Installation and Upgrade Guide

for

OmniVista 2500 NMS Enterprise Version 4.4R2

January 2020

Revision D

Part Number 060648-10

READ THIS DOCUMENT

OmniVista 2500 NMS

for

VMware ESXi: 5.5, 6.0, 6.5, 6.7

VirtualBox: 5.2.x

MS Hyper-V: 2012 R2, 2016, 2019

MS Hyper-V on Windows 10 Professional

ALE USA Inc.
26801 West Agoura Road
Calabasas, CA 91301
+1 (818) 880-3500

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

OmniVista 2500 NMS Enterprise 4.4R2 Installation and Upgrade Guide

This document details the OmniVista 2500 NMS Enterprise 4.4R2 (OV 2500 NMS-E 4.4R2) installation/upgrade process. OV 2500 NMS-E 4.4R2 can be installed as a fresh installation from a download file available on the Customer Support website; or you can upgrade directly from OV 2500 NMS-E 4.4R1 to 4.4R2 using the Virtual Appliance Menu.

Note: You can only directly upgrade via the VA Menu from an OV 4.4R1 Standalone Installation to an OV 4.4R2 Standalone Installation, or an OV 4.4R1 HA Installation to an OV 4.4R2 HA Installation. If you are upgrading from an earlier release, you must first upgrade to OV 4.4R1 before upgrading to OV 4.4R2.

If you are upgrading from releases 3.5.7 – 4.2.2.R01 (MR1), you must first upgrade to 4.2.2.R01 (MR2). You can then continue follow the upgrade paths below to 4.4R2 using the Virtual Appliance Menu. The Upgrade Matrix below shows the upgrade paths that must be followed to get to OV 2500 NMS-E 4.4R2.

Upgrade Matrix For OV 4.4R2

From	To OV 4.4R2
OV 3.5.7	Step 1: Upgrade to 4.2.1.R01 GA Step 2: Upgrade to 4.2.1.R01 MR 2 Step 3: Upgrade to 4.2.2.R01 GA Step 4: Upgrade to 4.2.2.R01 MR2 Step 5: Automatic Upgrade to 4.3R1 From VA Menu Step 6: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 7: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 8: Automatic Upgrade to 4.4R1 (Standalone) From VA Menu Step 9: Automatic Upgrade to 4.4R2 (Standalone) From VA Menu
OV 4.1.1.R01	Step 1: Upgrade to 4.1.2.R02 Step 2: Upgrade to 4.1.2.R03* Step 3: Upgrade to 4.2.1.R01 GA* Step 4: Upgrade to 4.2.1.R01 MR 2 Step 5: Upgrade to 4.2.2.R01 GA Step 6: Upgrade to 4.2.2.R01 MR2 Step 7: Automatic Upgrade to 4.3R1 From VA Menu Step 8: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 9: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 10: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 11: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.1.2.R01	Step 1: Upgrade to 4.1.2.R03* Step 2: Upgrade to 4.2.1.R01 GA* Step 3: Upgrade to 4.2.1.R01 MR 2 Step 4: Upgrade to 4.2.2.R01 GA Step 5: Upgrade to 4.2.2.R01 MR2 Step 6: Automatic Upgrade to 4.3R1 From VA Menu Step 7: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 8: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 9: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 10: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu

From	To OV 4.4R2
OV 4.1.2.R02	Step 1: Upgrade to 4.1.2.R03* Step 2: Upgrade to 4.2.1.R01 GA* Step 3: Upgrade to 4.2.1.R01 MR 2 Step 4: Upgrade to 4.2.2.R01 GA Step 5: Upgrade to 4.2.2.R01 MR2 Step 6: Automatic Upgrade to 4.3R1 From VA Menu Step 7: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 8: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 9: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 10: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.1.2.R03	Step 1: Upgrade to 4.2.1.R01 GA Step 2: Upgrade to 4.2.1.R01 MR 2 Step 3: Upgrade to 4.2.2.R01 GA Step 4: Upgrade to 4.2.2.R01 MR2 Step 5: Automatic Upgrade to 4.3R1 From VA Menu Step 6: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 7: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 8: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 9: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.2.1.R01-GA (Build 69)	Step 1: Upgrade to 4.2.1.R01 MR 2 Step 2: Upgrade to 4.2.2.R01 GA Step 3: Upgrade to 4.2.2.R01 MR2 Step 4: Automatic Upgrade to 4.3R1 From VA Menu Step 5: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 6: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 7: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 8: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.2.1.R01 MR 1 (Build 85)	Step 1: Upgrade to 4.2.1.R01 MR 2 Step 2: Upgrade to 4.2.2.R01 GA Step 3: Upgrade to 4.2.2.R01 MR2 Step 4: Automatic Upgrade to 4.3R1 From VA Menu Step 5: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 6: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 7: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 8: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.2.1.R01 MR 2 (Build 95)	Step 1: Upgrade to 4.2.2.R01 GA Step 2: Upgrade to 4.2.2.R01 MR2 Step 3: Automatic Upgrade to 4.3R1 From VA Menu Step 4: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 5: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 6: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 7: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.2.2.R01 GA (Build 81)	Step 1: Upgrade to 4.2.2.R01 MR2 Step 2: Automatic Upgrade to 4.3R1 From VA Menu Step 3: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 4: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 5: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.2.2.R01 MR1 (Build 92)	Step 1: Upgrade to 4.2.2.R01 MR2 Step 2: Automatic Upgrade to 4.3R1 From VA Menu Step 3: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 4: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 5: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 6: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu

From	To OV 4.4R2
OV 4.3R1	Step 1: Automatic Upgrade to 4.3R2 (Standalone) From VA Menu Step 2: Automatic Upgrade to 4.3R3 (Standalone) From VA Menu Step 3: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 4: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV 4.3R2	Step 1: Automatic Upgrade to 4.3R3 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 3: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu
OV4.3R3	Step 1: Automatic Upgrade to 4.4R1 (Standalone/HA) From VA Menu Step 2: Automatic Upgrade to 4.4R2 (Standalone/HA) From VA Menu

* This step includes Mongodb Database Password change. Please make sure all the steps for changing the password are followed as detailed in the applicable *OmniVista 2500 NMS Installation Guide.*

Important Note: A minimum reserved OmniVista VA RAM of 20GB is now recommended for "Low" Sized Network configurations (up to 500 devices). If you are managing a "Low" Sized Network and are upgrading from OVE 4.4R1 to 4.41R2, make sure you have a **minimum** of 20GB of reserved OmniVista VA RAM. See Required Minimum System Configurations for details on Hypervisor configurations based on network size.

Note: If you are upgrading from an older release, take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.

Note: As you complete each upgrade in the upgrade path, make sure **all services are running** and you can access the OmniVista Web GUI before proceeding to the next upgrade.

Note: If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.

For information on getting started with OmniVista 2500 NMS after installation (e.g., using the Web GUI, discovering network devices) see the *Getting Started Guide* in the OmniVista 2500 NMS on-line help (accessed from Help link at the top of the main OmniVista NMS Screen).

Installing OmniVista 2500 NMS-E 4.4R2

OV 2500 NMS-E 4.4R2 is distributed as a Virtual Appliance only. It is run as a service using VirtualBox. There are no other standalone installers (e.g., Windows/Linux). OV 2500 NMS-E 4.4R2 is installed as a Virtual Appliance, and can be deployed on the following hypervisors: VMware ESXi, VirtualBox, Hyper-V:

- VMware ESXi: 5.5, 6.0, 6.5, and 6.7
- VirtualBox: 5.2.x
- MS Hyper-V: 2012 R2, 2016, and 2019

- MS Hyper-V on Windows 10 Professional.

The sections below detail each of the steps required to deploy OV 2500 NMS-E 4.4R2 as Virtual Appliance on VMware, VirtualBox, and Hyper-V. Note that If you are deploying OV 2500 NMS-E 4.4R2 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See Appendix A for details.

Important Note: Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. Insufficient memory or disk space for the chosen network size may cause OV instability. OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 16GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to Required System Configurations for details.

Required Minimum System Configurations

The table below provides required minimum Hypervisor configurations for the OmniVista VM based on the number of devices being managed (500, 2,000, 5,000, and 10,000 devices). These configurations should be used as a guide. Specific configurations may vary depending on the network, the number of wired/wireless clients, the number of VLANs, applications open, etc. For more information, contact Customer Support.

	Network Size			
Configuration	**Low**	**Medium**	**High**	**Very High**
Total Number of Managed Devices (AOS, Third-Party, and Stellar APs)	500	2,000	5,000*	10,000*
Stellar AP Devices	500	2,000	4,000	4,000
Stellar AP Client Association	50,000	200,000	200,000	200,000
UPAM Authentication	15,000	30,000	100,000	100,000
Hypervisor Processor	2.4 GHz 8 Logical Processors	2.4 GHz 8 Logical Processors	2.4 GHz 12 Logical Processors	2.4 GHz 12 Logical Processors
Minimum Reserved OmniVista VA RAM	20GB	32GB	64GB	64GB
HDD Provisioning	HDD1:50GB HDD2:256GB	HDD1:50GB HDD2:512GB	HDD1:50GB HDD2:2048GB	HDD1:50GB HDD2:2048GB

*If there are 4,000 Stellar AP in a “High” network size, up to 500 AOS Switches can be supported. If there are 4,000 Stellar APs in a “Very Hight” network size, up to 1,000 AOS Switches can be supported.

Notes:

- When provisioning RAM for a new VM for OmniVista, never allocate more memory than is available on the Host Server. For example, if you are running a Host Server with 128GB of memory and have already allocated 96GB of memory to your existing

VMs, accounting for the Host Server's own memory use, you are not left with enough memory to run OmniVista without incident. VM RAM is configured from the Hypervisor.

- Allocate the recommended amount of RAM for the OmniVista VM based on your network size as shown in the above table. In addition, it is recommended that you **reserve** that RAM for the OmniVista VM to prevent performance issues.
- Set CPU Shares to "High".
- Do not exceed the number of Logical Processors recommended for your network size as shown in the above table. Hypervisor Processors are configured from the Hypervisor.
- HDD Provisioning is configured from the VA Menu. By default, OV 2500 NMS-E 4.4R2 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you go to the Virtual Appliance Menu on the VA to increase the OmniVista disk space. For a **Standalone** Installation, use the "Extend Data Partition" option under Configure Network Size in the Configure The Virtual Appliance Menu (Configure The Virtual Appliance Menu – Configure Network Size – Extend Data Partition). For a **High-Availability** Installation, use the "Extend Data Partition" option under Configure Current Node in The HA Virtual Appliance Menu (The HA Virtual Appliance Menu - Configure Current Node - Extend Data Partition).
- OmniVista can be configured to use SNMPv3 to communicate with devices. When editing this configuration, you can specify which algorithms should be used. A recommended algorithm is AES ("Advanced Encryption Standard"). To get the best performance from your hypervisor, we recommend that you use Intel processors with the AES-NI instruction set enabled.
- AES-NI was introduced by Intel in 2010 in its Westmere family of processors and allows your hypervisor and its VMs to manage AES-related workloads natively. To realize the full benefits of AES-NI, you need to ensure that it is made available to the VM running OmniVista. To do this:
  - Your hypervisor's CPUs must be newer CPUs (> 2010)
  - AES-NI must be enabled in your hypervisor's BIOS
  - The AES-NI feature must not be "masked" by your hypervisor.
- By default, VMWare and Hyper-V are "pass-through" meaning that OmniVista's VM will be able to use AES acceleration. When using VirtualBox, please verify that "Nested paging" is enabled.
- The High-Availability Feature supports up to 2,000 devices. 10,000?

Standalone and High-Availability Installations

OV 2500 NMS-E 4.4R2 can be installed in a Standalone or High-Availability configuration. A High-Availability Installation consists of two VMs (Node 1 and Node 2), with one node acting as the Active OV Server (Node 1) and the other as a Standby OV Server (Node 2). If Node 1 fails, OmniVista will automatically failover to Node 2.

Deploying OmniVista on a Virtual Appliance

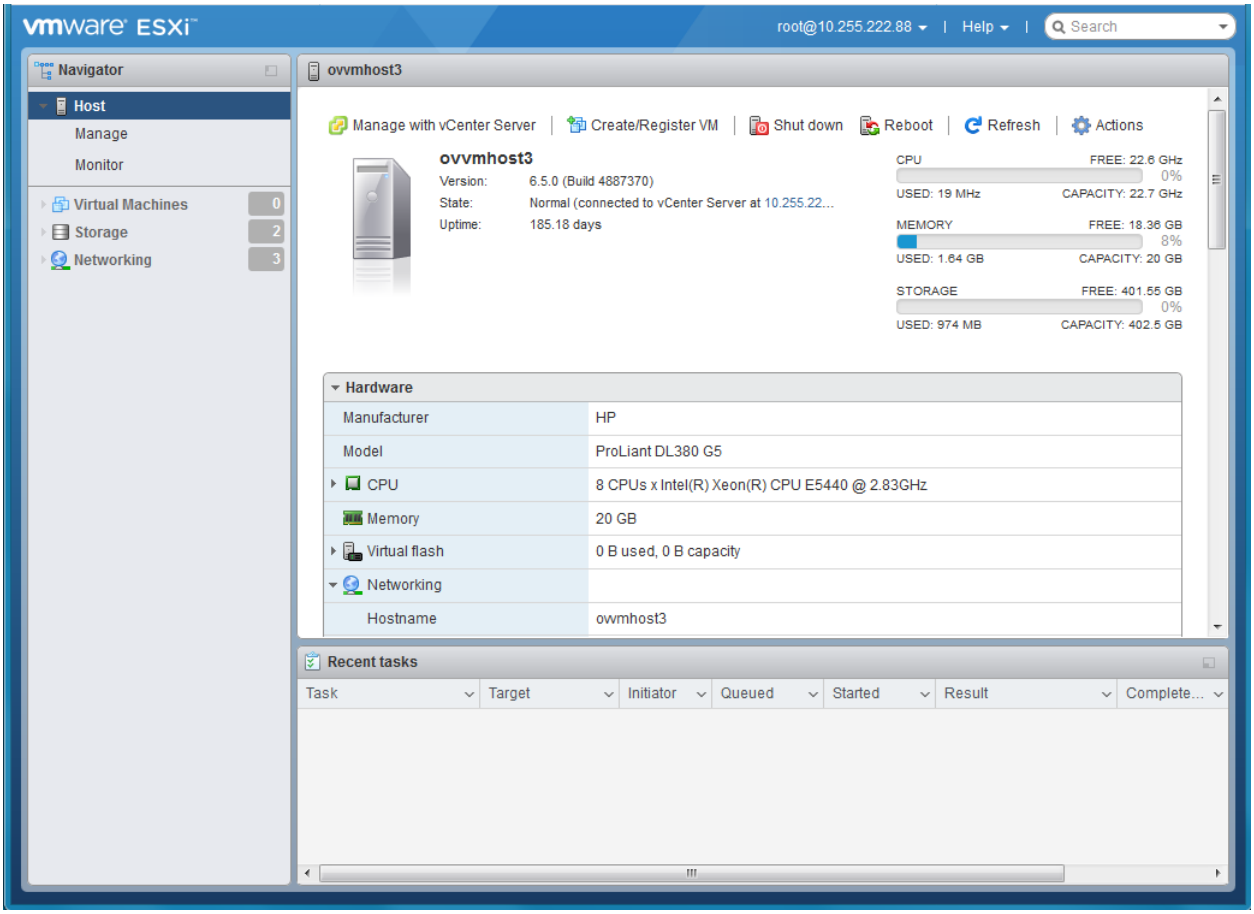
The sections below detail deploying OmniVista on a VM. For a High-Availability installation, you must deploy **two** (2) VMs – one for the Active OV Server (Node 1) and one for the Standby OV Server (Node 2).

Note: The High-Availability Feature supports up to 2,000 devices. 10,000?

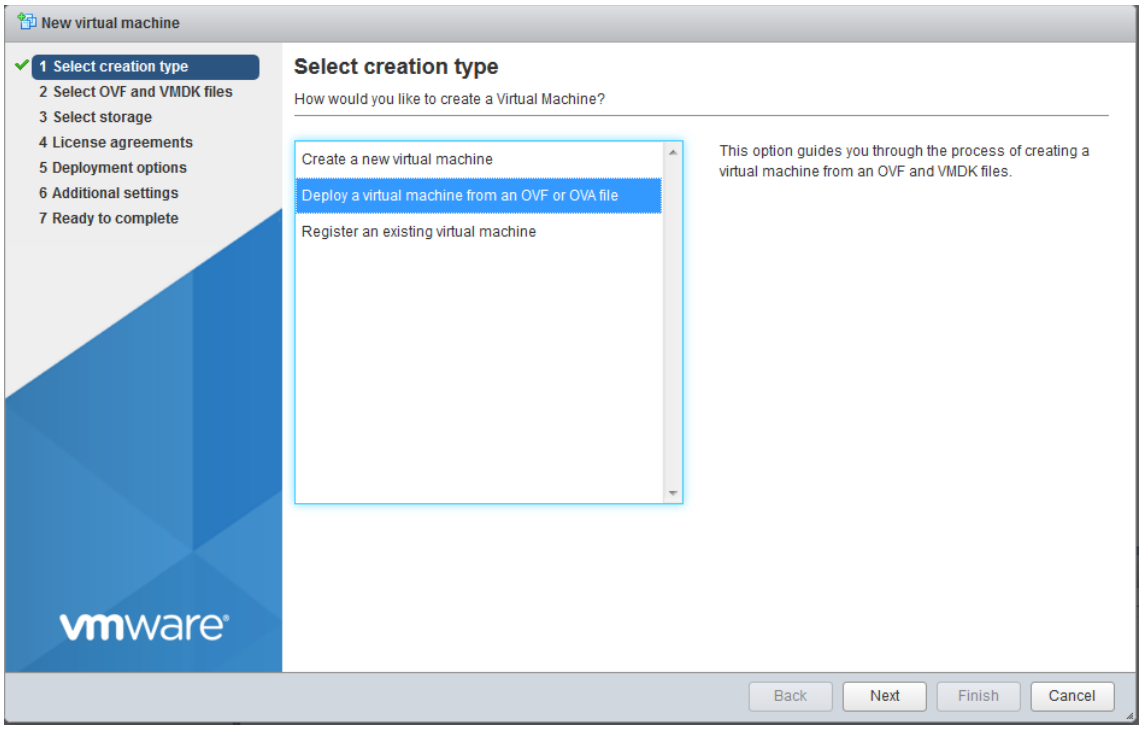
Deploying the Virtual Appliance in VMware ESXi

