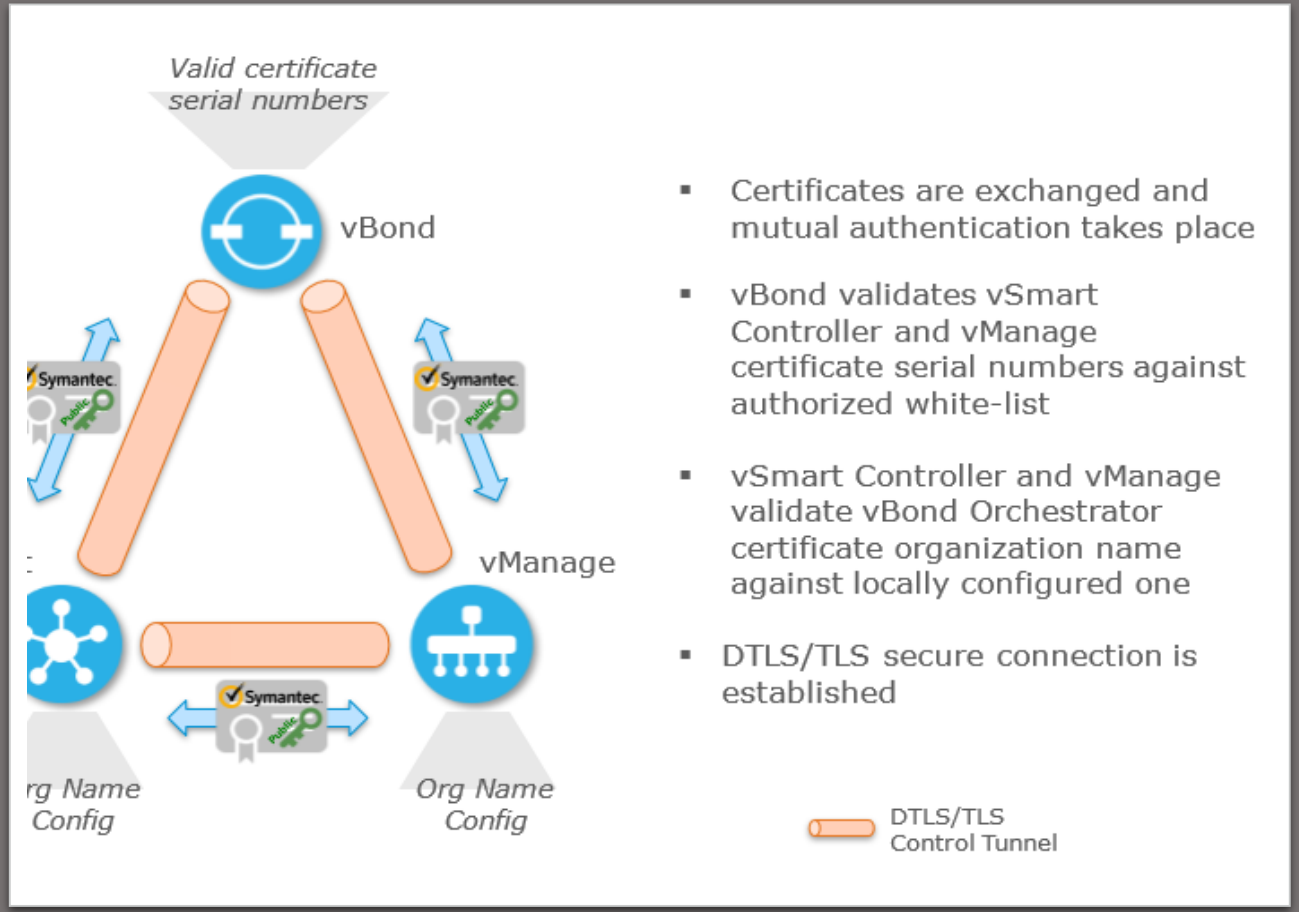
2.3 Configure and verify certificates and whitelisting

Virtual Fabric Bringup



- Strong authentication
  - PKI certificates, 2048bit keys
- Highly secure connections
  - DTLS/TLS AES256
  - White-list model

