Deploying and configuring OMIVV in a dual-NIC environment

Isolating vSphere management and out-of-band networks for enhanced security.

Abstract

Starting from version 5.0, OMIVV supports dual-NIC environment. This document outlines the scenarios where dual-NIC capabilities of OMIVV can be used, and how to configure it.

April 2020

Revisions

Date	Description
April 2020	Initial release

Acknowledgments

DELLEMC

Contents

Terminology

The following table lists the terminology and acronyms that are used in this document:

Term	Description
OMIVV	OpenManage Integration for VMware vCenter
iDRAC	Integrated Dell Remote Access Controller
VM	Virtual Machine
CMC	Chassis Management Controller
OME-M	OpenManage Enterprise–Modular
NIC	Network Interface Card
LAN	Local Area Network
VLAN	Virtual Local Area Network
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
OOB	Out-of-Band
MAC Address	Media Access Control Address
CIDR	Classless Inter-Domain Routing
DRS	Distributed Resource Scheduler
vSAN	Virtual Storage Area Network
vSphere Management Network	A network which is intended for vSphere management and has access to vSphere components such as vCenter and ESXi.
Out-of-Band Network	An isolated network where the iDRAC, or, CMC, or OME-M components are connected to.

Lightning symbol in the diagram indicates that the two devices have connectivity to each other, either within the same network or with multiple hops.

DELLEMC

Executive summary

In the current scenario, vSphere management network and out-of-band networks are expected to have interconnectivity. As security threats are increasing every day, there is a raising risk of somebody using these exploits to gain unauthorized access. To reduce impact to businesses because of such cyberattacks, starting from version 5.0, OpenManage Integration for VMware vCenter (OMIVV) supports dual-NIC environment to support customers who have implemented isolated networks for vCenter management and out-of-band networks.

This technical white paper describes the possible dual-NIC scenarios, dual-NIC capability of OMIVV, and how to configure dual-NIC.

DELLEMC

1 Introduction

The OMIVV is designed to streamline the management processes in data center environment by allowing you to use VMware vCenter server to manage full server infrastructure—both physical and virtual. From monitoring system level information, showing system alerts for action in vCenter, updating firmware for an ESXi or vSAN cluster without impacting the workload to bare-metal deployment, the OMIVV will expand and enrich VMware management experience with Dell EMC PowerEdge servers.

Earlier with the single-NIC configuration in OMIVV, vSphere (vCenter and ESXi) and iDRAC were supposed to be in the same network or to be routed without isolation.

Starting from version 5.0, OMIVV supports two isolated networks.

1.1 Audience

This technical white paper is intended for server administrators and network administrators for managing VMware virtualization solutions in their data centers running on Dell EMC PowerEdge servers and using OMIVV for systems management requirements.

1.2 Applicable scenario to configure dual-NIC

In data center environment, if the in-band management network and out-of-band management networks have route to communicate with each other, you should continue to have single network interface to OMIVV. The scenarios that is explained in the subsequent section are applicable if the in-band management network and out-of-band management networks cannot communicate to each other.

Figure 1 describes a typical scenario where out-of-band management network is isolated and does not have route to the in-band management network. In this case, OMIVV is configured with two network interfaces, and has connectivity with both the networks.
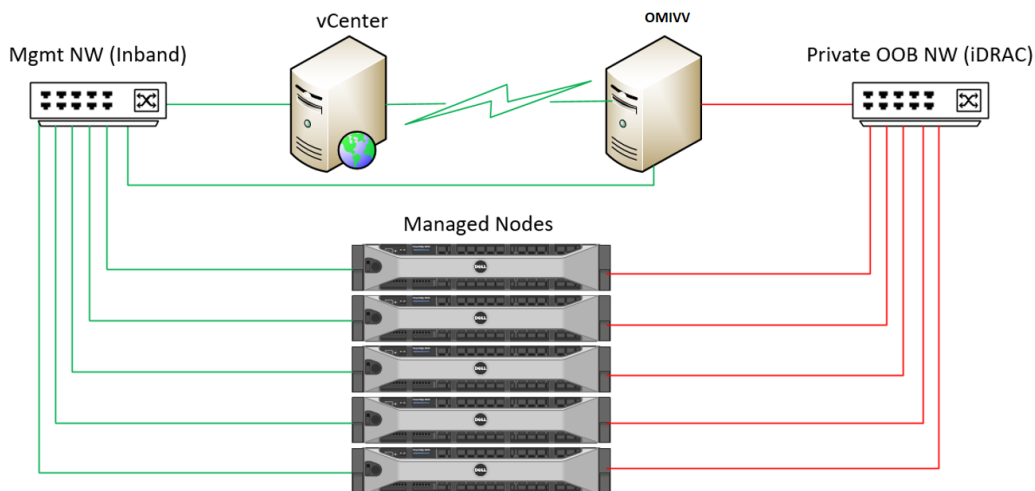

Figure 1: Isolated out-of-band management network

1.3   Possible Multi-NIC configuration

The following are the different ways to configure dual-NIC in data center environment:

1. Two isolated sets of vCenter and associated hosts, each having separate vSphere management and out-of-band networks with network accessibility internally, and OMIVV has common access to both the setups.
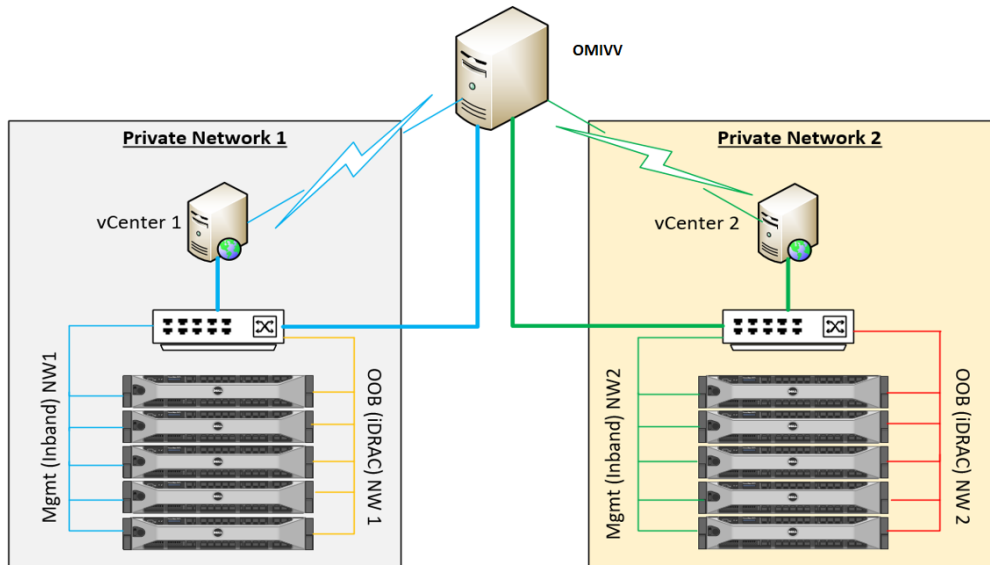