1. Download and unzip the OVF package. You will be using the OVF File and both VMDK Files (disk 1 and disk 2) for the installation. **The Zip file also contains an *.mf File. Delete the *.mf File from the folder before importing the files in Step 5.**

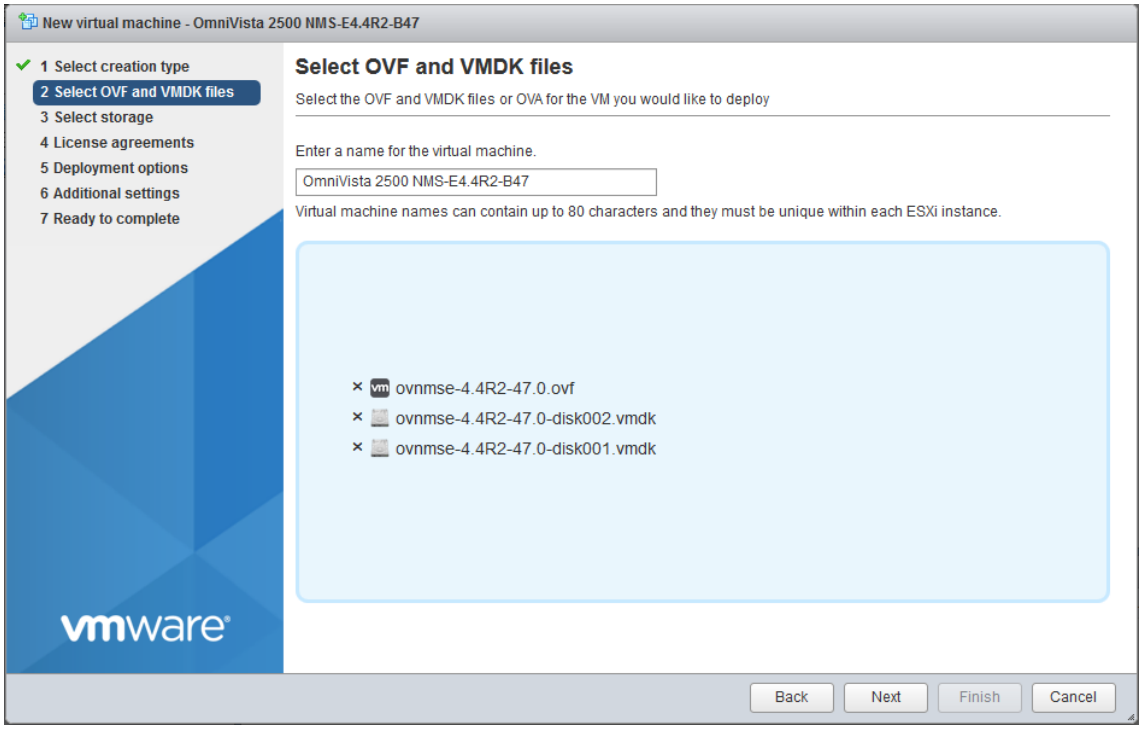
2. Log into VMware ESXi.



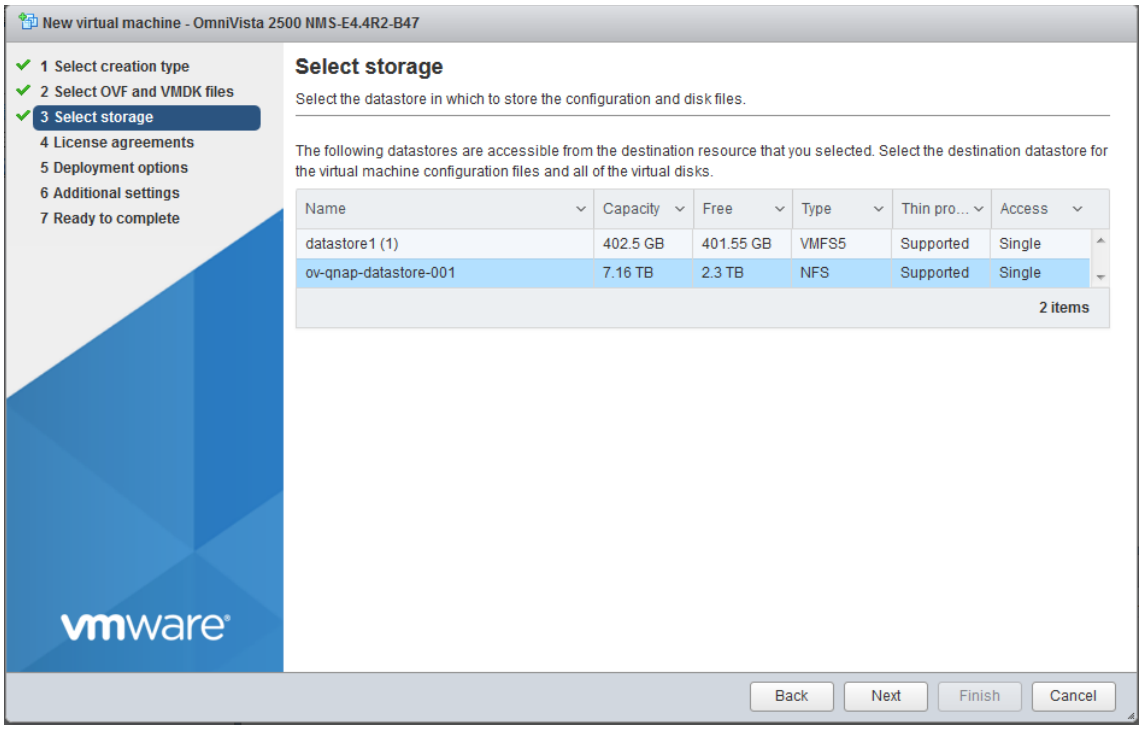
3. Select the Host on which you want to install OV 2500 NMS-E 4.4R2 and click on **Create/Register VM**. The first screen of the New Virtual Machine Wizard appears.



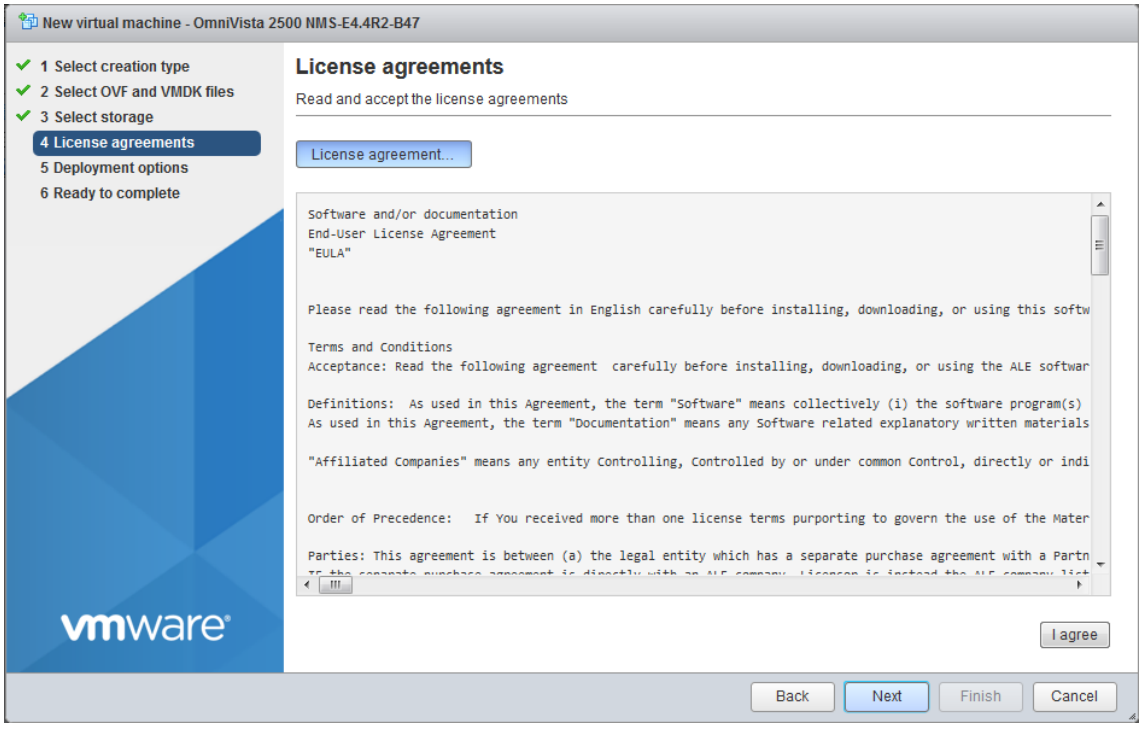
4. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



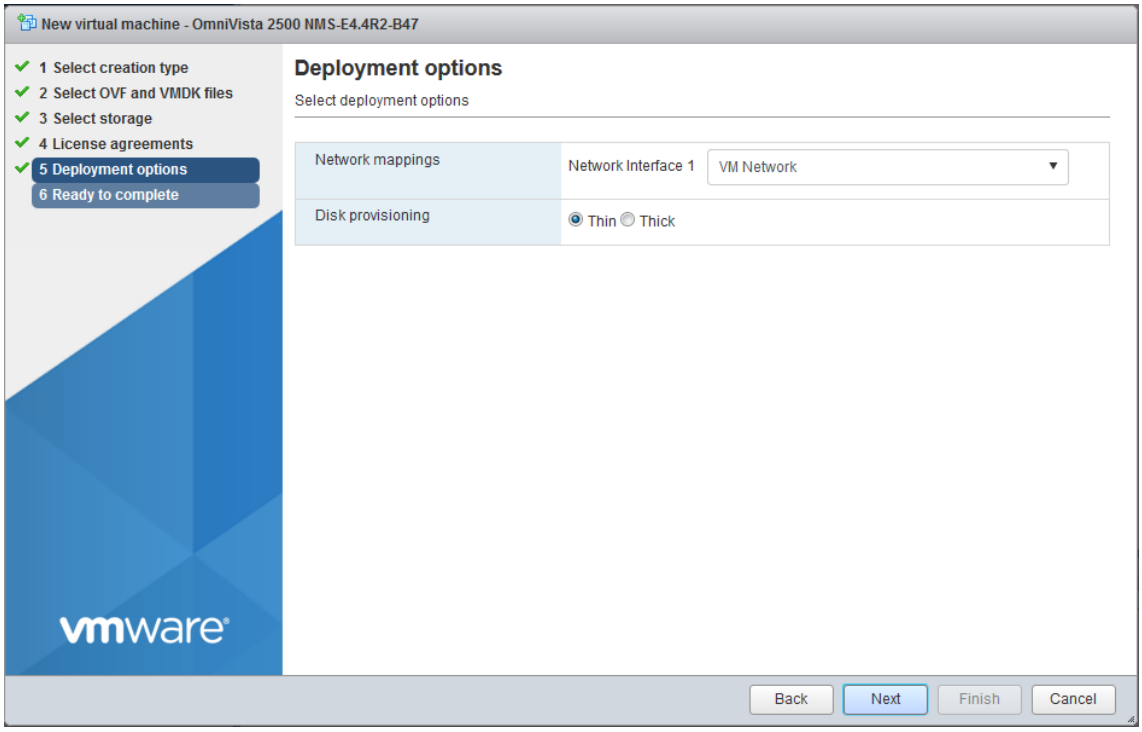
5. Enter a name for the VM (e.g., OmniVista 2500 NMS-E44R2-B47, click to locate and select the downloaded installation files (or drag the files into the window), then click **Next**. Note that if you plan on configuring a High-Availability installation, you could add Node information to the name (e.g., OmniVista 2500 NMS-E44R2-B47 Node 1) to more easily identify the VM.



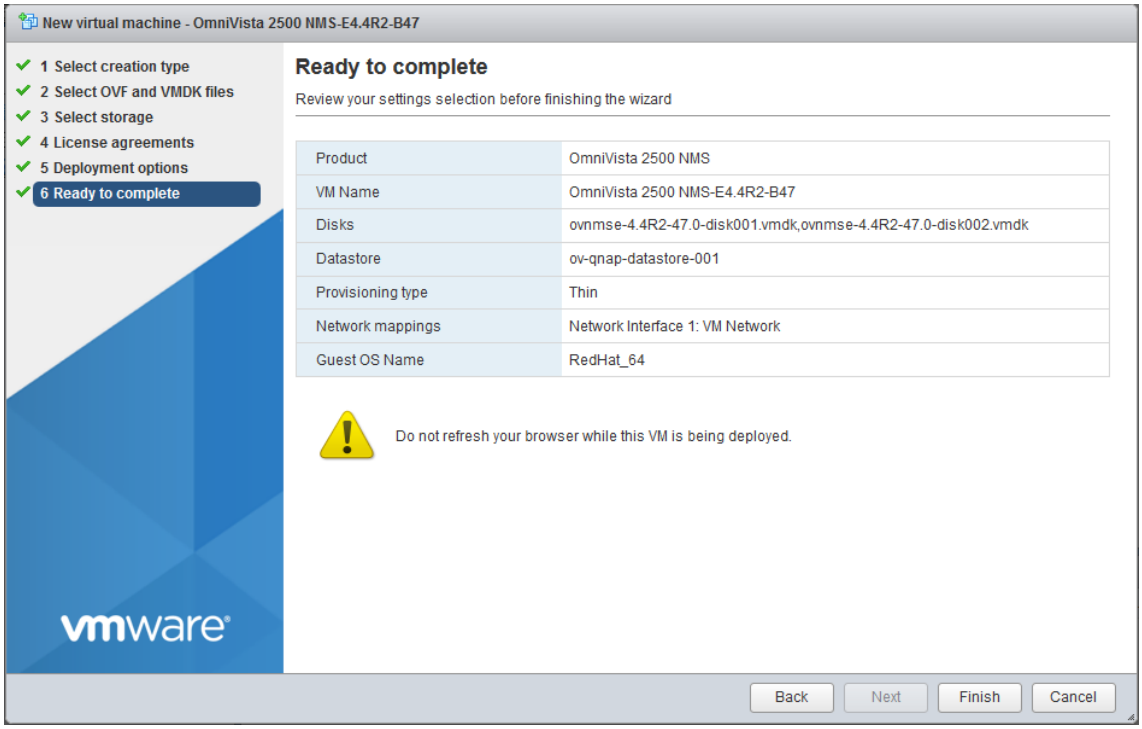
6. Select the destination storage where the template is to be deployed, then click **Next**.



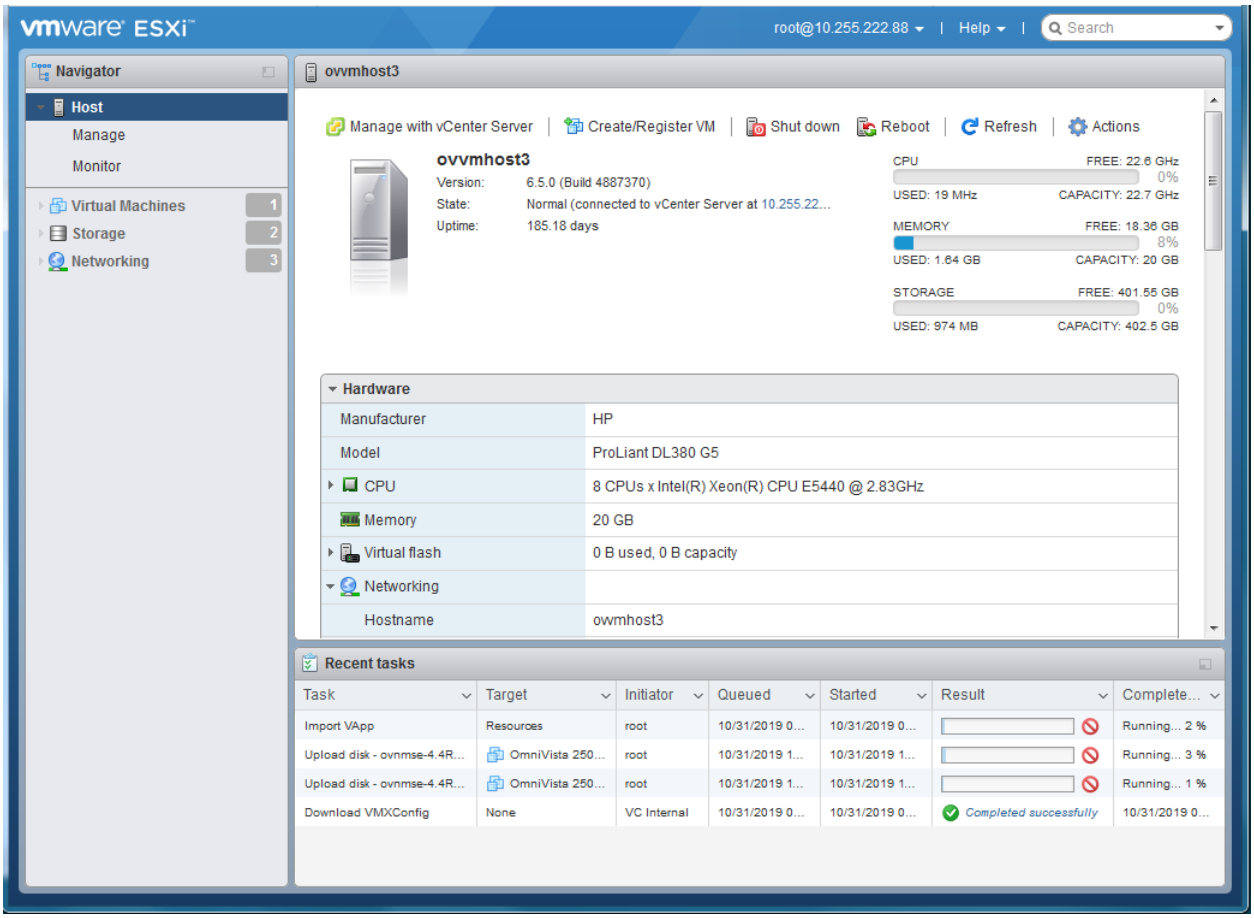
7. Review the License Agreement, click **I agree**, then click **Next**.