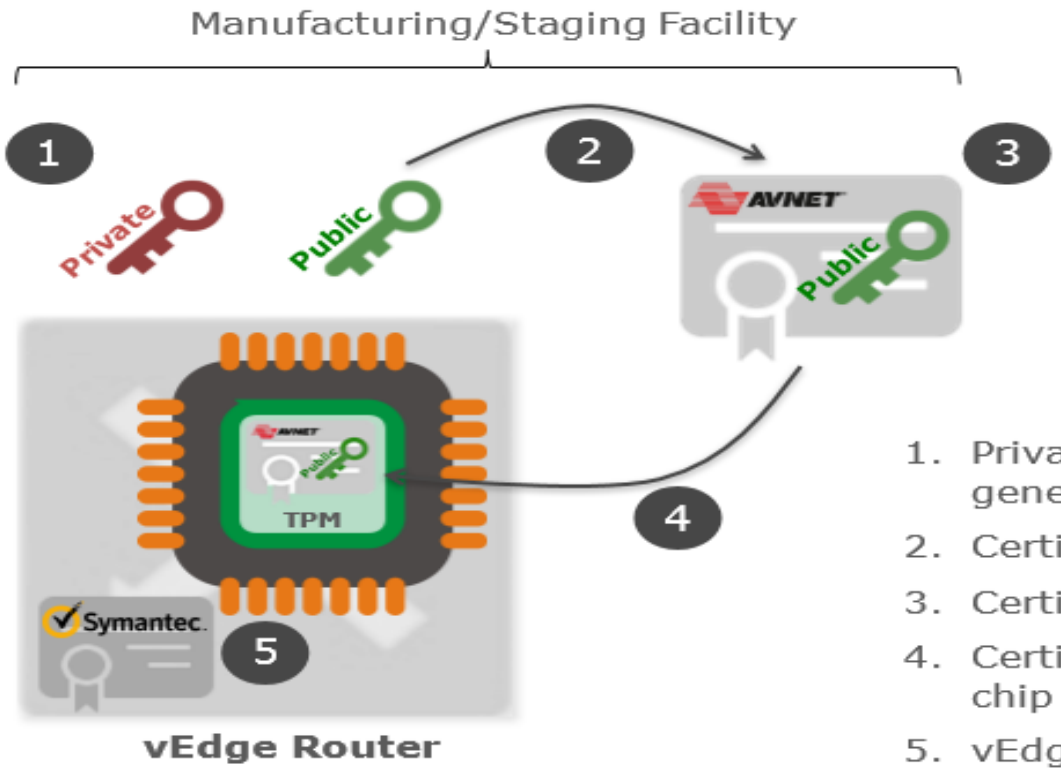
DTLS/TLS Control Tunnel



- Certificates are exchanged and mutual authentication takes place
- vBond validates vSmart Controller and vManage certificate serial numbers against authorized white-list
- vSmart Controller and vManage validate vBond Orchestrator certificate organization name against locally configured one
- DTLS/TLS secure connection is established