Figure 2: Two isolated sets of vCenters and associated hosts having separate vSphere management and out-of-band networks

DELLEMC

2. Two different isolated vSphere networks and one common out-of-band private network to manage the servers and chassis. OMIVV has access to all three different isolated networks.
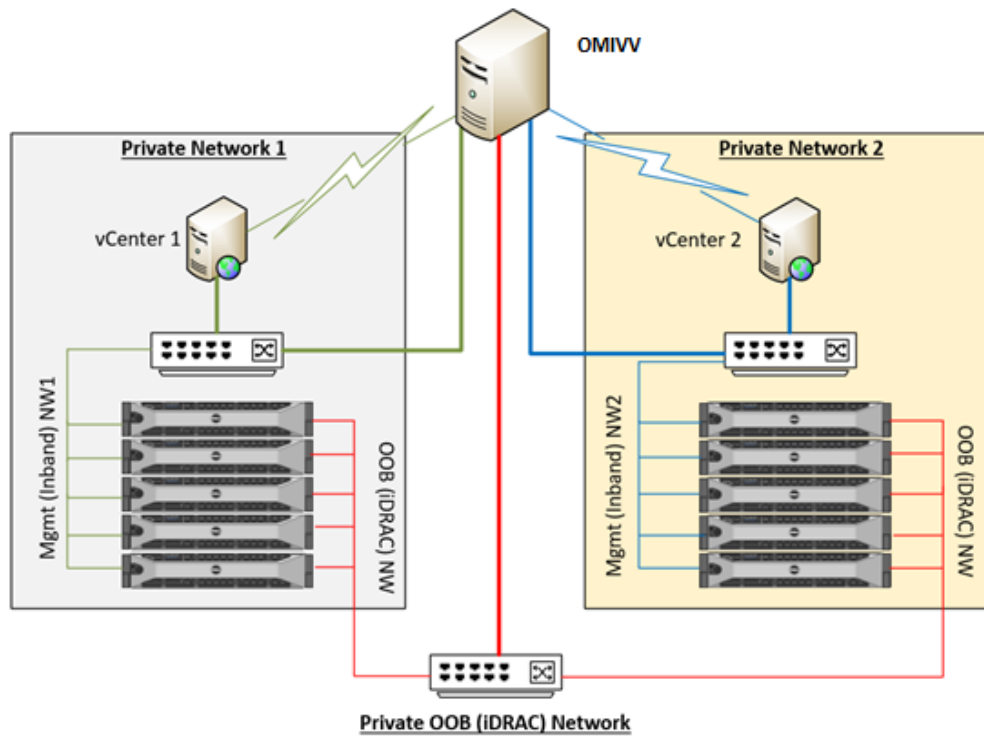

Figure 3: Two different isolated vSphere networks and one common out-of-band network

3. One common vSphere network and different out-of-band private networks to manage the servers and chassis. OMIVV has access to all three different isolated networks.
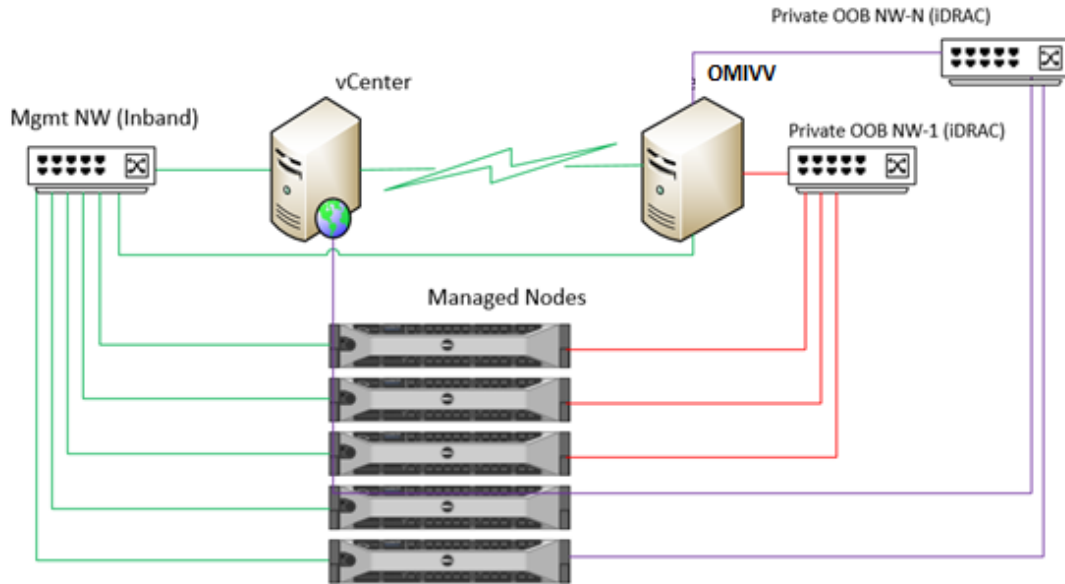

Figure 4: One common vSphere network and different out-of-band private networks

4. One common vSphere and out-of-band private networks to manage the servers and chassis and another network explicitly to have access to Internet.
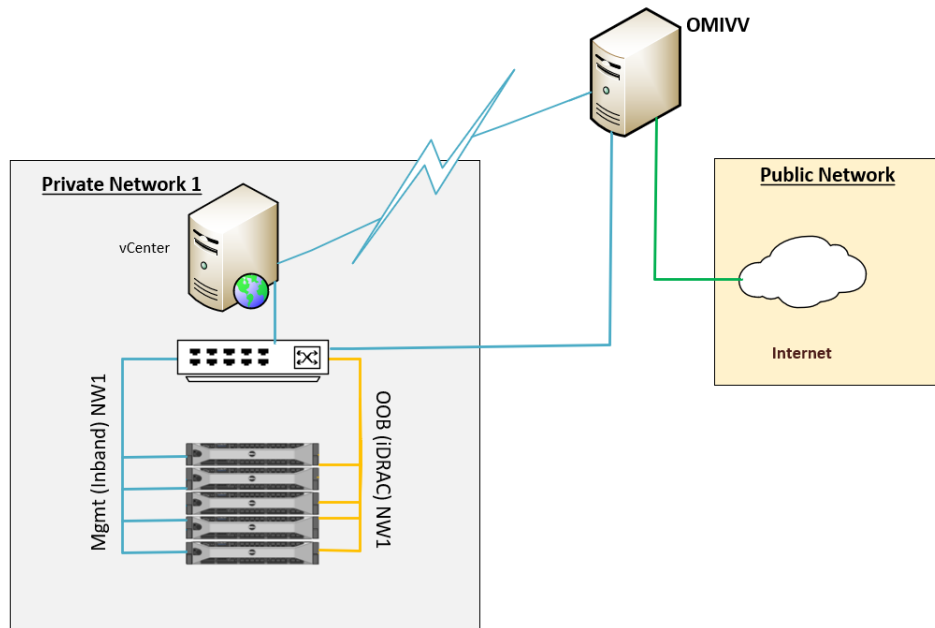

Figure 5: One common vSphere and out-of-band networks

D&LLEMC

2 Configure dual-NIC in OMIVV

This section describes how to configure dual-NIC in OMIVV, along with the steps for configuring DNS forwarding as needed.