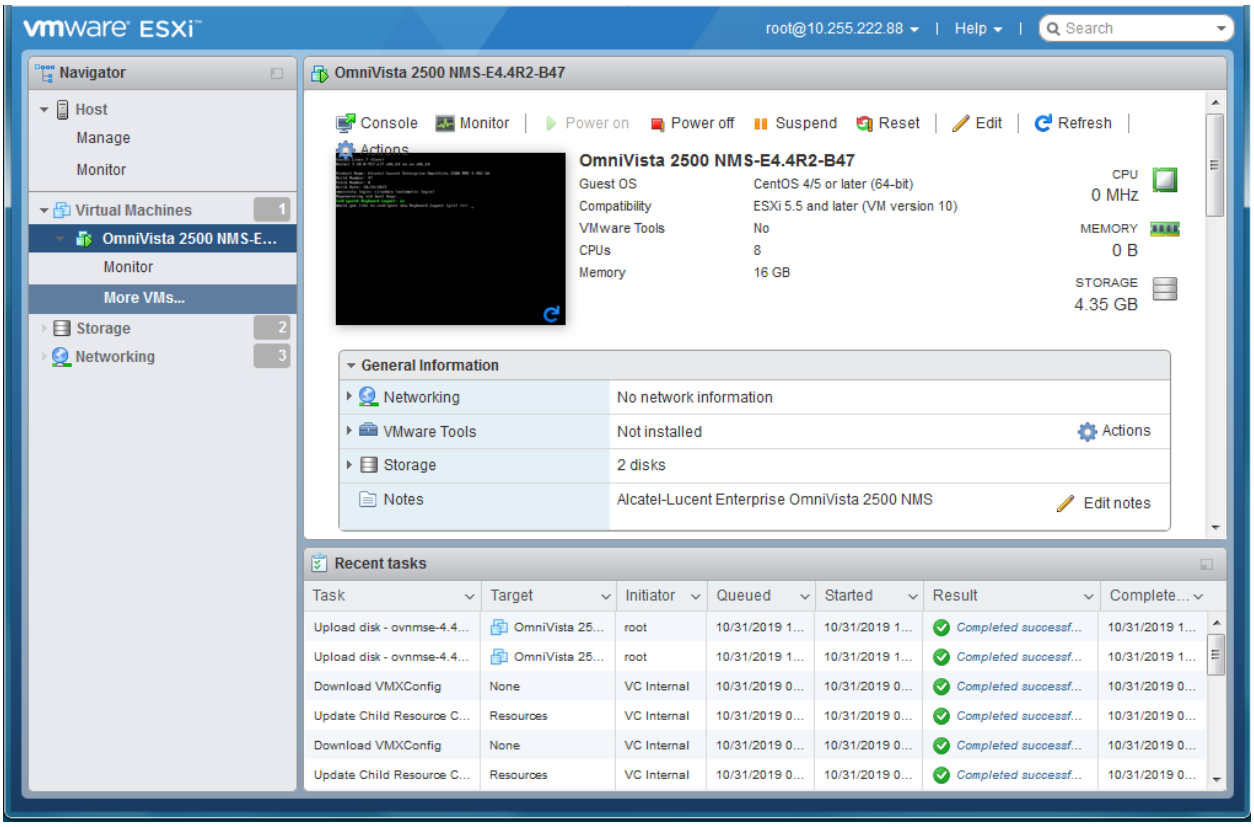
8. In the **Network mapping** field, select the Destination network that the deployed VM will use. In the **Disk provisioning** field, select **Thin**. Click **Next**.



9. Review the configuration and click **Finish**. You will be returned to the main screen with the deployment progress displayed in the **Recent tasks** table.



10. When the installation is complete (indicated by all three files showing “Completed Successfully” in the Result column of the Recent tasks table), click on **Virtual Machines** in the Navigator Tree on the left side of the screen to display a list of VMs. Select the VM you just deployed. Basic details for the VM are displayed, as shown below.



11. Click on the small Console Screen or click on **Console** at the top of the screen and select **Open Browser Console** to open a Console and go to Completing the OmniVista Installation to complete the installation.

> **Note:** After deploying the OmniVista VM, configure any additional NICs you may need on the VM before Completing the OmniVista Installation.

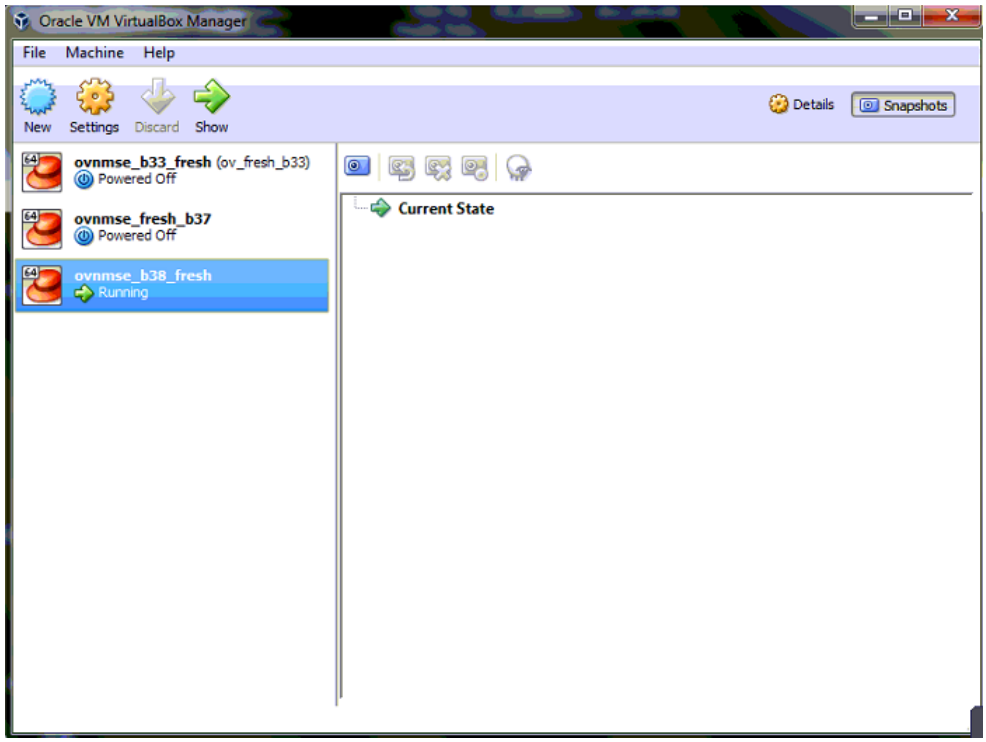
Deploying the Virtual Appliance in VirtualBox

Note that in the instructions below, VirtualBox 5.2.x in Windows 7 is used for demonstration purposes. The screens shown may depict an older OmniVista Release.

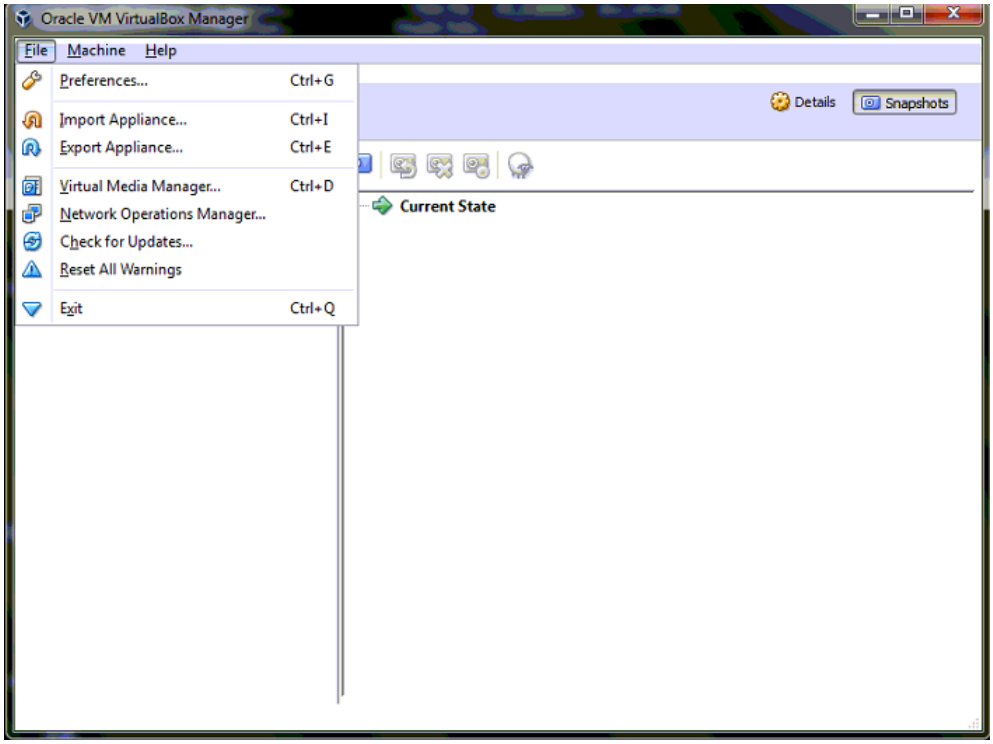
> **Note:** If you are deploying OV 2500 NMS-E 4.4R2 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See Appendix A for details.

1. Download and unzip the OVF package. You will be using the OVF File and both VMDK Files (disk 1 and disk 2) for the installation. **The Zip file also contains an *.mf File. Delete the *.mf File from the folder before importing the files in Step 5.**

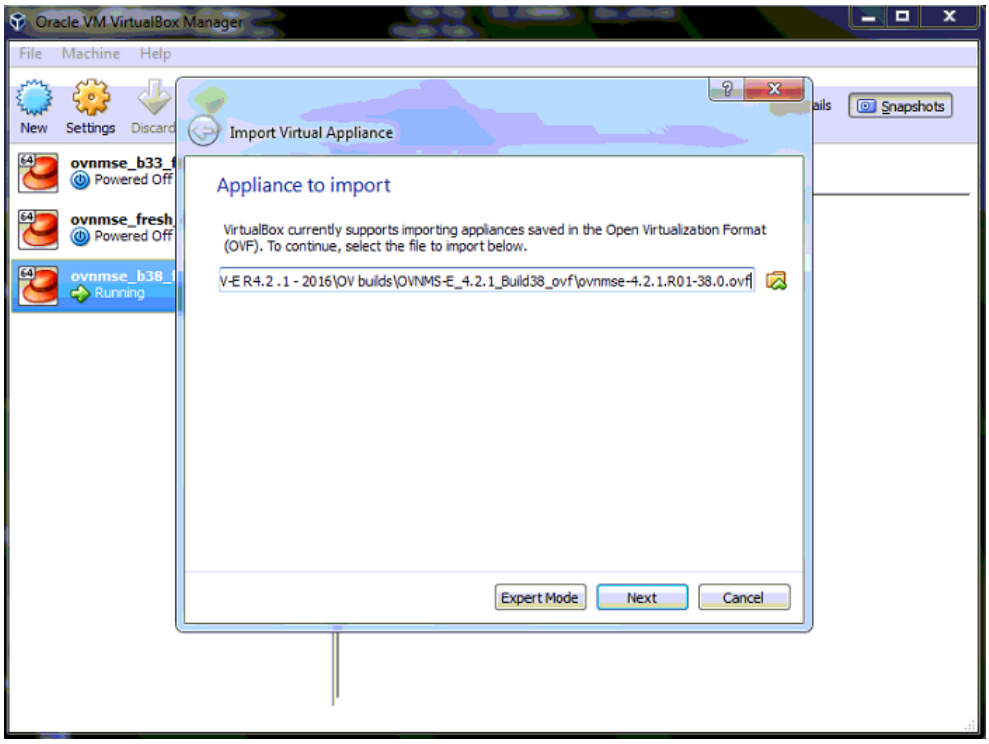
2. Log into Windows 7 and open the Oracle VM VirtualBox tool.



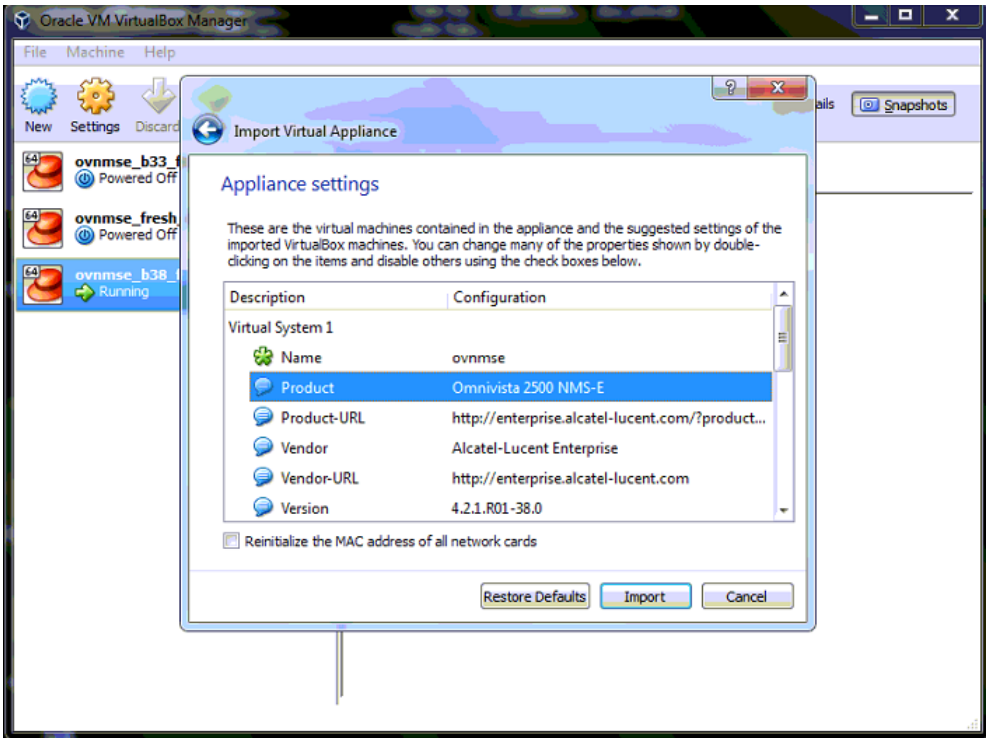
3. Click **File > Import Appliance**.



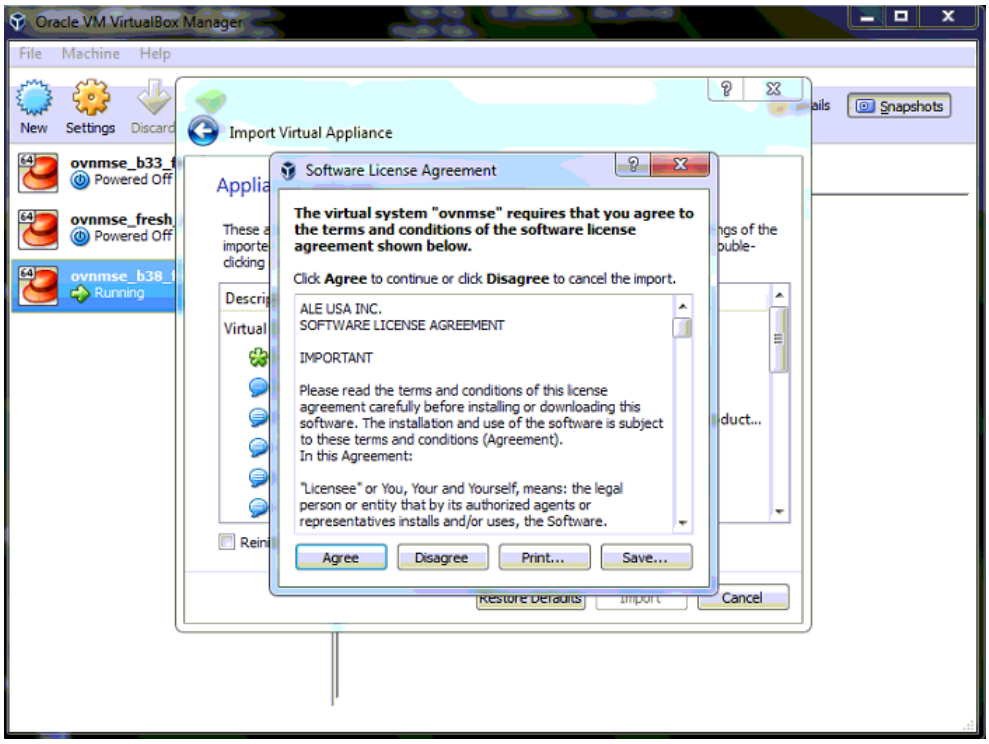
4. Click **browse** icon then select the **folder** which you extracted at step 1 above, then click **Next**.



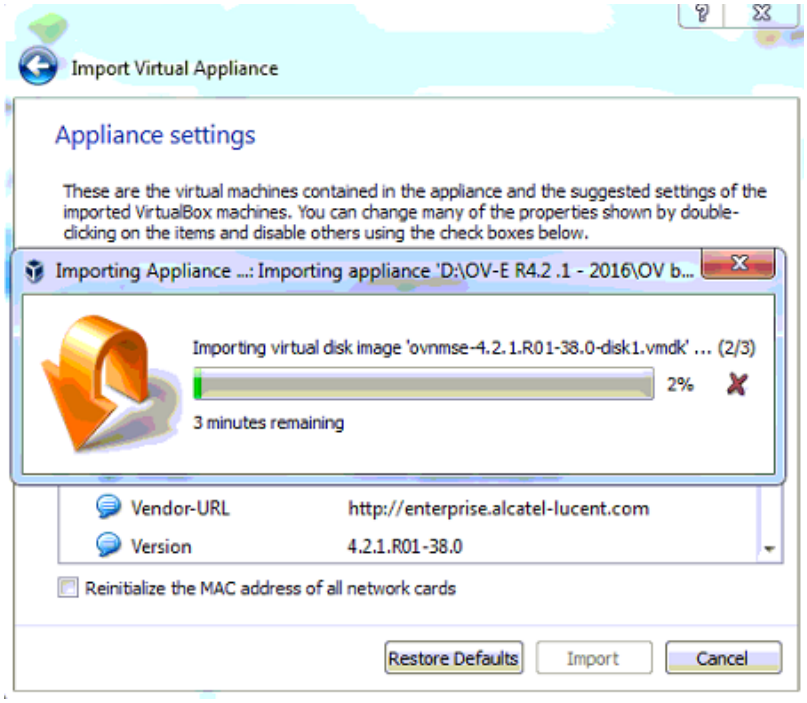
5. Review the configuration and click **Import**.