Secure Control Channel: Control Elements

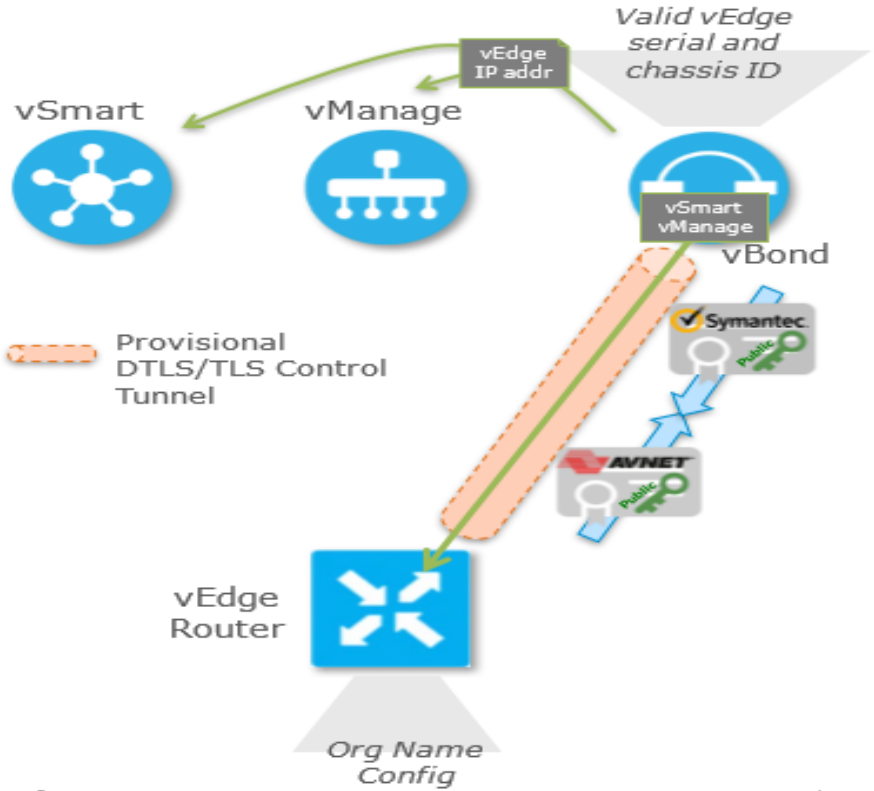
Establish vEdge Router Identity



Note: Can use Enterprise CA

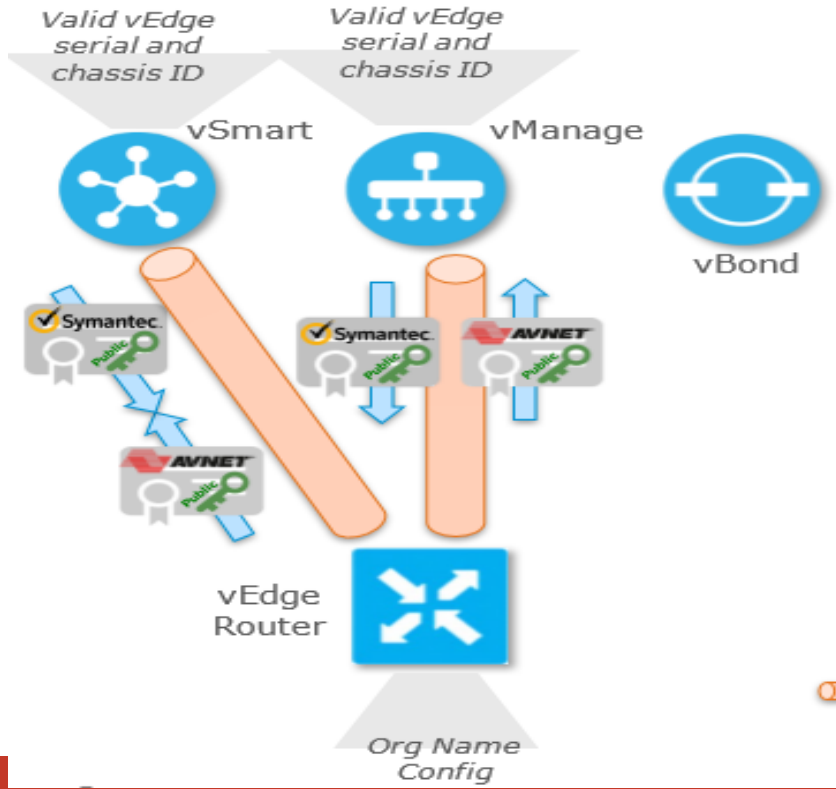
1. Private and public keys are generated on the vEdge router
2. Certificate is generated
3. Certificate is signed by Avnet
4. Certificate is loaded into TPM-lite chip on the vEdge router
5. vEdge router has a root CA trust chain for Symantec Root CA

Secure Control Channel: vEdge Routers Connection to vBond Orchestrator



- Certificates are exchanged and mutual authentication takes place between vBond and vEdge
  - Over encrypted tunnel
- vBond validates vEdge Router serial number and chassis ID against authorized vEdge white-list
- vEdge Router validates vBond certificate organization name against locally configured one
- Provisional DTLS/TLS tunnel is established between vBond and vEdge
- vBond returns to vEdge a list of vSmart Controllers and vManage
- vBond notifies vSmart and vManage of vEdge Router public IP address
- Provisional DTLS/TLS tunnel between vBond and vEdge is terminated

Secure Control Channel: vEdge Routers Connection to vSmart Controller and vManage



- Certificates are exchanged and mutual authentication takes place between vSmart, vManage and vEdge
- vSmart and vManage validate vEdge Router serial number and chassis ID against authorized vEdge white-list
- vEdge Router validates vSmart and vManage certificate organization name against locally configured one
- Permanent DTLS/TLS tunnel between vSmart, vManage and vEdge is established

Permanent DTLS/TLS Control Tunnel

```
vsmart# show control connections

      PEER    PEER PEER            SITE       DOMAIN PEER

INDEX TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP
E           UPTIME
-------------------------------------------------------------------------------------------
-----------------------
0     vedge   dtls 10.1.0.1        100        1      172.16.10.2
            0:13:53:56
0     vedge   dtls 10.1.0.1        100        1      172.16.11.2
            0:13:54:20
0     vedge   dtls 10.1.0.2        100        1      172.16.12.2
            0:13:53:50
0     vedge   dtls 10.1.0.2        100        1      172.16.13.2
            0:13:54:27
0     vedge   dtls 10.2.0.1        200        1      172.16.20.2
            0:13:53:53
0     vedge   dtls 10.2.0.1        200        1      172.16.21.2
            0:13:53:53
0     vedge   dtls 10.3.0.2        300        1      10.10.10.2
            0:13:58:16
0     vedge   dtls 10.3.0.2        300        1      100.64.3.2
            0:13:58:18
0     vedge   dtls 10.3.0.1        300        1      10.20.20.2
            0:13:58:14
0     vedge   dtls 10.3.0.1        300        1      172.16.3.2
            0:13:58:15
0     vedge   dtls 10.4.0.1        400        1      100.64.4.2
```

Verification

2.4 Troubleshoot control-plane connectivity between controllers

3.0 Router Deployment 20 %