Ensure that the OMIVV appliance is imported, deployed, and not powered on for new installation.

Note: Any network configuration is done to the OMIVV appliance when the appliance is up and running will not be reflected in the application until the VM is rebooted.

1. Edit the VM settings using the vSphere Client (HTML-5) and add the additional NIC. To edit the VM settings, right-click VM, and then click **Edit Settings**.
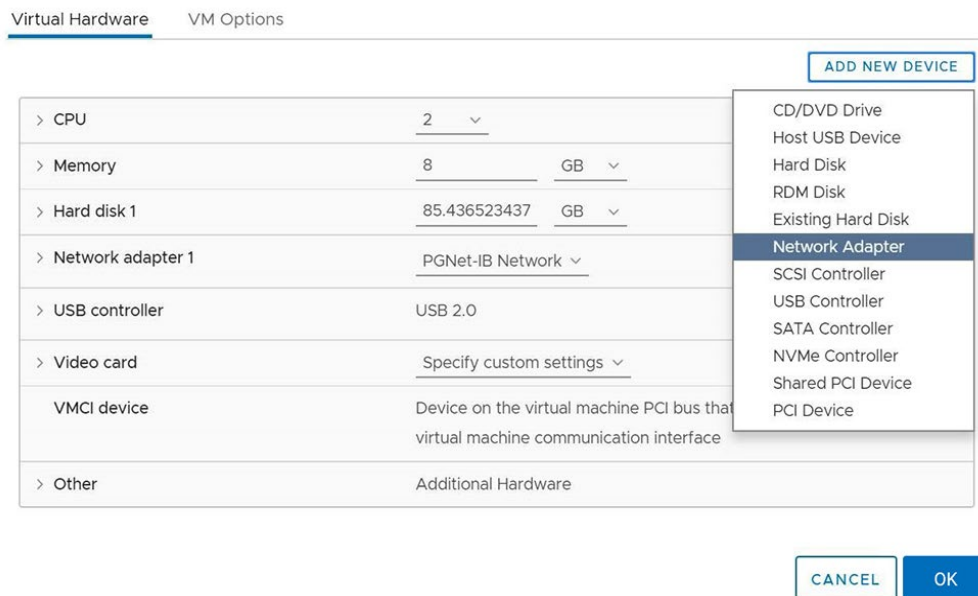2. Click **ADD NEW DEVICE** and select **Network Adapter**.

Figure 6: Select Network Adapter

    a. Select the appropriate network for the NIC, and then select the **Connect At Power On** check box.

    b. Select the **E1000/VMXNET3** adapter type from the **Adapter Type** drop-down menu. OMIVV 5.0 supports only E1000 type of NIC.

DELLEMC
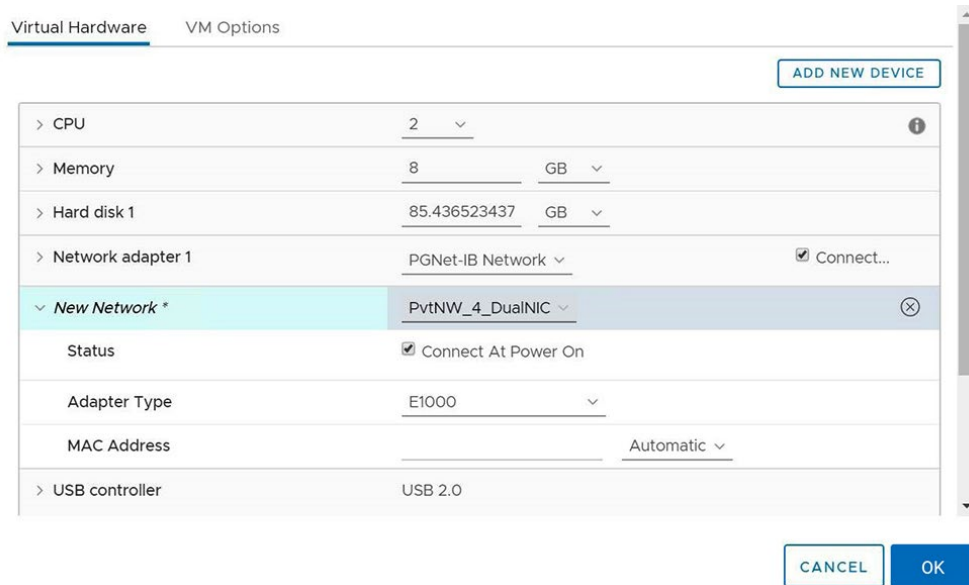
Figure 7: Select network and adapter type

3. Click **OK** to save the configuration.
4. Power on the VM. Log in as admin and provide the password for Administration console.
5. On the **Open Manage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Network Configuration**.
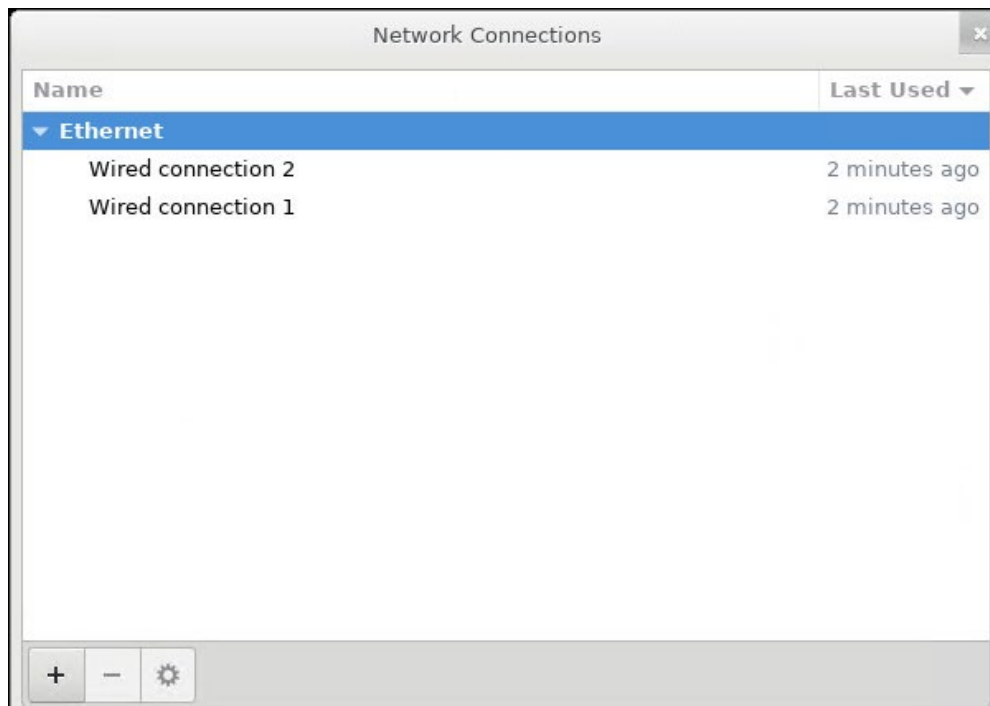   The **Network Connections** page displays two NICs.