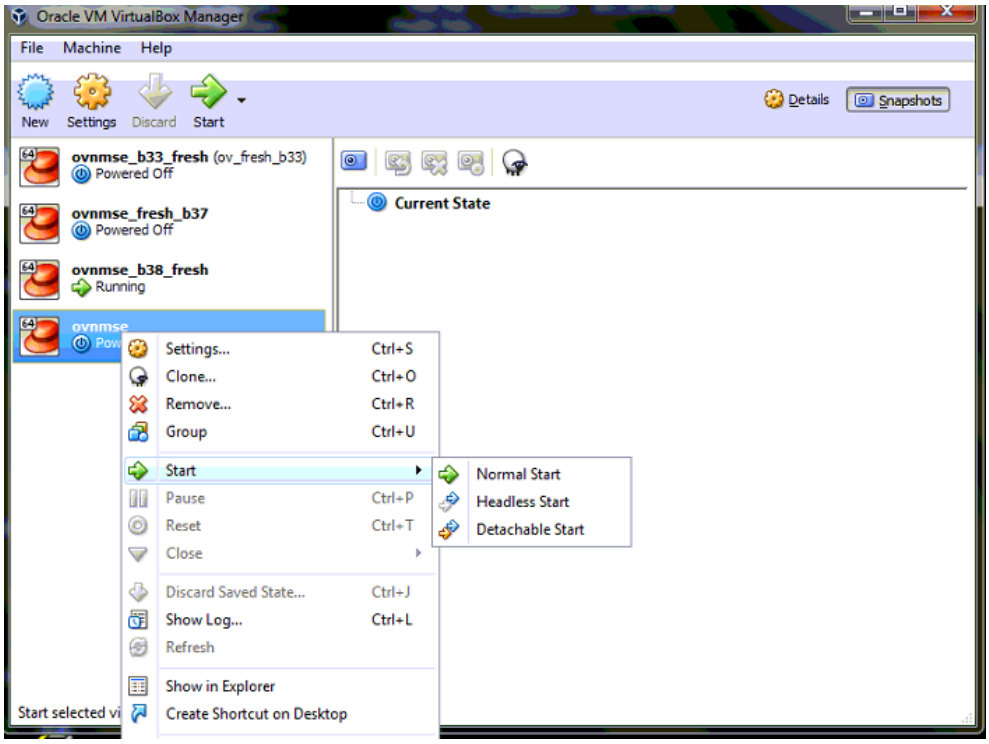
6. The **Software License Agreement** window displays, click on **Agree**.



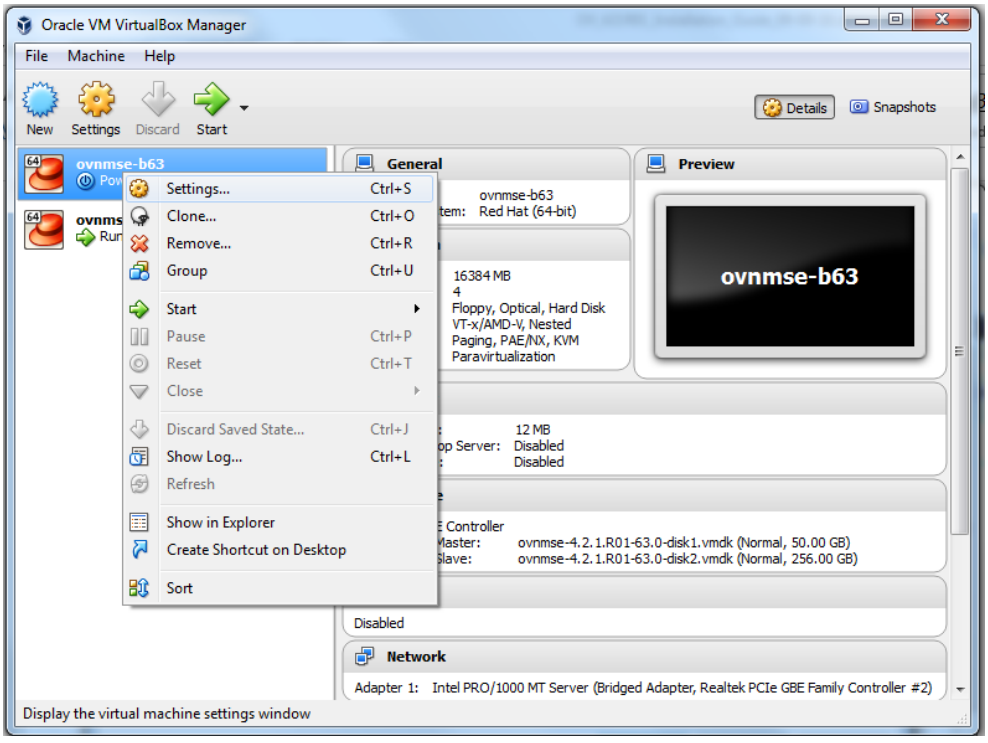
7. A status window appears and displays the progress of the deployment.



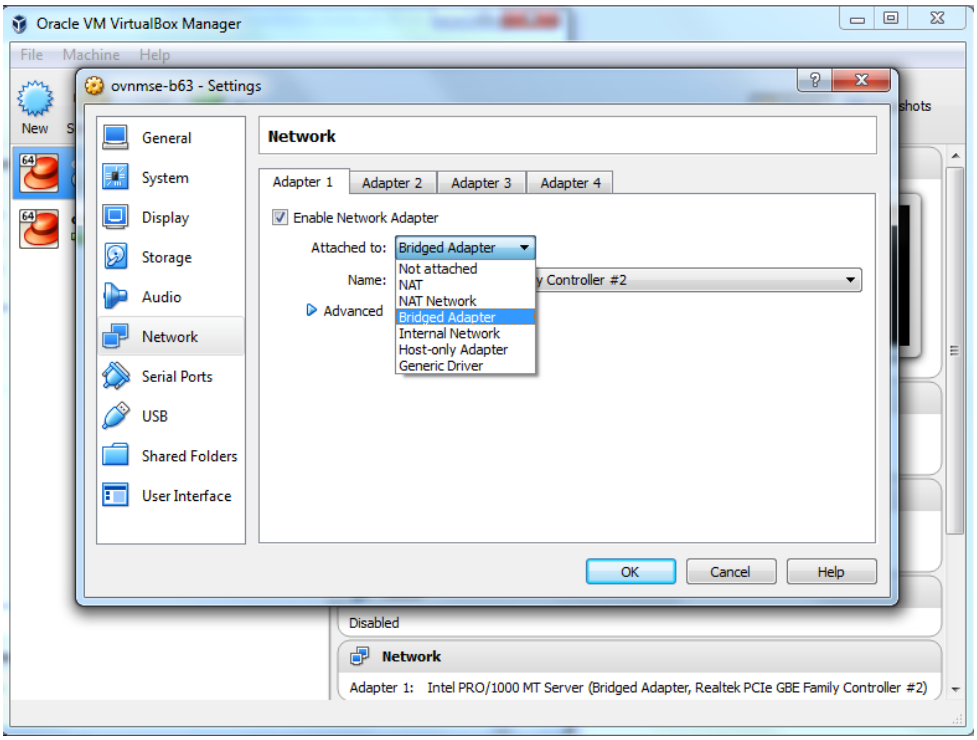
8. After the process is completed, right-click on the VM in the Navigation Panel and select **Start - Normal Start**.



9. Configure the Network Adapter. Right-click on the VA and select **Settings**.



10. Select **Network**, then select the Network Adaptor that you created when you configured VirtualBox.



Once the Virtual Appliance is powered on, go to Completing the OmniVista Installation to complete the installation.

> **Note:** After deploying the OmniVista VM, configure any additional NICs you may need on the VM before Completing the OmniVista Installation.

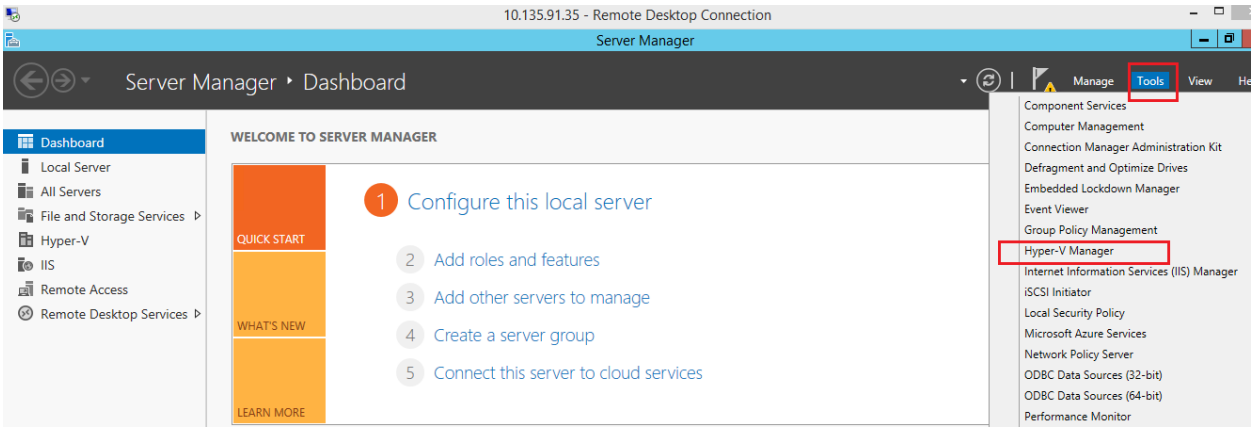
Deploying the Virtual Appliance in Hyper-V

Note that in the instructions below, Hyper-V in Windows 2012 is used for demonstration purposes. Some of the screens shown may depict an older OmniVista Release.

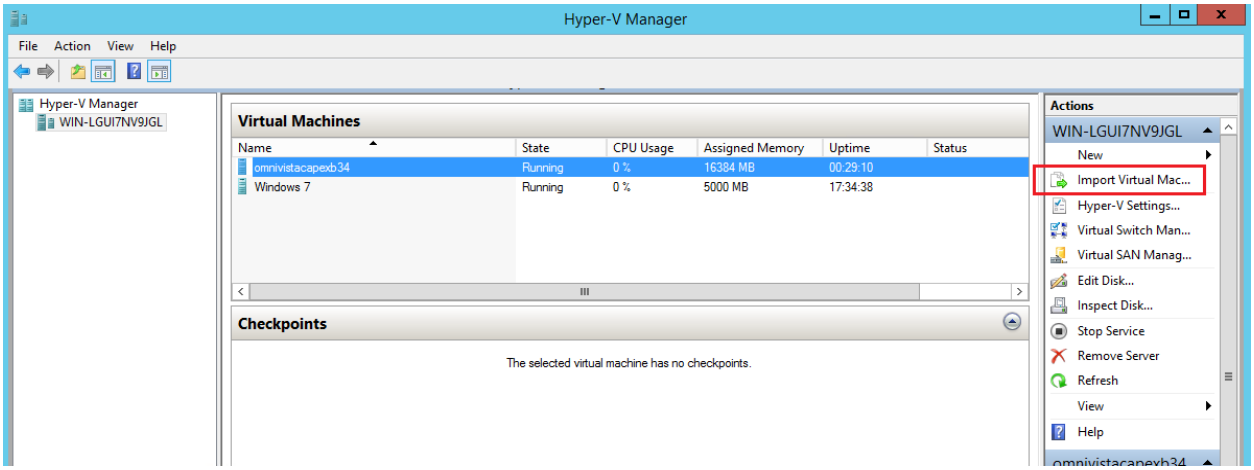
> **Note:** OmniVista does not support Hyper-V Live Migration. Also note that the OmniVista VM Manager application is not supported on Hyper-V 2019.

1. Download and unzip the OVF Hyper-V package. You will be using the OVF File and both VMDK Files (disk 1 and disk 2) for the installation. **The Zip file also contains an *.mf File. Delete the *.mf File from the folder before importing the files in Step 5.**

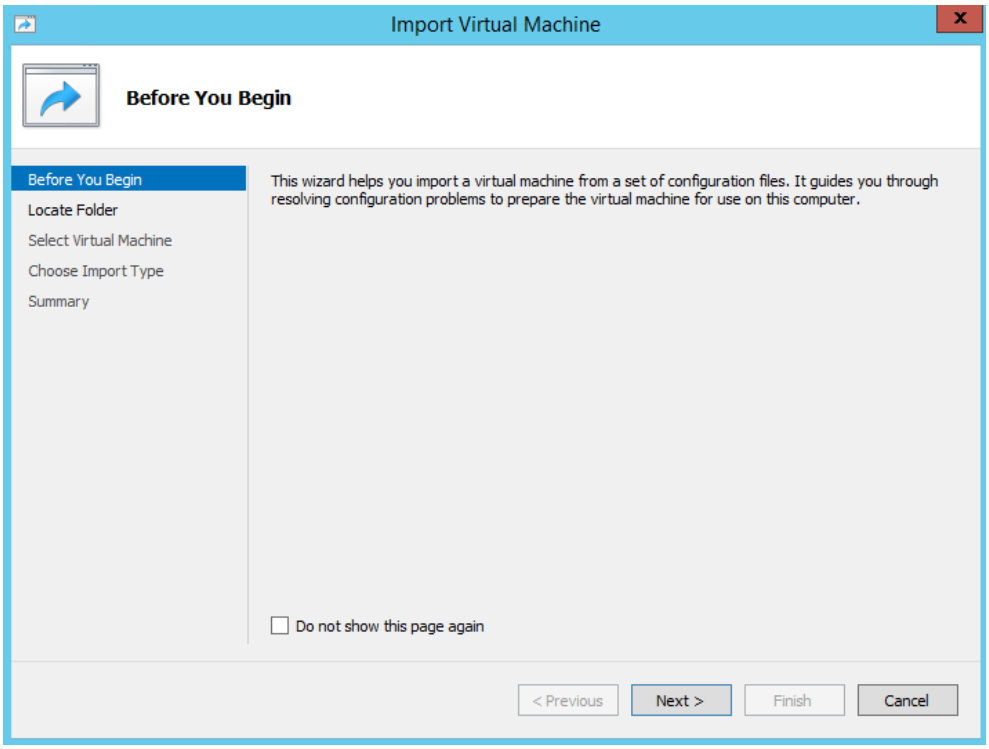
2. Log into Windows 2012 and open the Hyper-V tool.



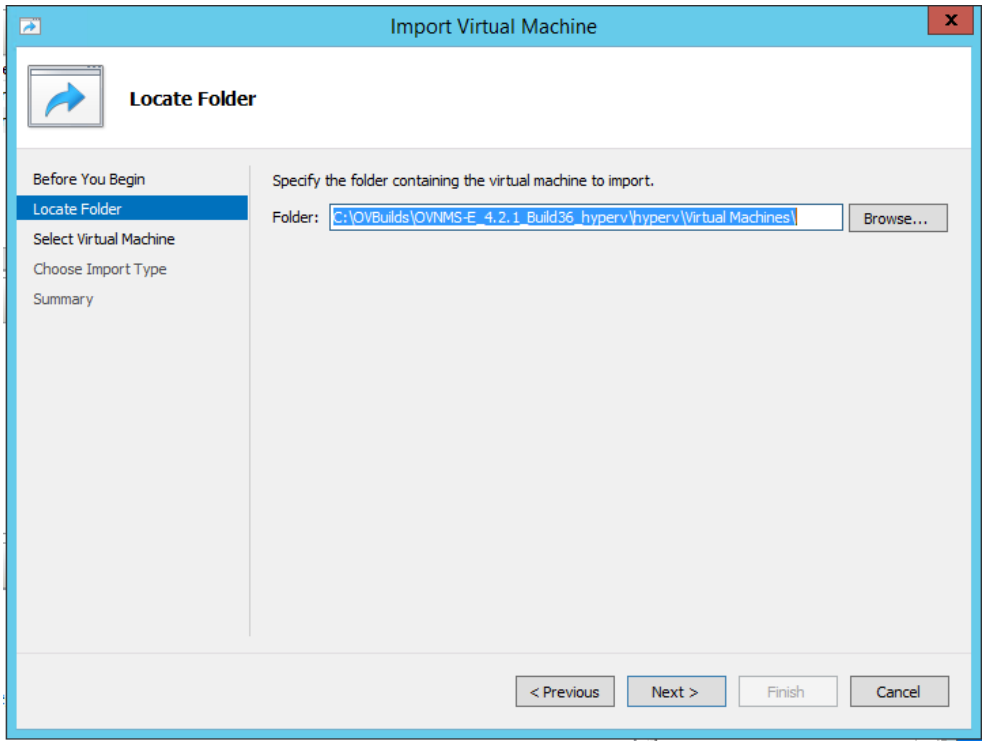
3. Select the Host on which you want to install OmniVista 2500 NMS, click on **Actions > Import Virtual Machine**.



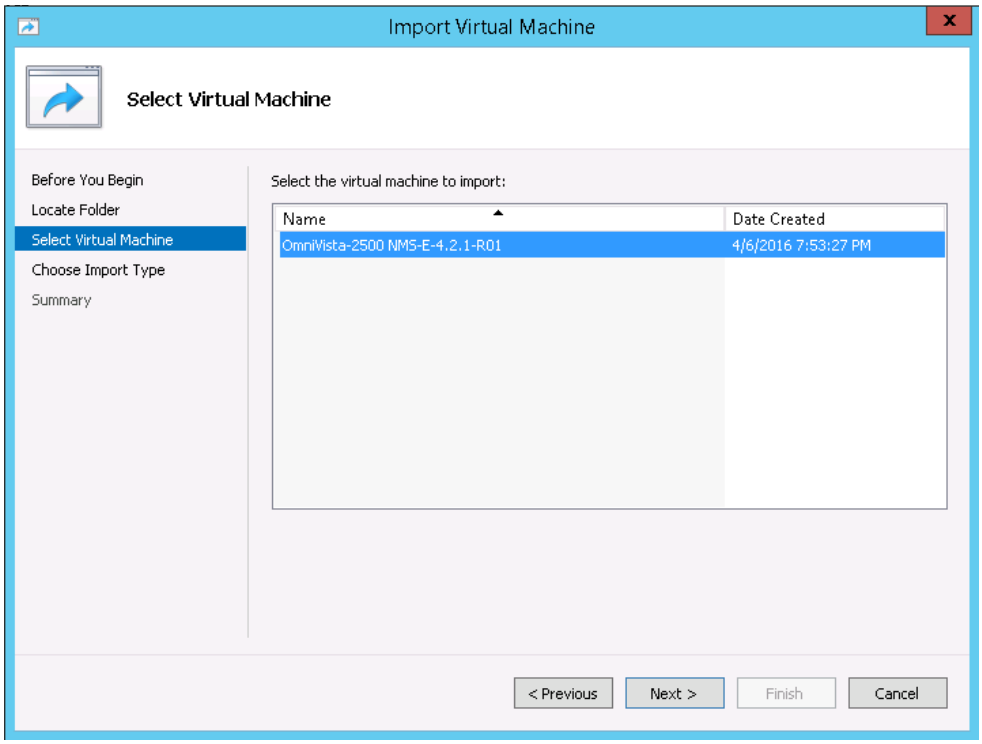
4. The Import Virtual Machine Wizard appears.