Figure 8: Available network connections

6. Select the NIC that you want to configure and click.

7. To identify the correct NIC, use the MAC ID displayed on the **Ethernet** tab, and then compare it against the MAC ID displayed in the vSphere Client. Ensure that you do not change the default MAC address that is listed in the **Ethernet** tab.
8. Go to **General** tab and ensure that the check box against **Automatically connect to this network when it is available** is selected.
9. Click the **IPv4 Settings** tab, and do the following:

   a. Select **Manual** or **Automatic (DHCP)** from the **Method** drop-down list.
   b. If you select the **Manual** method, click **Add**, and then enter the valid IP address, Netmask (in the CIDR format), and gateway details.

      It is recommended to use the static IP in case if you want to control over the priority of the DNS servers (primary and secondary DNS entries).

      Note: It is recommended you to configure the DNS settings corresponding to the vSphere management network for seamless operations.

      Note: CentOS consumes the last configured DNS server as the primary DNS irrespective of which network the DNS is configured for.

   c. Enter the DNS server IP and domains to be searched for in the **DNS Servers** and **Search Domains** fields respectively.
   d. Select the **Require IPV4 addressing for this connection to complete** check box.

Figure 9: IPv4 Settings

e. You must restrict the appliance to have only one default gateway. If the network interface you are configuring is out-of-band network, click **Routes**, and then select the **Use this connection only for resources on its network** check box.

   Note: Adding multiple networks as default gateways may result in network issues, and OMIVV functionalities may get affected.

f. If you want to reach to any external network using the known gateways, click **Add** on the same page, and then add the network IP address, netmask (in the CIDR format), and gateway details for a new static route.
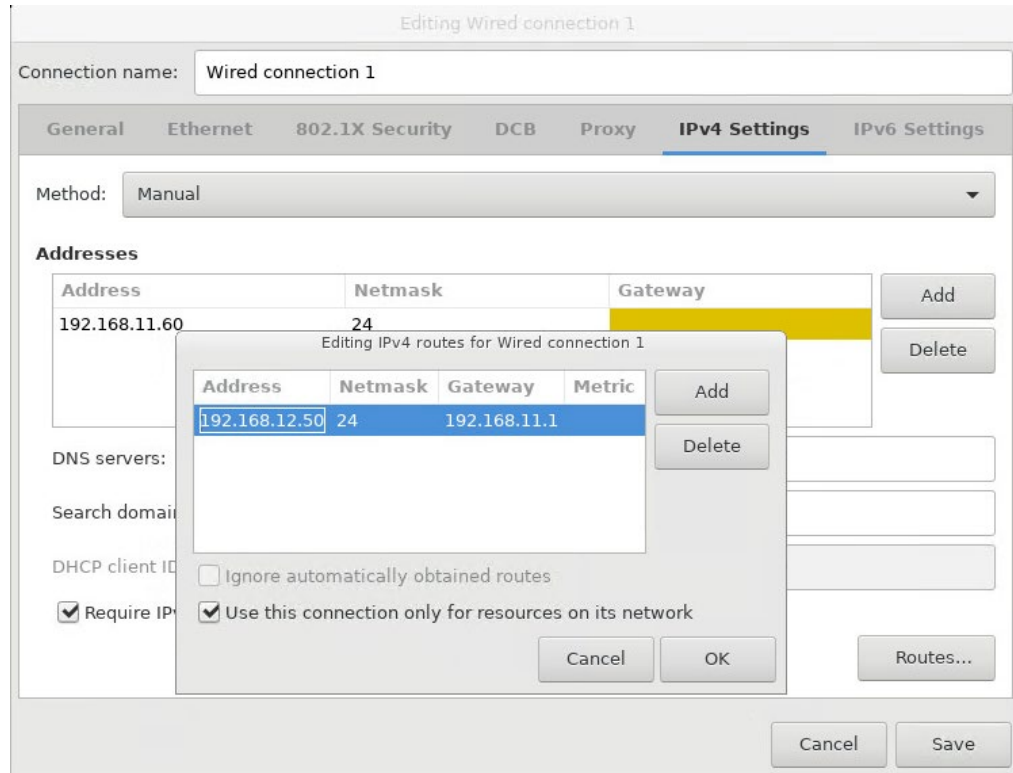

Figure 10: Configure routes

Typically, the network that you have configured as the default gateway does not require any manual route configuration because the gateway can provide the reachability.
However, for networks where default gateway is not configured (the **Use this connection only for resources on its network** check box is selected to restrict connections only to the local network), a manual route configuration may be required because the default gateway is not configured for this network to reach external networks, manual routing configurations are required.
Note: Incorrect routing configuration may abruptly stop the network interface from responding. Ensure to configure the routing entries appropriately.

g. Click **OK**.

10. Click **Save**.
11. To configure another NIC, repeat the tasks 7—11.
12. Go to the **Open Manage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Reboot Appliance**. The network configuration is complete only after restarting the OMIVV appliance.

Note: After the appliance is successfully restarted, the NICs start working as configured.

DELLEMC

The status of NICs can be viewed by logging in as **readonly** user and running the following commands: *ifconfig*, *ping*, and *route -n* or by logging in to admin portal of the appliance as shown below.
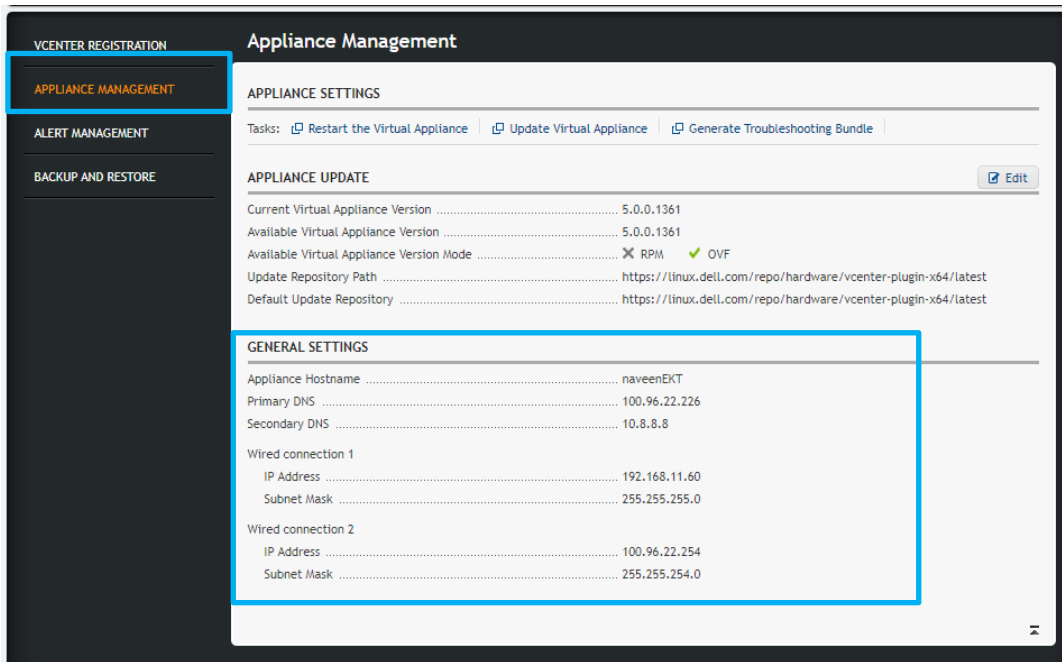