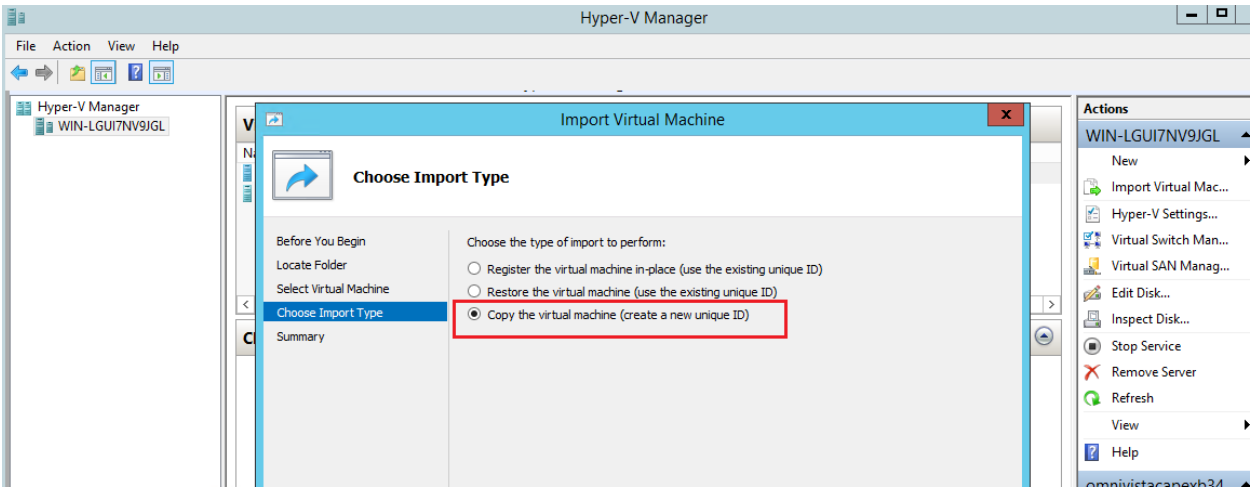
5. Click **Next** to go to the Locate Folder Screen, select the **Folder** that you extracted in Step 1, then click **Next**.



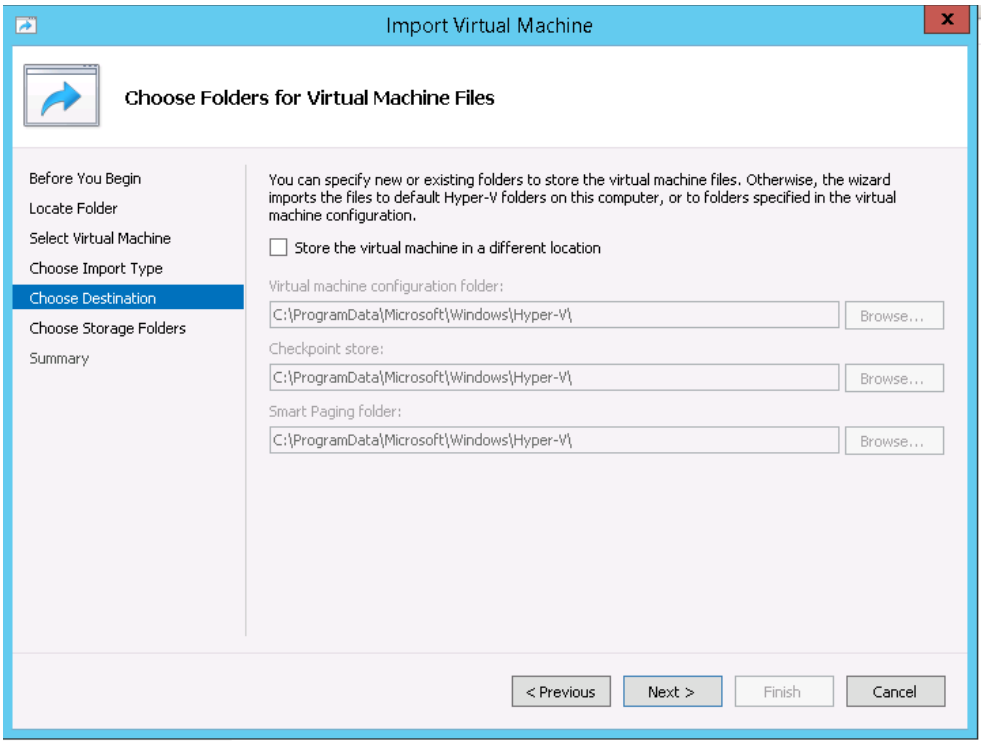
6. Select the Virtual Machine to import, then click **Next**.



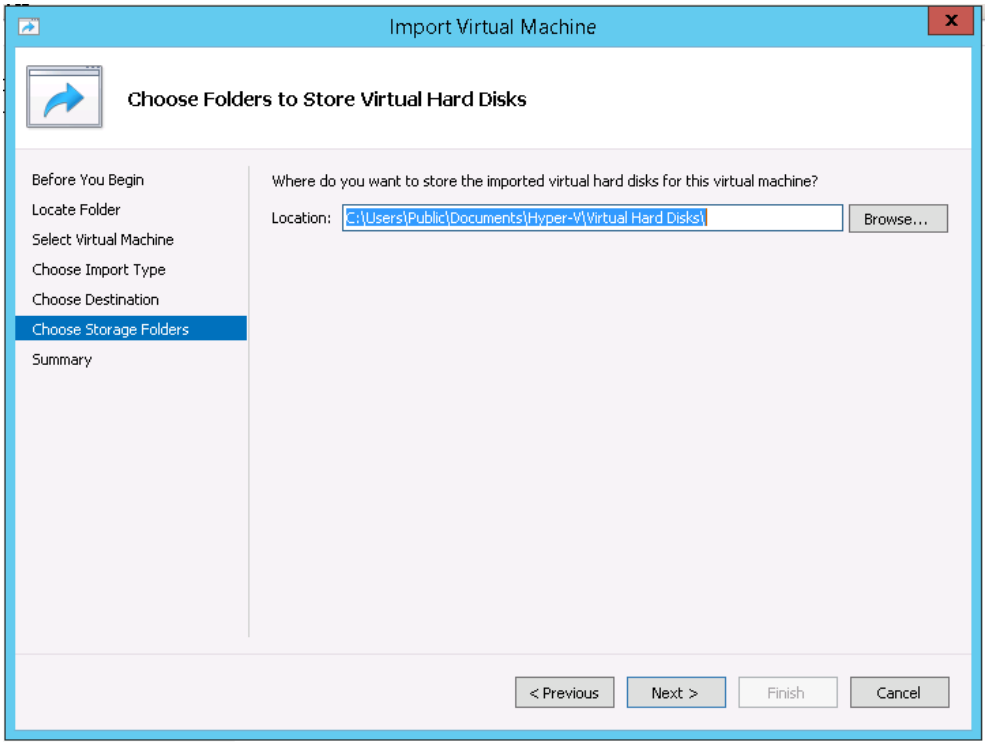
7. Select the default Import Type: **Copy the virtual machine (create a new unique ID)**, then click **Next**.



8. Specify folders to store the Virtual Machine files (or accept the default folders), then click **Next**.

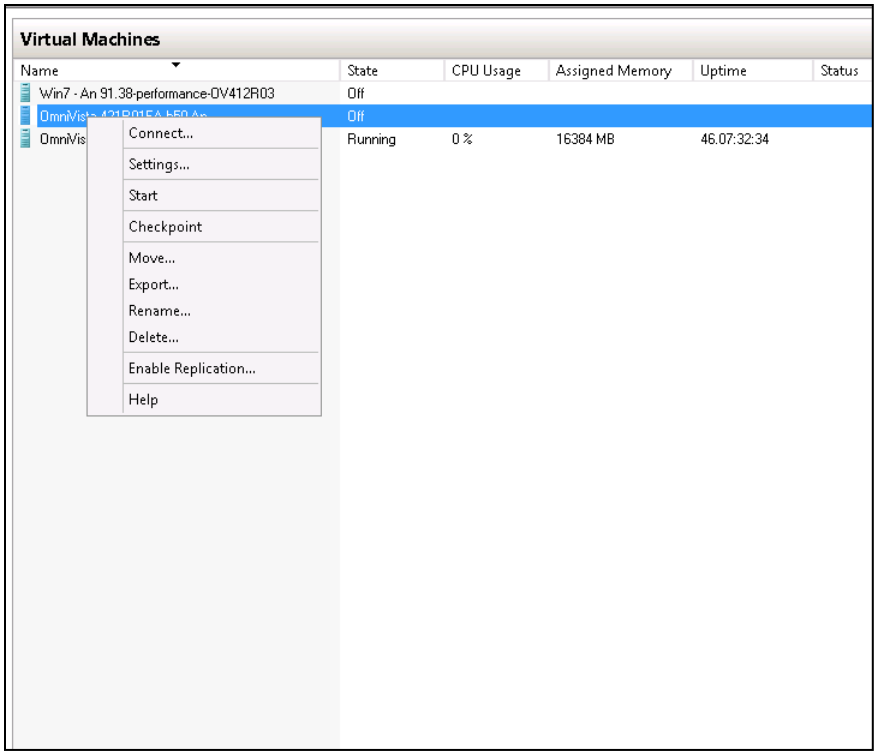


9. Choose folders to store the Virtual Hard Disks or accept the default location and click **Next**.

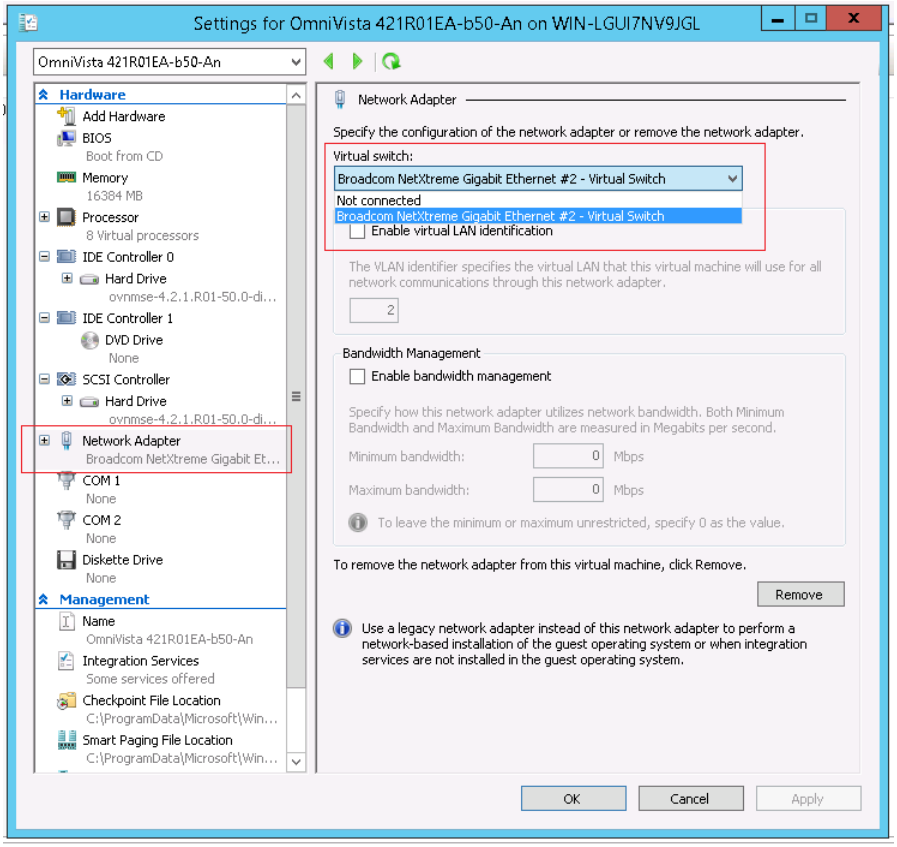


10. Review the import configuration and click **Finish**. (Click **Previous** to return to a screen and make changes.)

11. Configure the Network Adapter. Right-click on the VA and select **Settings**.



12. Select **Network Adapter**, then select the Virtual Switch that you created when you configured Hyper-V.



Once the Virtual Appliance is powered on, go to Completing the OmniVista Installation to complete the installation.

Note: After deploying the OmniVista VM, configure any additional NICs you may need on the VM before Completing the OmniVista Installation.

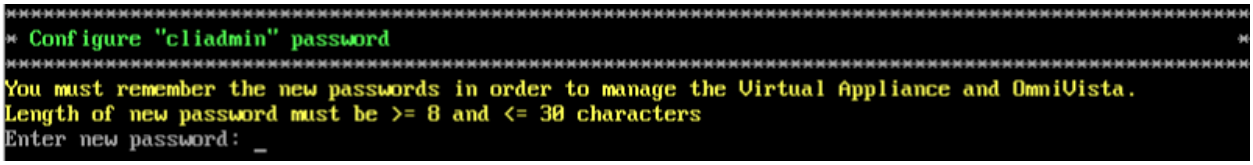
Completing the OmniVista Installation

Follow the steps in the following sections to complete the OV 2500 NMS-E 4.4R2 installation.

1. Launch the Hypervisor Console for the new VM. The Keyboard Layout prompt will appear. Press **Enter** if you do not want to change the default keyboard layout, or enter **y** then press **Enter** to change the default keyboard layout.

The Technical Support Code Password Screen appears.

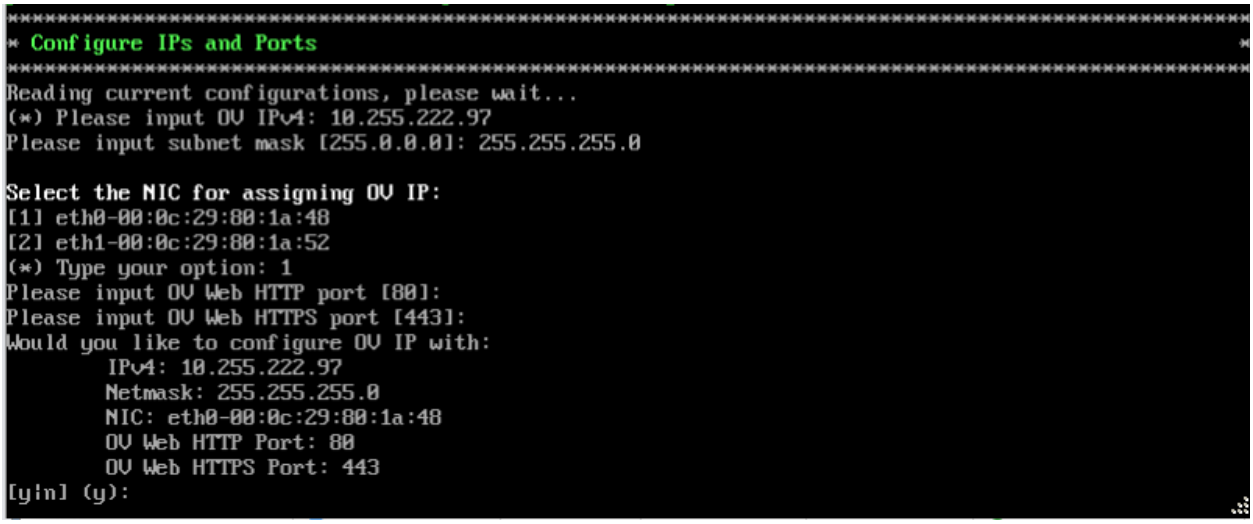
2. Press **Enter**, then enter and confirm a Technical Support Code Password. This is a password that will be used by Technical Support to access the VM, if necessary. The password prompt appears.



3. Specify an administrative password, then re-enter to confirm the new password. Follow the guidelines on the screen when creating the password.

Important Note: Be sure to store the password in a secure place. You will be prompted for the password at the end of the installation. **Lost passwords cannot be retrieved**.

The OV IP address prompt appears. Note that OmniVista supports configuration of three (3) IPs: the OmniVista IP, the Captive Portal IP and an additional OmniVista Web Management IP. These IPs are configured on the Configure IP and Ports Screen.



4. Press **Enter** to configure the OmniVista IP address and mask.

5. Enter an IPv4 address.

6. Enter the IPv4 network mask. If you have more than one NIC configured for the Virtual Machine, you will be prompted to select the NIC to use for the OmniVista IP. Select the NIC and press **Enter**.

7. Enter the OV Web HTTP Port.

8. Enter the OV Web HTTPS Port.

9. Enter **y** and press **Enter** to continue. The Configure Captive Portal IP & Ports prompt appears.

10. Enter **1** and press **Enter** to configure the Configure Captive Portal IP & Ports. If you are not managing a wireless network and will not be using Captive Portal, enter **2** and press **Enter**.

If you select **1** in this step, the Captive Portal IP & Ports configuration must be completed (Steps 11 – 12). If you select **2**, go to Step 13.

```
Configure Captive Portal IP & Ports
[1] Configure new Captive Portal IP & Captive Portal Ports
[2] Disable Captive Portal
(*) Type your option: 1
(*) Please input Captive Portal IPv4: 198.168.0.1
Please input subnet mask [255.255.255.0]:
We have only one unused NIC [eth1-00:0c:29:bc:92:4a], so use it for Captive Portal IP too
Would you like to configure Captive Portal IPv6 [y|n] (n): n
Please input Captive Portal HTTP port [80]: 80
Please input Captive Portal HTTPS port [443]:
Would you like to configure Captive Portal IP with:
        IPv4: 198.168.0.1
        Netmask: 255.255.255.0
        NIC: eth1-00:0c:29:bc:92:4a
        Captive Portal HTTP Port: 80
        Captive Portal HTTPS Port: 443
        IPv6:
        Prefix:
[y|n] (y):
```

11. Enter a Captive Portal IPv4 address and subnet mask. There are three (3) possible Captive Portal configurations:

- The Captive Portal IP is in a different subnet than the OmniVista IP and is assigned to a different NIC. (Recommended)
- The Captive Portal IP is in the same subnet as the OmniVista IP and it is assigned to the same NIC.
- The Captive Portal IP is the same as the OmniVista IP (you must use different ports).

After configuring a Captive Portal IPv4 address, an IPv6 Captive Portal Address prompt appears. Enter **y** and press **Enter** to configure an IPv6 Captive Portal address; otherwise enter **n** and press **Enter** to continue.

12. Enter the Captive Portal HTTP and HTTPS port numbers. The Captive Portal configuration is displayed. Enter **y** and press **Enter** at the confirmation prompt to continue. The following prompt appears.

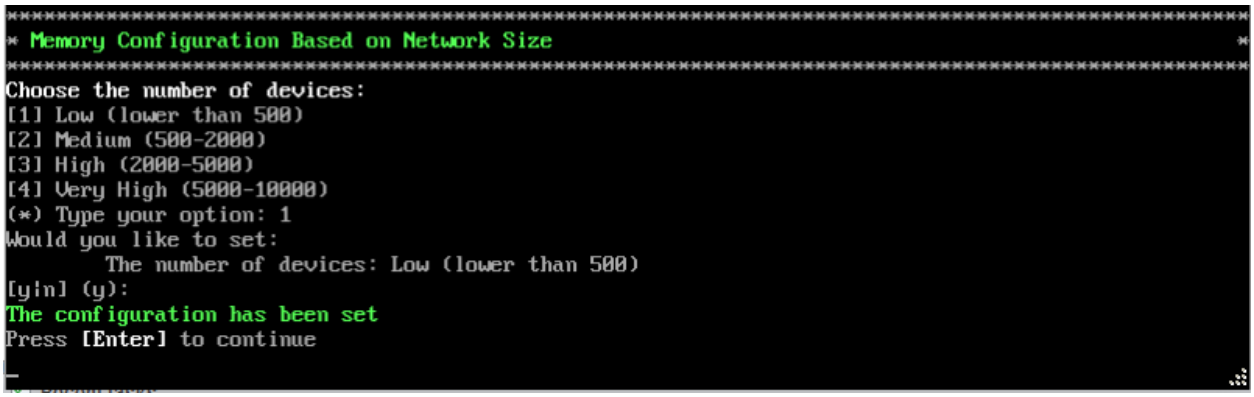
```
Configure Additional OV Web IP
[1] Configure new Additional OV Web IP
[2] Disable Additional OV Web IP
(*) Type your option:
```

13. If you want to configure an additional OV Web IP on a different NIC, enter **1** and press **Enter** to configure the IP address; otherwise, enter **2** and press **Enter**, then enter **y** and press **Enter** at the Confirmation Prompt to continue.

> **Note:** An additional OV Web IP address provides you with another way of accessing the OmniVista UI. The OV Web IP address must be configured on a different NIC and different subnet than the OmniVista IP and Captive Portal IP.

OmniVista will apply the configurations (this may take a minute). When configuration checks are complete, press **Enter** at the Confirmation Prompt to continue.

14. The Memory Configuration Based on Network Size screen is displayed.



Select the number of devices OV 2500 NMS-E 4.4R2 will manage. To select a range, enter its corresponding number at the command prompt (e.g., enter **1** for Low). Ranges include:

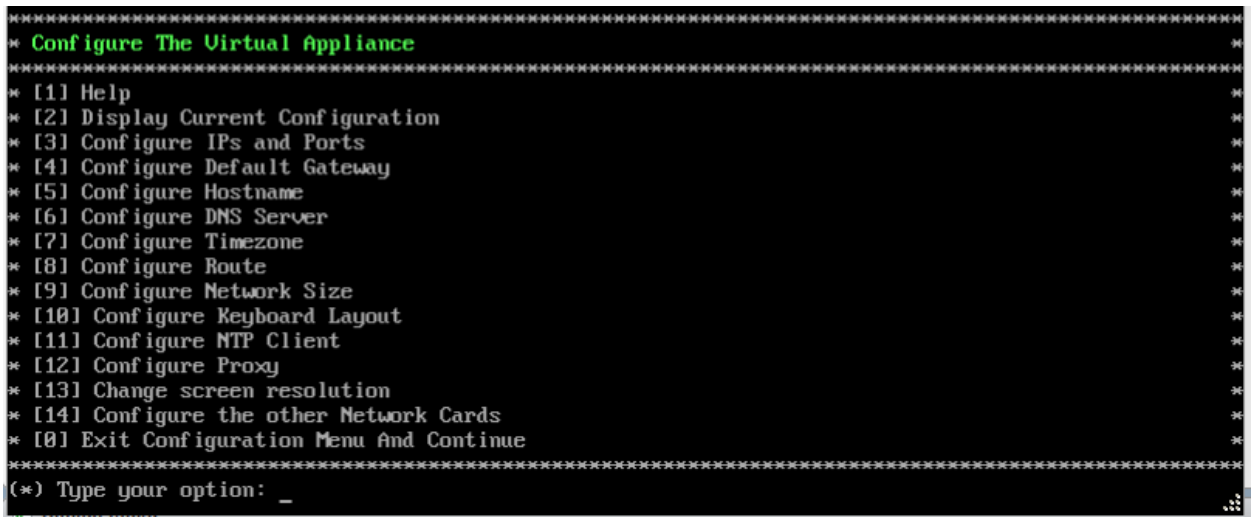
- Low (fewer than 500 devices)
- Medium (500 to 2,000 devices)
- High (2,000 to 5,000 devices)
- Very High (5,000 to 10,000 devices).

Press **Enter**; then enter **y** and press **Enter** at the confirmation prompt. The Default Language Prompt appears.

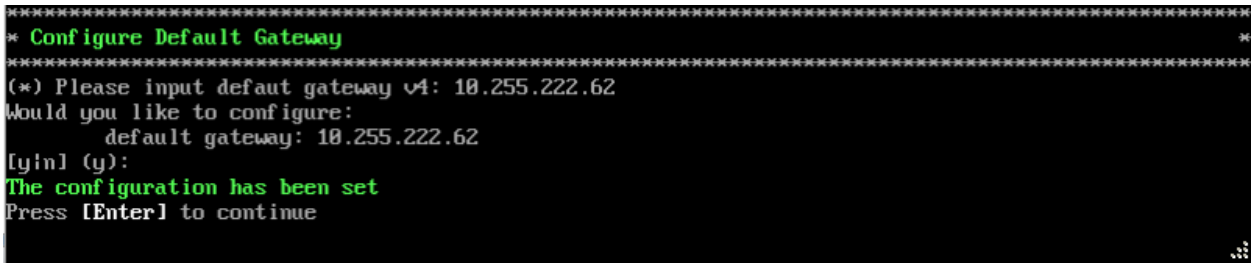
15. Select the default language to be displayed on the OmniVista UI, then press **Enter**. Enter **y** and press **Enter** at the at the Confirmation Prompt. The Configure the Virtual Appliance Menu will appear.

Note that you can always change the UI language display in the Preferences application (Administration – Preferences – User Settings – Locale).

> **Important Note:** Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. Insufficient memory or disk space for the chosen network size may cause OV instability. OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 16GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to Recommended System Configurations for details.
>
> **Important Note:** The High-Availability feature supports up to 2,000 devices. 10,000?

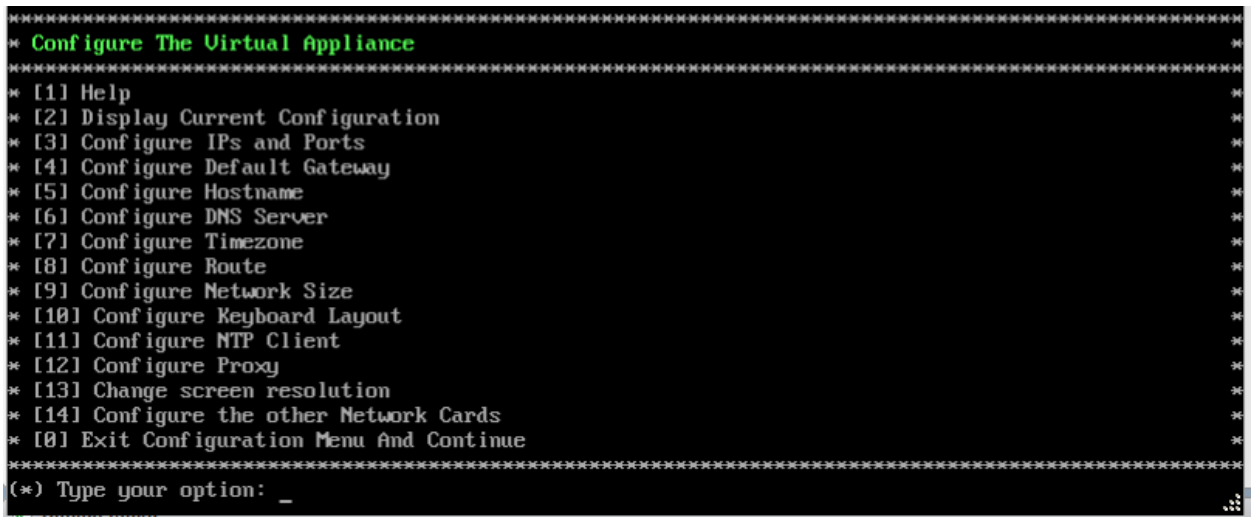


16. Type **4** then press **Enter** to configure the Default Gateway.



17. Enter an IPv4 default gateway IP address.

18. Press **Enter** at the confirmation prompt to set the gateway. Press **Enter** to continue and return to the Configure the Virtual Appliance Menu.



19. Type **0** and press **Enter** to exit the menu and complete the installation. Press **Enter** to continue. OmniVista will display the current configuration and reboot (it takes about a minute to go display the current configuration and start the reboot). When the reboot is complete, the OmniVista Login Screen will appear.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R2 GA
Build Number: 47
Patch Number: 0
Build Date: 10/24/2019
Technical Support Code: alcatel
omnivista login: _
```

20. Log into the VM.

- **omnivista login –** cliadmin
- **password –** Enter the administrative password you created in Step 3.

After successful login, the Virtual Appliance Menu appears.

```
*************************************************************************************************************
* The Virtual Appliance Menu                                                                                *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] Configure The Virtual Appliance                                                                       *
* [3] Run Watchdog Command                                                                                  *
* [4] Upgrade/Backup/Restore VA                                                                             *
* [5] Change Password                                                                                       *
* [6] Logging                                                                                               *
* [7] Login Authentication Server                                                                           *
* [8] Power Off                                                                                             *
* [9] Reboot                                                                                                *
* [10] Advanced Mode                                                                                        *
* [11] Set Up Optional Tools                                                                                *
* [12] Convert to Cluster                                                                                   *
* [13] Join Cluster                                                                                         *
* [0] Log Out                                                                                               *
*************************************************************************************************************
(*) Type your option: _
```

If necessary, you can configure additional settings (e.g., Proxy, DNS) that may be required to access OV 2500 NMS-E 4.4R2. For more information on configuring the VM, see Appendix B – Using the Virtual Appliance Menu.

> **Note:** OV 2500 NMS-E 4.4R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management (PALM). If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.4R2 to connect to these external sites (Port 443):
>
> - **ALE Central Repository -** ovrepo.fluentnetworking.com
> - **AV Repository -** ep1.fluentnetworking.com
> - **PALM -** palm.enterprise.alcatel-lucent.com
> - **Call Home Backend -** us.fluentnetworking.com
> - **Device Fingerprinting Service -** api.fingerbank.org.

21. After completing all required settings, verify that all services are running using the **Run Watchdog Command** in the Virtual Appliance Menu. Select **3**, then press **Enter**, then select **3** and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details.

22. Once all services are running, enter *https://<OVServerIPaddress>* in a supported browser to launch OV 2500 NMS-E 4.4R2.

Note: If you changed the default HTTPs port (8443) during VA configuration, you must enter the port after the IP address (e.g., *https://<OVServerIPaddress>:<HTTPsPort>).*

23. The first time you launch OmniVista you will be prompted to activate the OmniVista License. Import the license file (.dat) or enter the license key to activate the license. You can also activate any additional licenses (e.g., Stellar APs, VM, BYOD) at this time.

Important Note: It is highly-recommended that you change all default user passwords (Admin, Netadmin, Writer, User) after logging into OmniVista for the first time. Go to the **User Management Screen** (Security – Users & User Groups – User) to update the passwords. **Be sure to store the password(s) in a secure place. Lost passwords cannot be retrieved**.

Remember, if you want to configure a High-Availability Installation, you must deploy **two** (2) VMs – one for the Active OmniVista Server (Node 1) and one for the Standby OmniVista Server (Node 2). Make sure to deploy **both** VMs **before** converting them to a High-Availability Installation.

Converting to a High-Availability Installation

After deploying two (2) VMs, you can convert the VMs to a High-Availability (HA) Installation. An HA installation consists of a cluster of two VMs (Node 1 and Node 2), with one node acting as the Active OV Server (Node 1) and the other as a Standby OV Server (Node 2). They are referred to as “Peer Nodes” in the installation process. If Node 1 fails, OmniVista will automatically failover to Node 2. Once you have installed both VMs, you can convert them to a High-Availability Cluster Configuration.

Note:

- You can convert a fresh 4.4R2 Standalone Installation to a 4.4R2 HA Installation.
- You can convert a 4.4R2 Standalone Installation to a 4.4R2 HA Installation if the 4.4.R2 Standalone installation was upgraded from a 4.3R2 Standalone Installation.
- You cannot convert a 4.4R2 Standalone Installation to an HA Installation if the 4.4R2 Standalone Installation was upgraded from a 4.3R1 Standalone Installation.

There are two HA Installation configurations:

- Layer 2 Configuration – In a Layer 2 HA Configuration both OmniVista Server VMs must be on the same subnet. In this configuration, you configure a virtual Cluster IP address. Both the Active and Standby Nodes are reached through the Cluster IP address. Network devices communicate with the Active Node through the Cluster IP address. In the event of a failover, the Standby Node becomes the Active Node and network devices, again, communicate to it through the Cluster IP address.

  Generally, when converting an existing Standalone Installation, you will configure it as a Layer 2 Installation (using the existing OmniVista Server IP address as a virtual Cluster IP address). This will avoid having to re-configuring devices to a new OmniVista Server IP address after the conversion because network devices will still be communicating with OmniVista using the same IP address. During the conversion process, there is an option to assign a new IP address to the existing OmniVista Server. The existing IP address is then available in the next step to configure it as the Cluster IP address.

  Important Note: Stellar APs are **only** supported in a Layer 2 HA Configuration. If you are using Stellar APs, you must use a Layer 2 HA Configuration.

- Layer 3 Configuration – In a Layer 3 HA Configuration the OmniVista Server VMs are on different subnets, with a unique IP address for each server. Network devices can communicate with both VMs (Active and Standby Nodes). Network devices communicate with the Active Node. In the event of a failover, devices automatically communicate with the new Active Node. You can convert an existing Standalone Installation to a Layer 3 Installation; however, you will have to re-configure network devices to communicate with both Nodes. Make sure network devices can communicate with **both** nodes (Active and Standby).

  Important Notes:

  - Features or functions that require devices to contact OmniVista are **not** supported in a Layer 3 Configuration (e.g., sFlow, Policy). This includes:
    - Analytics Top N Applications and Top N Clients Reports
    - AP Registration
    - Groups
    - PolicyView
    - Syslog
    - Unified Policy
    - UPAM.

Notes:

- The Hypervisor's on which you are installing OmniVista must have the latest Network Adaptor drivers:
  - Hyper-V:
    - Broadcom: Version b57nd60a.sys version 16.8 and later.
    - HP: Version 16.8 and later.
  - VMware:
    - Broadcom: Version Tg3-3.133d.v55.1-101300361 and later.
- The recommended network bandwidth is 1Gbps. The recommended network latency is 1ms.
- You must have a High-Availability License to enable the High Availability Feature. After you complete the installation, the first time you open OmniVista in a browser, you will be prompted to activate the OmniVista License and the High-Availability License.

To configure the Cluster, you will need IP addresses for the following:

- **Node 1 –** This is the physical IP address of the Active Node (Node 1).
- **Node 2 –** This is the physical IP address of the Standby Node (Node 2).
- **Cluster IP Address (Layer 2 Installation Only) –** This is a virtual IP address that is used to communicate with the network (and with the Active and Standby Nodes).

  Important Note: Make sure to plan the Cluster IP address, Node IP addresses and Hostnames carefully and have them available for reference throughout the installation process for both VMs (Node 1 and Node 2).
- **Captive Portal Virtual IP Address (Layer 2 Configuration Only) –** This IP address is needed if you want to use Captive Portal in HA Cluster Mode (Layer 2 Configuration). This virtual IP address is used to communicate with the network (and with the Active and

Standby Nodes) when you use the Captive Portal. This IP address must be on the same subnet as the Static Captive Portal IP address.

- **Additional OV Web Virtual IP (Layer 2 Configuration Only) –** This optional additional OV Web Virtual IP provides you with another way of accessing the OmniVista UI. The OV Web Virtual IP address must be on the same subnet as the static OV Web IP address.

Layer 2 Configuration

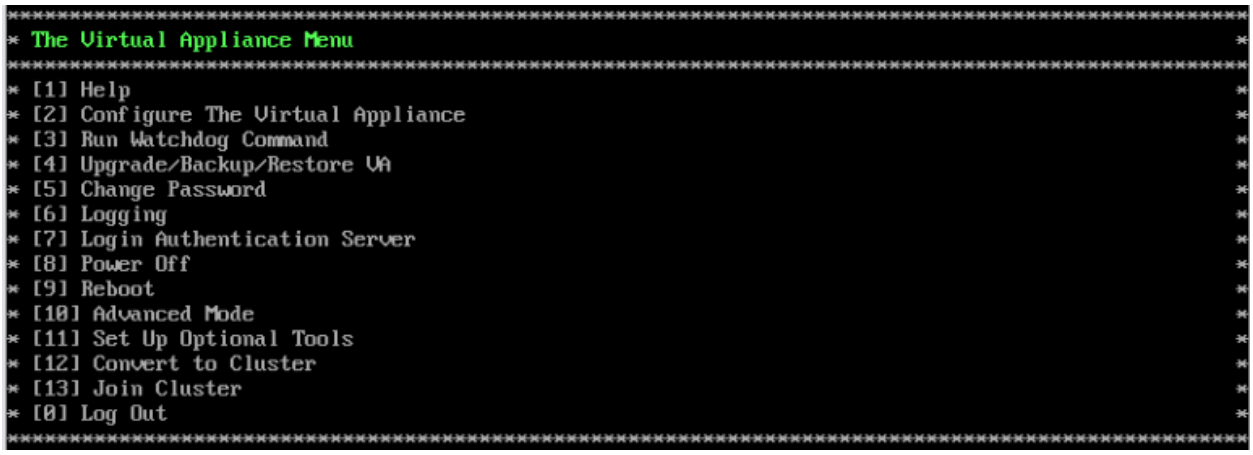
In a Layer 2 HA Configuration both OmniVista Server VMs must be on the same subnet. In this configuration, you configure a virtual Cluster IP address. Both the Active and Standby Nodes are reached through the Cluster IP address. Converting a Layer 2 HA Configuration consists of the following steps:

- Converting Node 1 to Cluster Mode
- Joining Node 2 to the Cluster
- Verifying the Conversion
- Logging Into the OmniVista UI

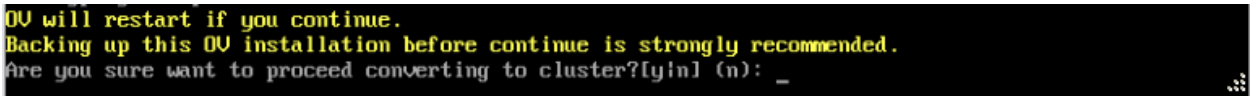
Converting Node 1 to Cluster Mode

First, convert Node 1 to Cluster Mode. If you are converting an existing 4.4R2 Standalone Installation, these steps are performed on the existing Standalone VM.

1. Launch a Hypervisor Console on the VM you want to configure as Node 1 and log in. The Virtual Appliance Menu will appear.



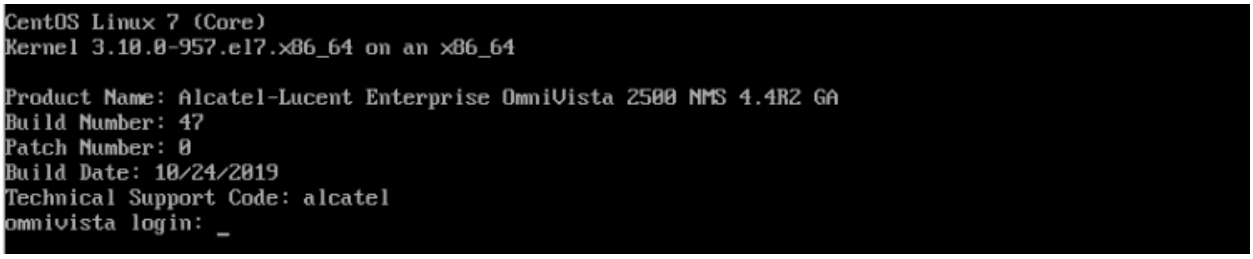
2. On the Virtual Appliance Screen, enter **12** (Convert to Cluster) and press **Enter**. The following Warning Prompt will appear:



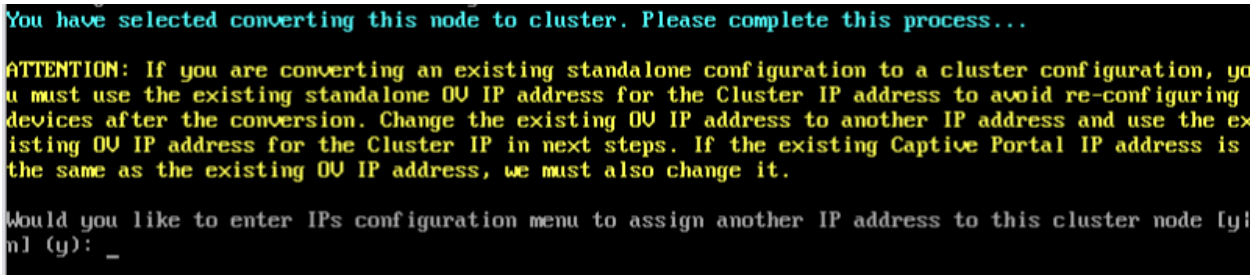
3. Enter **y** and press **Enter** to continue. A second Warning Prompt will appear.

4. Press **Enter** to continue. The VM will reboot. (The screen will go black for about 30 seconds before displaying the reboot progress.) The process will continue for some time in the background while the rebooting screen is displayed (the screen may appear to be “stuck” on the reboot progress display). It can take up to 15 – 20 minutes for the process to complete. When it completes, the VM configuration will be displayed, followed by the Login Screen.

> **Important Note:** Do **not** attempt to log into the VM through SSH while the process is running. Wait for it to complete and login to the VM through the Hypervisor Console when the Login Screen is displayed.

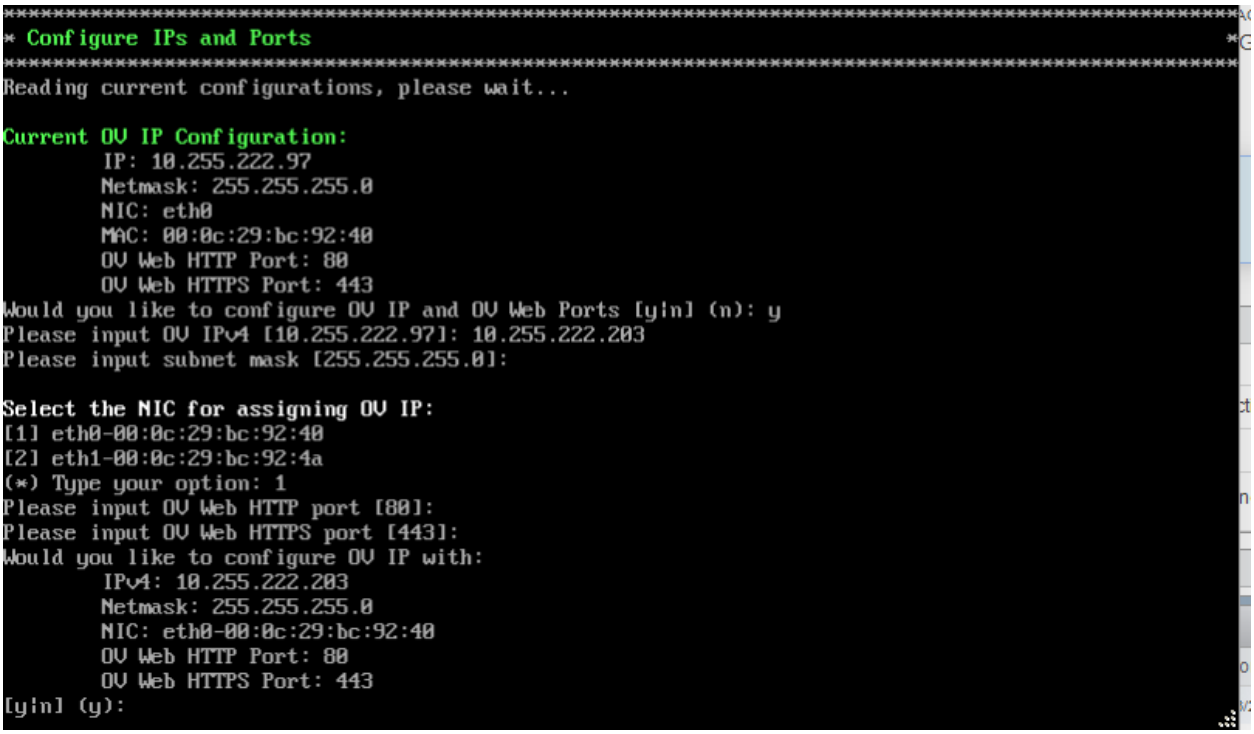


5. When the process is complete, log into the VM. The following screen will appear.



Here you are given the option of re-configuring the current Node’s IP address. What you are doing in this step is configuring a new physical IP address for the current Node (e.g., 10.255.222.203); and freeing up the current IP address (10.255.222.97) to be used as the virtual Cluster IP address (Step 9). Network devices will then communicate with the virtual Cluster IP address.

6. Enter **y** and press **Enter** to re-configure the current Node’s IP address and ports. The current configuration is displayed and you are prompted for a new IP address. Enter **y** and press **Enter** at the prompt and enter a new IP address (e.g., 10.255.222.203). (If you have multiple NICs installed on the VM you will be prompted to select the NIC. Select the same NIC on which you configured the original IP address.) Enter a subnet mask, and ports for the current Node, enter **y** and press **Enter** at the Confirmation Prompt.



7. You are prompted to configure Captive Portal IP and Ports. If you have already configured Captive Portal on the Node, the current Captive Portal IP configuration is displayed. If you do not want to configure Captive Portal, enter **n** and press **Enter**. To configure Captive Portal IP and Ports enter **y** and press **Enter**.

By default, if you previously configured Captive Portal on the Node, the existing Captive Portal IP address and default ports are prefilled with the address and ports. Press **Enter** to accept the defaults).