Figure 11: The status of the NICs in Admin portal

2.1 Configure dual-NIC with multiple subnets

The following section describes the dual-NIC with Multi-Subnets configuration.

The following image is an example where the OMIVV appliance is connected with two different isolated networks with multiple subnets for out-of-band network. The vSphere network is configured with DHCP server where the IP and DNS information are provided by the DHCP server whereas the out-of-band network is configured with static IP, which also has multiple subnetworks.
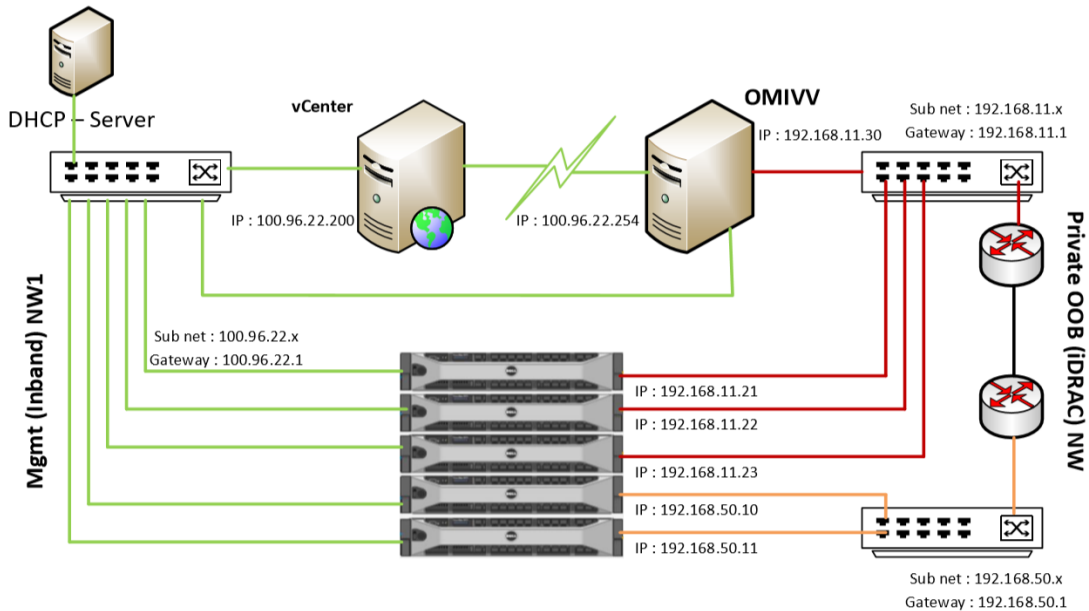

Figure 12: Dual-NIC configuration with multiple subnets

Figure 13: Routing table and manual IP configuration with IP, netmask and gateway

Here the default gateway is assigned to 100.96.22.1. Any packets sent to 192.168.11.0 will be sent to gateway 192.168.11.1 and any packets sent to 100.96.22.0 or any other will be forwarded gateway 100.96.22.1.

However, packets to be sent to 192.168.50.x subnet of private network will be forwarded to default gateway which is 100.96.22.1 due to which the packets are sent to wrong destination or dropped as there is no destination host in vSphere network.

To avoid this issue we need to configire the routes in the network configuration tab by providing subnet, mask, and its gateway to pass the packets as shown in the following images:
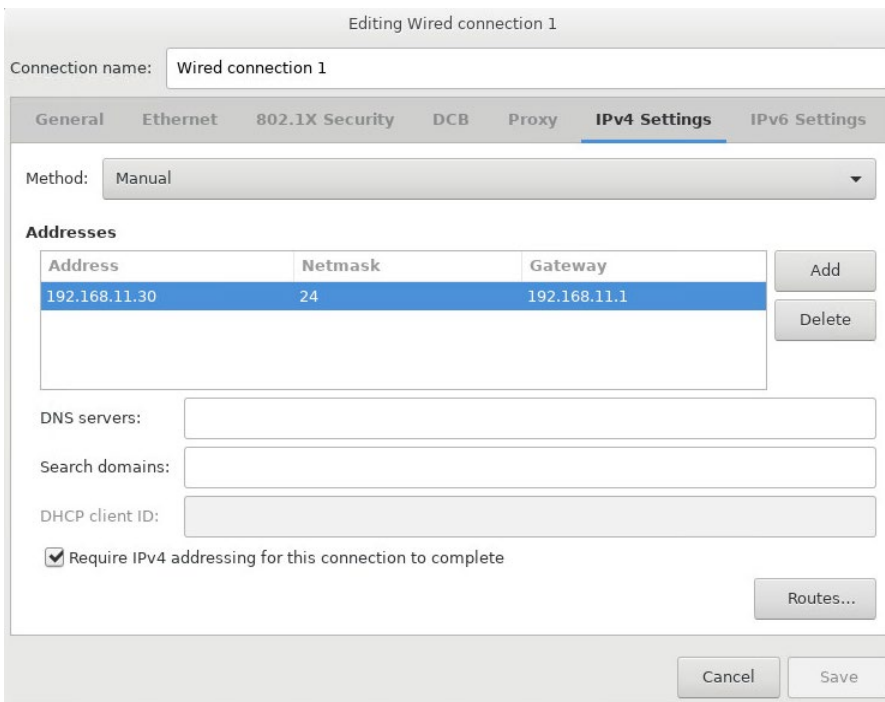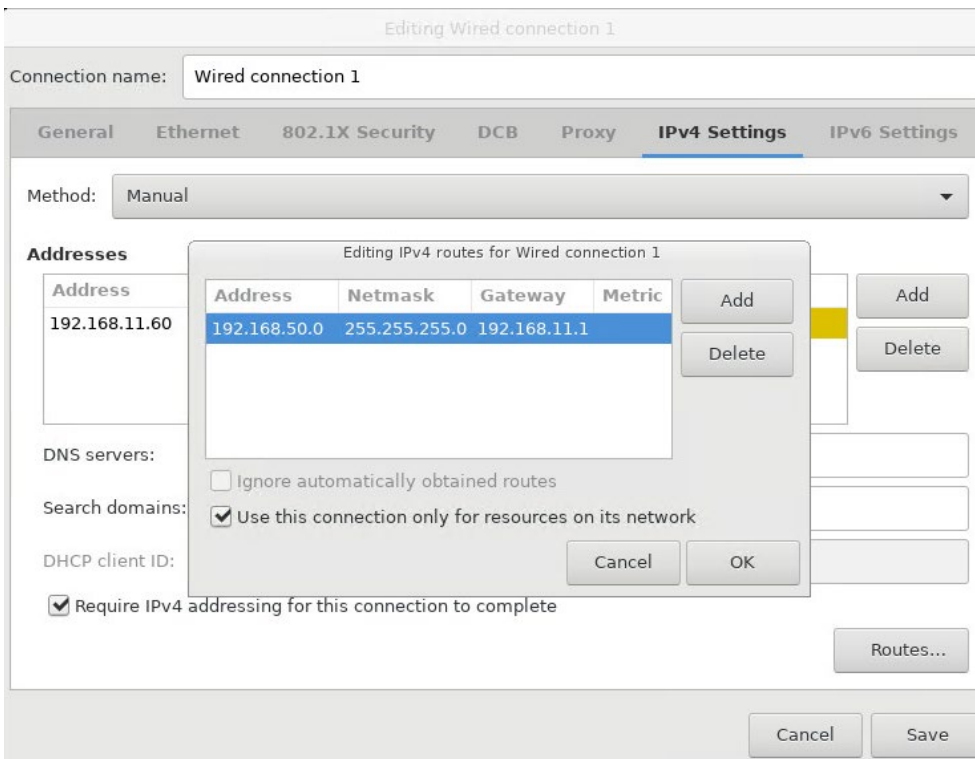
DELLEMC