```
Current Captive Portal IP Configuration:
        IPv4: 198.168.0.1
        Netmask: 255.255.255.0
        NIC: eth1
        MAC: 00:0c:29:bc:92:4a
        Captive Portal Web HTTP Port: 80
        Captive Portal Web HTTPS Port: 443
        IPv6:
        Prefix:

Important Note: Modifying the Captive Portal IP Address in the VA Menu will not update the existing
configuration on devices. You must modify the Global Settings in the UI on the Global Configuration
- Settings page (Unified Access - Unified Profile - Template - Global Configuration - Setting) and a
pply the new setting to devices.

Would you like to configure Captive Portal IP and Ports [y|n] (n): y

Configure Captive Portal IP & Ports
[1] Configure new Captive Portal IP & Captive Portal Ports
[2] Disable Captive Portal
(*) Type your option: 1
Please input Captive Portal IPv4 [198.168.0.1]:
Please input subnet mask [255.255.255.0]:
We have only one unused NIC [eth1-00:0c:29:bc:92:4a], so use it for Captive Portal IP too
Would you like to configure Captive Portal IPv6 [y|n] (n):
Please input Captive Portal HTTP port [80]:
Please input Captive Portal HTTPS port [443]:
Would you like to configure Captive Portal IP with:
        IPv4: 198.168.0.1
        Netmask: 255.255.255.0
        NIC: eth1-00:0c:29:bc:92:4a
        Captive Portal HTTP Port: 80
        Captive Portal HTTPS Port: 443
        IPv6:
        Prefix:
[y|n] (y): _
```

Important Note: If Captive Portal was already configured on the Node you are converting, it is **recommended that you keep the existing configuration**. If you do change the existing Captive Portal configuration, you must manually re-configure all Captive Portal related device configurations (including the Global Settings in the Unified Profile application).

8. If there is an additional OV Web IP configuration on the Node, it will be displayed. If an additional OV Web Configuration does not exist for the Node you can enter **y** and press **Enter** to configure it, or just press **Enter** to continue.

```
Current Additional OV Web IP Configuration:
        IP:
        Netmask:
        NIC:
        MAC:
Would you like to configure Additional OV Web IP [y|n] (n):
```

OmniVista will apply the new configurations. This may take several minutes. When complete, the following prompt will appear.

```
Configurations has been affected.
Press [Enter] to continue
```

9. Press **Enter** to continue. The Hostname Configuration Prompt will appear.

```
This cluster node must have unique hostname among all other nodes in the same cluster.
Do you want to assign new hostname for this node? [y|n] (y):
```

10. Enter y and press **Enter** to continue. The Configure Hostname Screen will appear.

```
**********************************************************************************************************
* Configure Hostname                                                                                     *
**********************************************************************************************************
Please input hostname [omnivista]: ov1
Would you like to configure:
        hostname: ov1
[y|n] (y):
The configuration has been set
Press [Enter] to continue
```

11. Enter a Hostname for Node 1 and press **Enter**. The Hostname can be up to 15 characters, but must be lower case ("ov1" **not** "OV1"). Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** again to continue. After several minutes, the Cluster Name prompt will appear.

```
(*) Please input Cluster Name: ovcluster
Would you like to configure:
        Cluster Name: ovcluster
[y|n] (y): _
```

12. Enter a Cluster Name (e.g., ovcluster), enter **y**, then press **Enter**. The following prompt will appear.

```
Would you like to configure OV Virtual IP address [y|n] (y): _
```

13. Enter **y** and press **Enter**. The current IP configuration of the Node is displayed and you are prompted to enter the Cluster Virtual IP (the previous IP address of Node 1 – e.g., 10.255.222.97). Enter the IP address and press **Enter**, then enter **y** and press **Enter** at the Confirmation Prompt.

```
Current OV IP Configuration:
        IP: 10.255.222.203
        Netmask: 255.255.255.0
Would you like to configure OV Virtual IP address [y|n] (y):
(*) Please input OV Virtual IP address: 10.255.222.97
Would you like to configure OV Virtual IP:
        IP address: 10.255.222.97
[y|n] (y): _
```

If you have Captive Portal configured on the Node, the Current Captive Portal IP Configuration is displayed, and you are prompted to enter the Captive Portal Virtual IP address.

```
Current Captive Portal IP Configuration:
        IP: 198.168.0.1
        Netmask: 255.255.255.0
(*) Please input Captive Portal Virtual IP address: 198.168.0.3
Would you like to configure Captive Portal Virtual IP:
        IP address: 198.168.0.3
[y|n] (y):
```

14. Enter the Virtual Captive Portal Virtual IP address at the prompt (e.g., 198.168.0.3). It must be on the same subnet at the Current Captive Portal.

If you have a Captive Portal IP v6 configuration or an additional OV Web IP configuration, you will be prompted to configure the virtual IP addresses for each. Otherwise, the conversion process will start with the progress displayed at the bottom of the screen (the process can take 15 – 20 minutes).

```
Current Captive Portal IPv6 Configuration:
        IP:
        Netmask:
Captive Portal static IPv6 isn't configured, so skip configuring Captive Portal Virtual IPv6!


Current Additional OV Web IP Configuration:
        IP:
        Netmask:
Additional OV Web static IP isn't configured, so skip configuring Additional OV Web Virtual IP!

Initializing (step 1/3).....................................................................0%
Initializing (step 1/3)....................................................................100%
Converting to cluster (step 2/3) ...........................................................37 5%
```

After the process completes (Initializing Steps 1 – 3 each reach 100%), the following prompt will appear.

```
Creating cluster is completed. Please access peer node and select 'join cluster'.
You must logout and re-login to use the HA administrator menu. Press enter to log out now.
```

15. Press **Enter** to bring up the Login Screen.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R2 GA
Build Number: 47
Patch Number: 0
Build Date: 10/24/2019
Technical Support Code: alcatel
ov1 login:
```

16. Log into the VM. The HA Virtual Appliance Menu will appear.

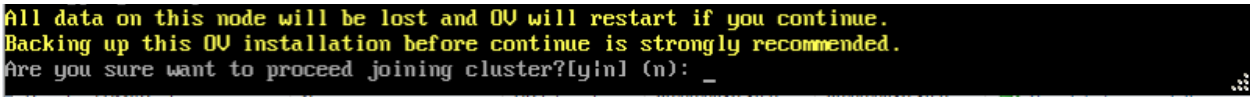
```
*****************************************************************************************************
* The HA Virtual Appliance Menu                                                                     *
*****************************************************************************************************
* [1] Help                                                                                          *
* [2] Show OV Cluster Status                                                                        *
* [3] Configure Cluster                                                                             *
* [4] Configure Current Node                                                                        *
* [5] Run Watchdog Command                                                                          *
* [6] Upgrade/Backup/Restore VA                                                                     *
* [7] Logging                                                                                       *
* [8] Setup Optional Tools                                                                          *
* [9] Advance Mode                                                                                  *
* [10] Power Off                                                                                    *
* [11] Reboot                                                                                       *
* [0] Log Out                                                                                       *
*****************************************************************************************************
```

Node 1 is now in High-Availability (Cluster) Mode. Join Node 2 to the Cluster as described below.

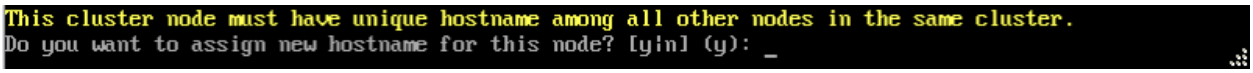
Joining Node 2 to the Cluster

1. Launch a Hypervisor Console on the VM you want to configure as Node 2.

2. On the Virtual Appliance Screen, enter **13** (Join Cluster) and press **Enter**. The following Warning Prompt will appear:



3. Enter **y** and press **Enter** to continue. The Cluster Hostname Prompt will appear.

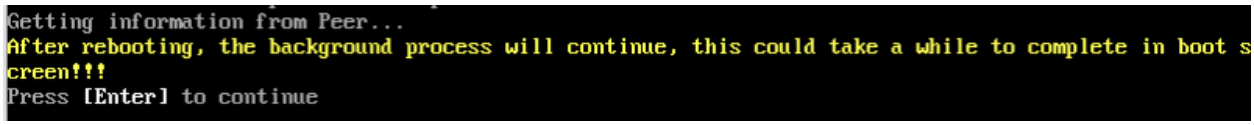


4. Enter **y** and press **Enter** to continue. The Configure Hostname Screen appears.

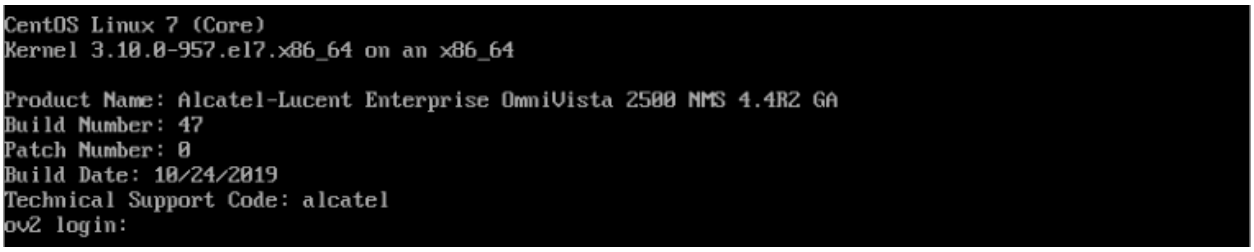
5. Enter a Hostname for Node 2 and press **Enter**. The Hostname can be up to 15 characters, but must be lower case ("ov2" **not** "OV2"). Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** again to continue. After a couple of minutes, the Configure Peer Node's Information Screen appears.

6. Enter the physical IP address of Node 1. This is the new physical IP address you assigned to Node 1 in Step 6 of the previous section (e.g., 10.255.222.203), then enter **y** and press **Enter** to confirm.

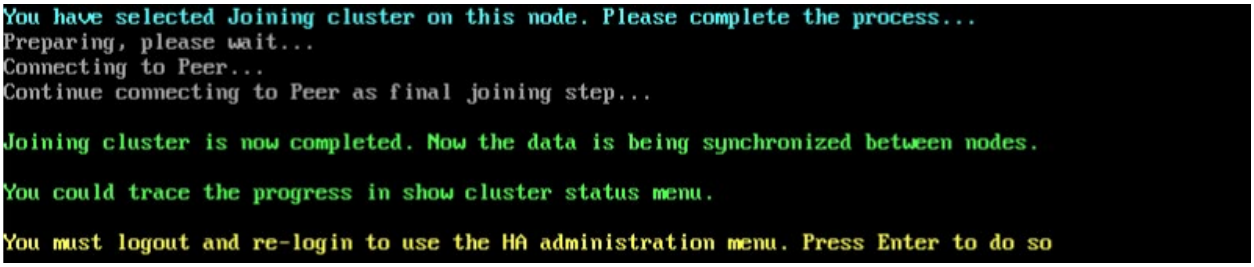
7. At the “Cluster Password” prompt, enter the “cliadmin” password for Node 1. The following prompt will appear.