Figure 14: Configure routes

Figure 15: Configure routes

Any data from OMIVV to subnet 192.168.50.x and 192.168.11.x will be sent via gateway 192.168.11.1 [shown in the following image].

Figure 16: Routing table

2.2 Configure dual-NIC managed with FQDN on both the network with different DNS

This section describes the dual-NIC configuration, where both vSphere and out-of-band are managed by FQDN using IP. However, CentOS allows you to configure maximum three DNS server primary, secondary, and ternary. The CentOS reaches the second DNS server, only when the first DNS server is down or and not reachable and the same applies to third DNS server.

In general, DNS server will send some invalid default IP when it cannot resolve the FQDN. In such cases, OMIVV will consider it as FQDN resolved IP and try to process the invalid IP.

To avoid such problems and continue managing with FQDN from different isolated networks, there must be a common DNS sever which is configured to synchronize with the DNS servers from both vSphere management and Out of Band management networks.

This can be done by configuring the forwarder DNS server of both, so that, when the DNS is not able to resolve the FQDN it forwards the request to the forwarder DNS server and try to get the actual IP.
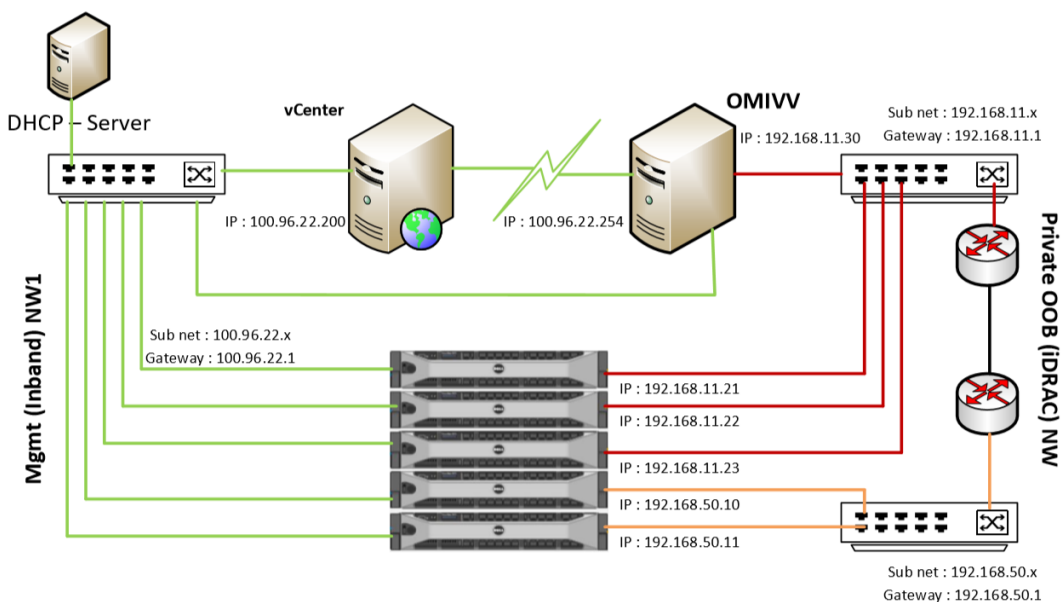
Figure 17: Dual-NIC configuration, where both vSphere and out-of-band are managed by FQDN using IP

DELLEMC

2.2.1   Configure DNS forwarder

1. Right-click DNS server and click **Properties**.
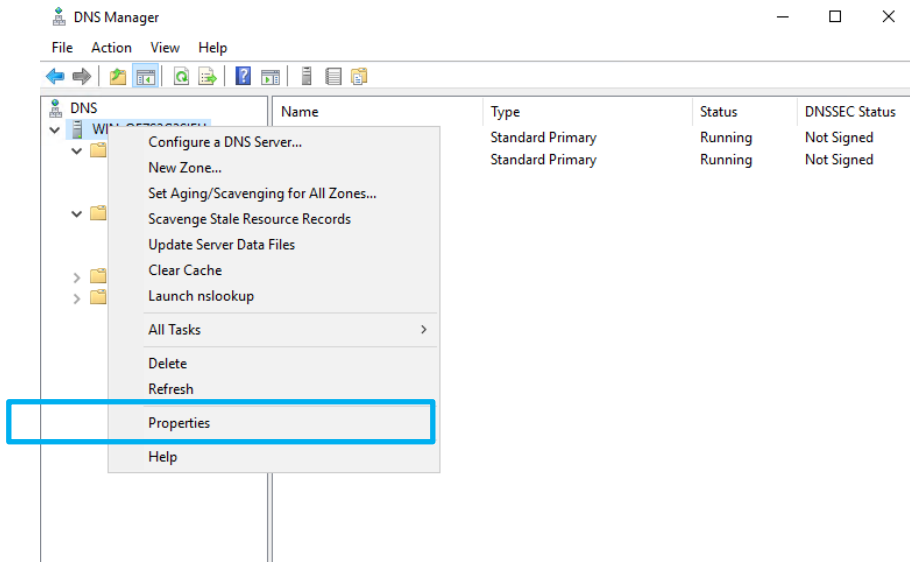
Figure 18 Configure DNS forwarders

2. In **Properties**, Click **Forwarders**.
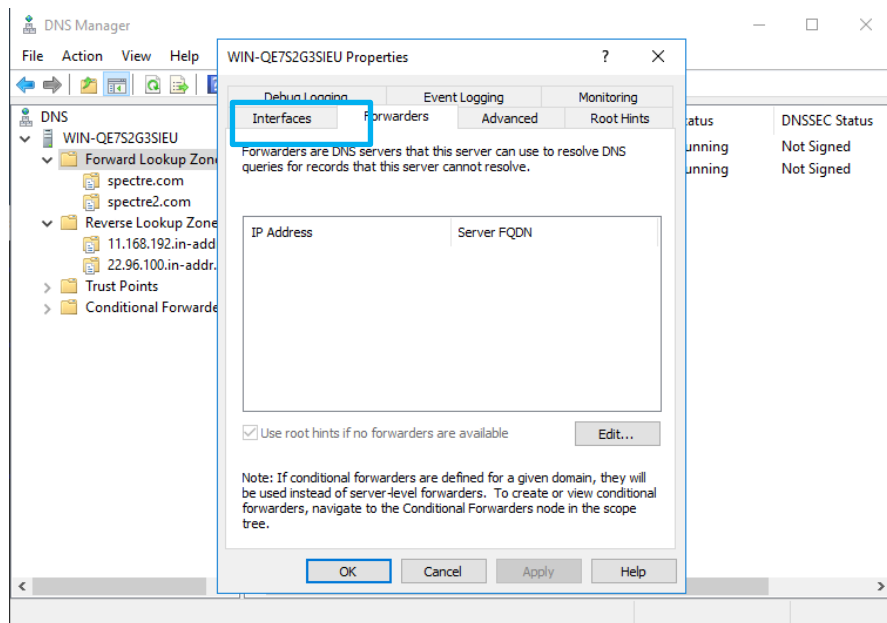
Figure 19 Configure DNS forwarders

3. Enter the IP address.
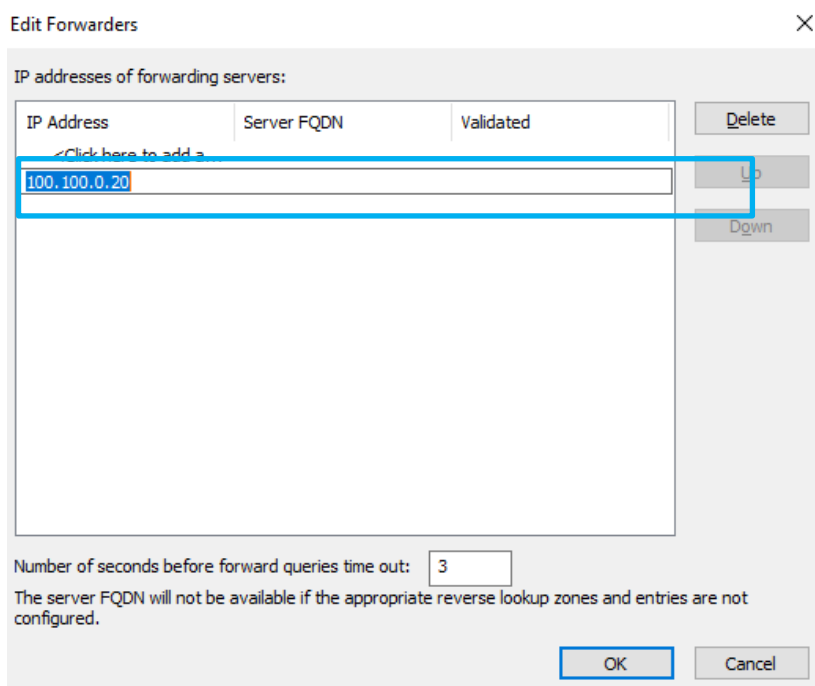
Figure 20 Configure DNS forwarders
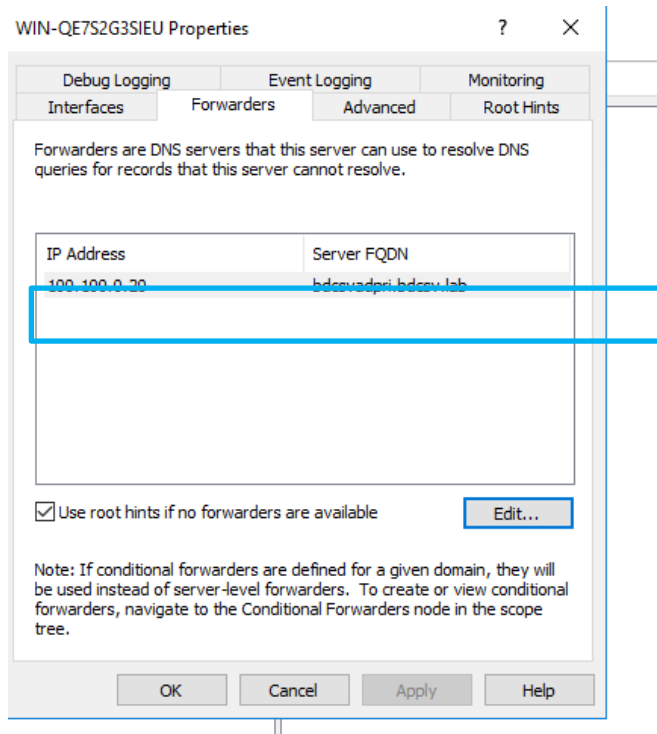
Figure 21 Configure DNS forwarders

Now the common DNS configured with forwarders will resolve the FQDN from both the DNS namespace.

DELLEMC

3 Change in area in OMIVV due to dual-NIC configuration

3.1.1 OS Deployment

While initiating OS deployment task, ensure that you select the NIC or interface which belongs to vSphere network.
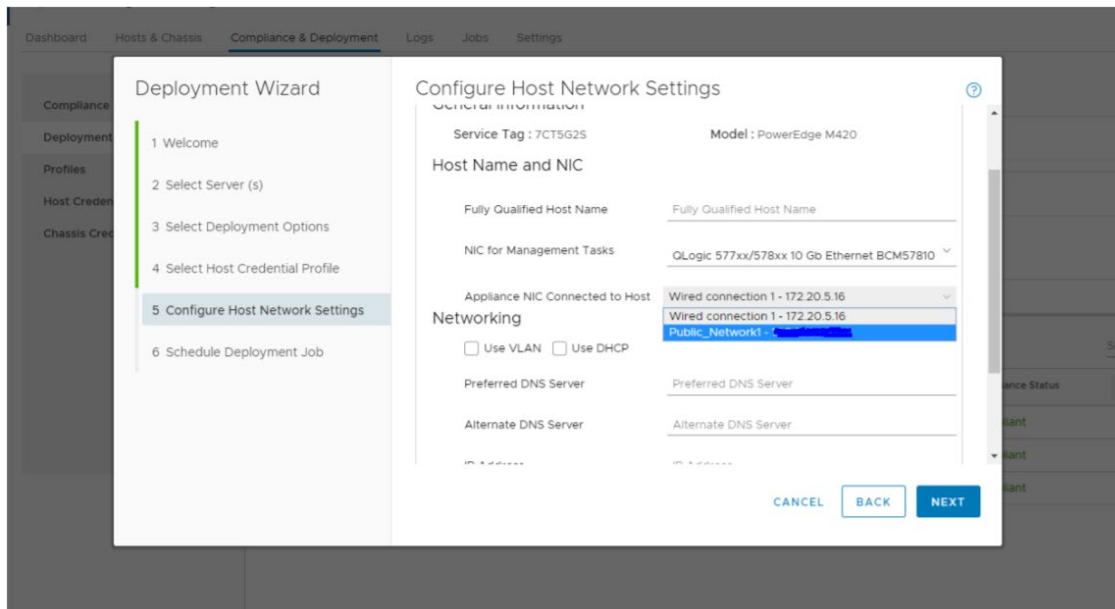
Figure 22 Configure host network settings in deployment wizard

3.1.2 SNMP Trap setting

If the OMIVV is configured with dual-NIC configuration with vSphere and out-of-band network, the SNMP trap destination set at iDRAC, or CMC, or OME-M will be appliance IP which belongs to out-of-band network.

Figure 23 SNMP Trap setting

DELLEMC

4 Network Port information

4.1 OMIVV to in-band network

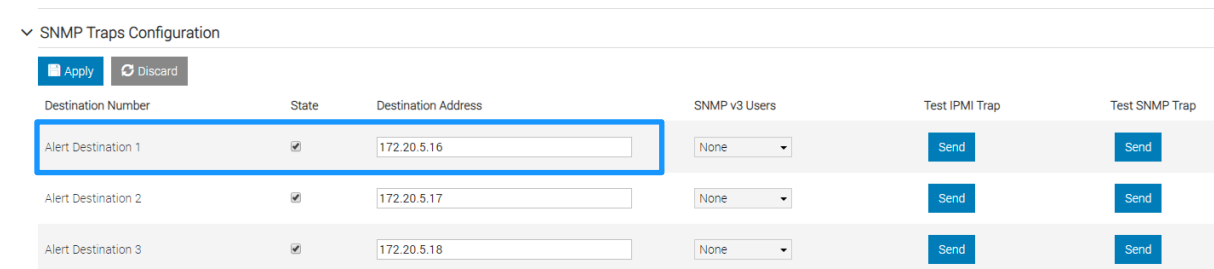| Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
53	DNS	TCP	None	Out	OMIVV appliance to DNS server	DNS client	Connectivity to the DNS server or resolving the host names
68	DHCP	UDP	None	In	DHCP sever to OMIVV appliance	Dynamic network configuration	To get the network details such as IP, gateway, Netmask and DNS
123	NTP	UDP	None	In	NTP to OMIVV appliance	Time Synchronization	To sync with specific time zone.
162	SNMP Agent	UDP	None	In	iDRAC/ESXi to OMIVV appliance	SNMP Agent (server)	To receive SNMP traps from managed nodes.
443	HTTPS	TCP	128-bit	In	ESXi server to OMIVV appliance	HTTPS server	Used in OS deployment flow for post installation scripts to communicate with the OMIVV appliance.
443	HTTPS WSMAN	TCP	128-bit	In/Out	OMIVV appliance from/to vCenter	HTTPS server	Web services offered by OMIVV. These Web services are consumed by vCenter Web Client and Dell Admin portal.
443	WSMAN	TCP	128-bit	In/Out	OMIVV appliance from/to vCenter	iDRAC/OMSA communication	iDRAC and CMC communication, used to manage and monitor the managed nodes.
443	HTTPS	TCP	None	Out	OMIVV appliance to internet	Dell Online Data Access	Connectivity to the online (internet) warranty, firmware, and latest RPM information
445/139	SMB	TCP	128-bit	Out	OMIVV appliance to CIFS	CIFS communication	To communicate with Windows share.
2049/111	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update and OS deployment flows.
4001 to 4004	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	These ports must be kept open to

							run the *statd*, *quotd*, *lockd*, and *mountd* services by the V2 and V3 protocols of the NFS server.
User defined	Any	UDP/ TCP	None	Out	OMIVV appliance to proxy server	Proxy	To communicate with the proxy server

Note: Dell EMC recommends configuring DNS to the in-band network.

Note: Ports related to CIFS or NFS share to be configured according to where the network share is in datacenter environment.

DELLEMC

4.2 OMIVV to out-of-band network

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
162	SNMP Agent	UDP	None	In	iDRAC/ESXi to OMIVV appliance	SNMP Agent (server)	To receive SNMP traps from managed nodes.
443	WSMAN	TCP	128-bit	In/Out	OMIVV appliance to/from iDRAC/OMSA	iDRAC/OMSA communication	iDRAC, OMSA, and CMC communication, used to manage and monitor the managed nodes.
445	SMB	TCP	128-bit	Out	OMIVV appliance to CIFS	CIFS communication	To communicate with Windows share.
4433	HTTPS	TCP	128-bit	In	iDRAC to OMIVV appliance	Auto Discovery	Provisioning server used for auto discovering managed nodes.
2049	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update and OS deployment flows.
4001 to 4004	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	These ports must be kept open to run the *statd*, *quotd*, *lockd*, and *mountd* services by the V2 and V3 protocols of the NFS server.
User defined	Any	UDP/TCP	None	Out	OMIVV appliance to proxy server	Proxy	To communicate with the proxy server

DELLEMC

4.3 OMIVV to Internet

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
443	HTTPS	TCP	None	Out	OMIVV appliance to internet	Dell Online Data Access	Connectivity to the online (internet) warranty, firmware, and latest RPM information
User defined	Any	UDP/TCP	None	Out	OMIVV appliance to proxy server	Proxy	To communicate with the proxy server

Note: Dell EMC recommends configuring in-band network for internet connectivity.

DELLEMC

5 Conclusion

Dell EMC provides products that simplify and streamline their IT processes, freeing administrator's time to focus on activities that help grow the business. This technical white paper provides comprehensive information about the dual network support capabilities of OMIVV, environments where this capability can be employed, and steps to configure, and verify.

DELLEMC

6　Technical support and resources

Dell.com/support

OMIVV product page

OMIVV Documentation page

External documentation for DNS forwarding

DELLEMC