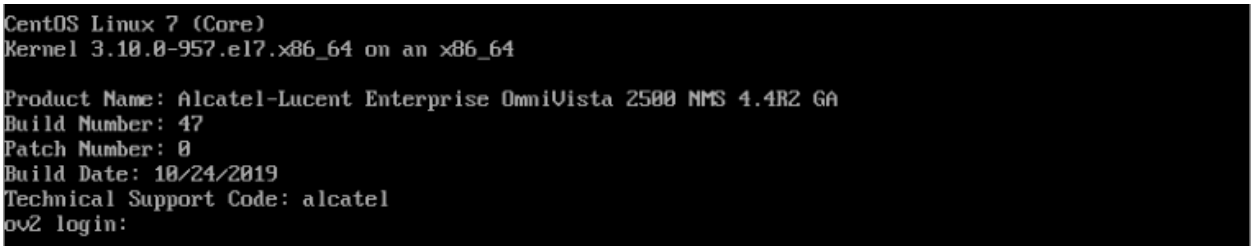
8. Press **Enter** to continue. The VM will reboot. It can take up to 5 – 10 minutes for the process to complete. When it completes, the VM configuration will be displayed, followed by the Login Screen.



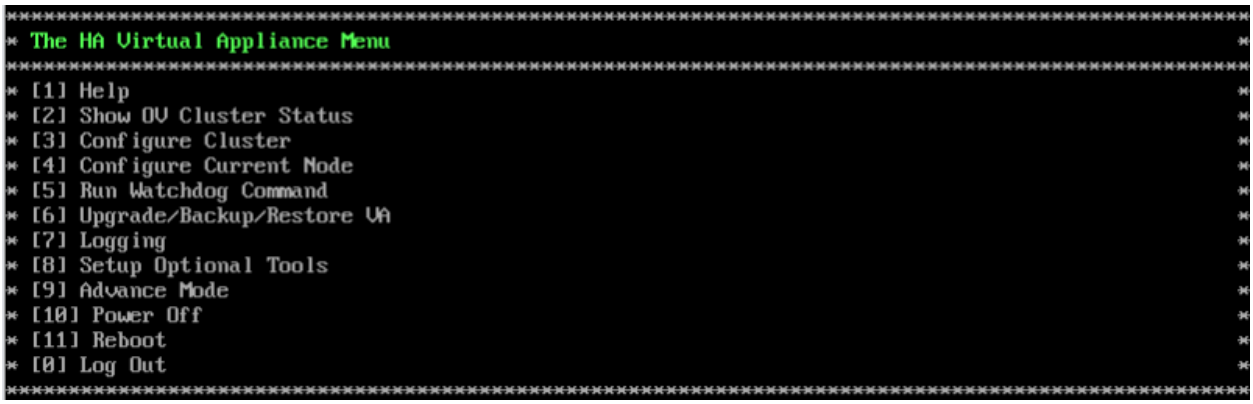
9. Log into the VM. The following screen will appear, showing the progress of the conversion process on Node 2. The process can take up to 10 minutes.



10. When the process is complete, you will be prompted to press **Enter** to logout and login (as shown above). Press **Enter** at the prompt. The Login Screen will appear.



11. Log into the VM. The HA Virtual Appliance Menu Screen will appear.



The High-Availability Conversion Process in now complete. Verify the configuration as described below.

Verifying the Conversion

1. Verify that all services are running on Node 1:

- Go to the HA Virtual Appliance Menu of Node 1.
  - Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details.

2. Verify that all services are running on Node 2:

- Go to the HA Virtual Appliance Menu of Node 2.
  - Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details. Note that on Node 2, all services should be running except upam and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”.

3. Check the Cluster status on Node 1.

- Go to the HA Virtual Appliance Menu of Node 1.
  - Enter **2** (Show OV Cluster Status) the press **Enter**. See Show OV Cluster Status for more information.

Logging into the OmniVista UI

1. Once all services are running, enter *https://<ClusterIPaddress>* in a supported browser to launch OV 2500 NMS-E 4.4R2.

> **Note:** If you changed the default HTTPs port (443) during VA configuration, you must enter the port after the IP address (e.g., *https://<IPaddress>:<HTTPsPort>).*

2. The first time you launch OmniVista you will be prompted to activate the OmniVista License (fresh installation) and the High-Availability License. Import the license file (.dat) or enter the license key to activate the license(s). You can also activate any additional licenses (e.g., Stellar APs, VM, BYOD) at this time.

> **Important Note:** It is highly-recommended that you change all default user passwords (Admin, Netadmin, Writer, User) after logging into OmniVista for the first time. Go to the **User Management Screen** (Security – Users & User Groups – User) to update the

passwords. **Be sure to store the password(s) in a secure place. Lost passwords cannot be retrieved**.

Layer 3 Configuration

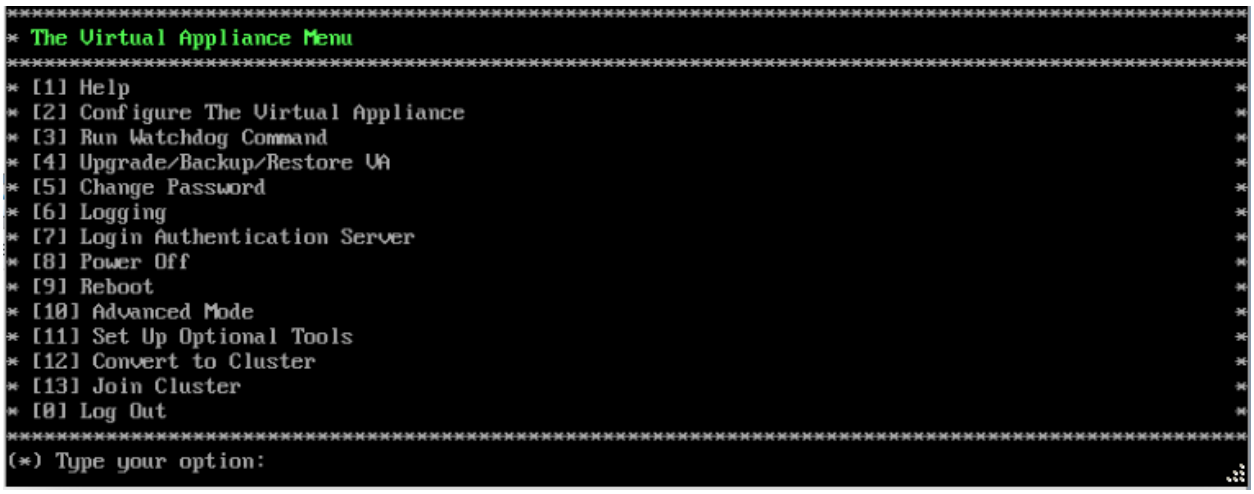
In a Layer 3 HA Configuration the OmniVista Server VMs are on different subnets. Network devices then communicate with both VMs (Active and Standby Nodes) simultaneously. You can convert an existing Standalone Installation to a Layer 3 Installation; however, you will have to re-configure network devices to communicate with both Nodes. Converting a Layer 3 HA Configuration consists of the following steps:

- Converting Node 1 to a Cluster Configuration
- Joining Node 2 to the Cluster
- Verifying the Conversion
- Logging Into the OmniVista UI

Converting Node 1 to Cluster Mode

First, convert Node 1 to Cluster Mode. If you are converting an existing 4.4R2 Standalone Installation, these steps are performed on the existing Standalone VM.

1. Launch a Hypervisor Console on the VM you want to configure as Node 1 and log in. The Virtual Appliance Menu will appear.

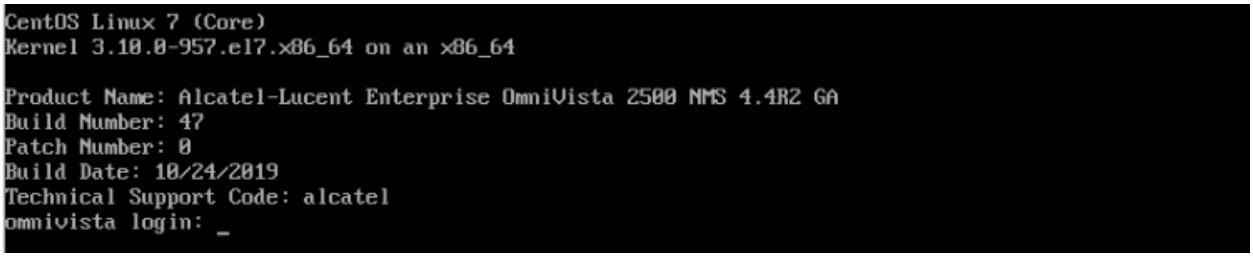


2. On the Virtual Appliance Screen, enter **12** (Convert to Cluster) and press **Enter**. The following Warning Prompt will appear:

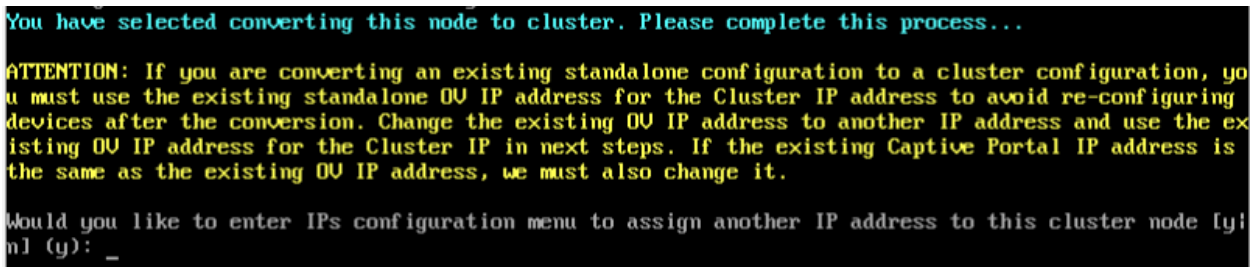
3. Enter **y** and press **Enter** to continue. A second Warning Prompt will appear.

4. Press **Enter** to continue. The VM will reboot. It can take up to 15 – 20 minutes for the process to complete. When it completes, the VM configuration will be displayed, followed by the Login Screen.

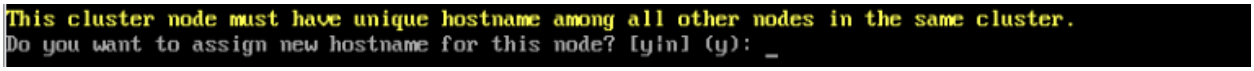
Important Note: Do **not** attempt to log into the VM through SSH while the process is running. Wait for it to complete and login to the VM through the Hypervisor Console when the Login Screen is displayed.



5. Log into the VM. The following screen will appear.



6. Enter **n** and press **Enter** to continue with the installation. The Hostname Prompt will appear.



7. Enter **y** and press **Enter**. The Configure Hostname Screen will appear.

8. Enter a Hostname for Node 1 and press **Enter**. The Hostname can be up to 15 characters, but must be lower case (“ov1” **not** “OV1”). Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** again to continue. After several minutes, the Cluster Name Prompt will appear.

9. Enter a Cluster Name, enter **y**, then press **Enter**. The following prompt will appear.

```
Current OV IP Configuration:
        IP: 10.255.222.98
        Netmask: 255.255.255.0
Would you like to configure OV Virtual IP address [y|n] (y): _
```

10. Enter **n**, press **Enter**, then enter **y** and press **Enter** again at the Confirmation Prompt. Note that if you are converting from an existing Standalone Installation and were using a Captive Portal, it will be disabled in a Layer 3 Configuration. The process will start with the progress displayed at the bottom of the screen (the process can take 10 – 15 minutes).

```
Current Captive Portal IP Configuration:
        IP: 198.168.0.2
        Netmask: 255.255.255.0
OV Virtual IP isn't configured, so skip configuring Captive Portal Virtual IP!


Current Captive Portal IPv6 Configuration:
        IP:
        Netmask:
Captive Portal Virtual IPv4 isn't configured, so skip configuring Captive Portal Virtual IPv6!


Current Additional OV Web IP Configuration:
        IP:
        Netmask:
OV Virtual IP isn't configured, so skip configuring Additional OV Web Virtual IP!

Initializing (step 1/3).....................................................................0%
Initializing (step 1/3).....................................................................67%
```

After the process completes (Initializing Steps 1 – 3 each reach 100%), the Login Screen will appear. (You may have to press **Enter** to display the Login Screen **after** the process completes.)

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R2 GA
Build Number: 47
Patch Number: 0
Build Date: 10/24/2019
Technical Support Code: alcatel
ov1 login:
```

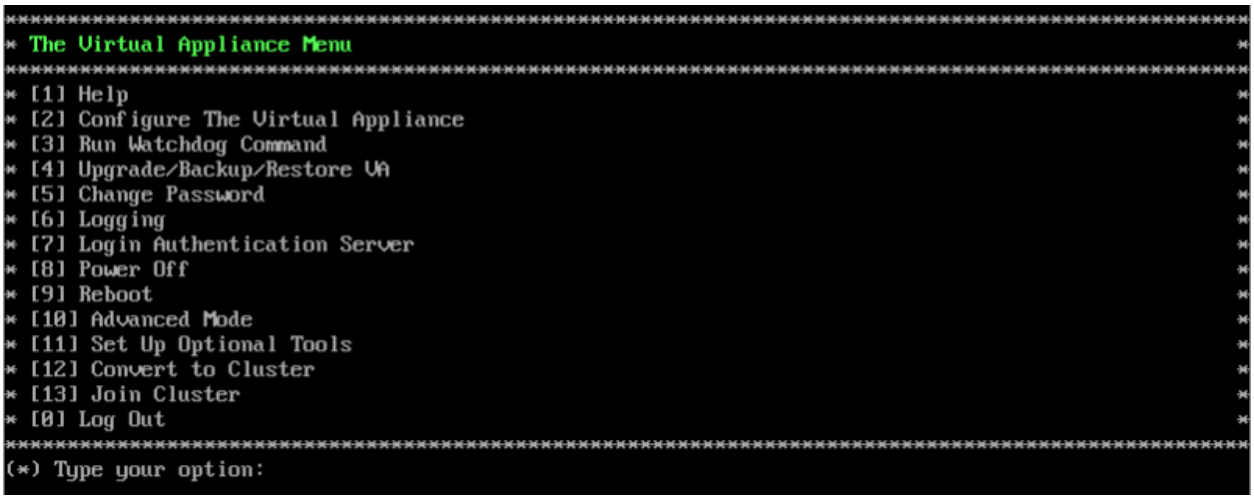
11. Log into the VM. The HA Virtual Appliance Menu will appear.

```
*****************************************************************************************************
* The HA Virtual Appliance Menu                                                                     *
*****************************************************************************************************
* [1] Help                                                                                          *
* [2] Show OV Cluster Status                                                                        *
* [3] Configure Cluster                                                                             *
* [4] Configure Current Node                                                                        *
* [5] Run Watchdog Command                                                                          *
* [6] Upgrade/Backup/Restore VA                                                                     *
* [7] Logging                                                                                       *
* [8] Setup Optional Tools                                                                          *
* [9] Advance Mode                                                                                  *
* [10] Power Off                                                                                    *
* [11] Reboot                                                                                       *
* [0] Log Out                                                                                       *
*****************************************************************************************************
(*) Type your option: _
```

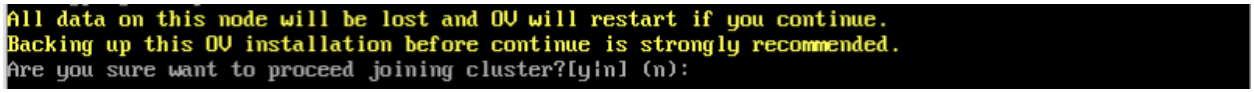
Node 1 is now in High-Availability (Cluster) Mode. Join Node 2 to the Cluster as described below.

Joining Node 2 to the Cluster

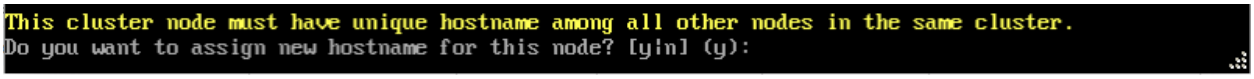
1. Launch a Hypervisor Console on the VM you want to configure as Node 2.



2. On the Virtual Appliance Screen, enter **13** (Join Cluster) and press **Enter**. The following Warning Prompt will appear:

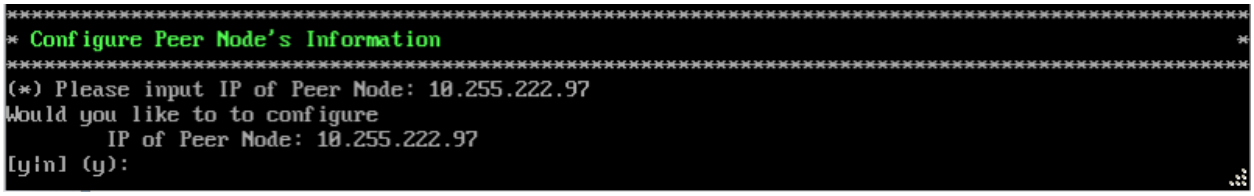


3. Enter **y** and press **Enter** to continue. The Hostname Prompt appears.



4. Enter **y** and press **Enter**. The Configure Hostname Screen appears.

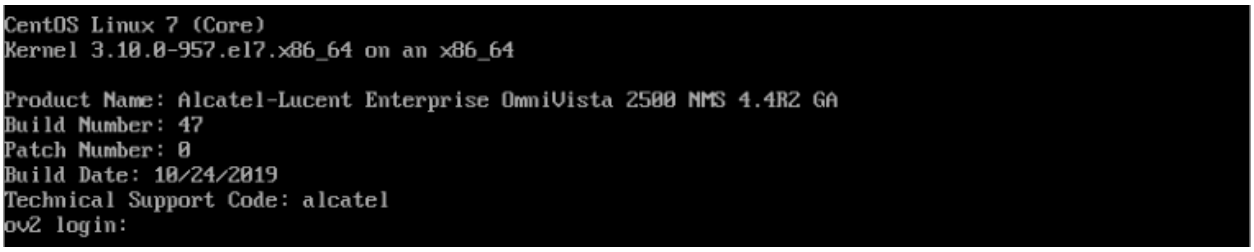
5. Enter a Hostname (up to 15 characters) for Node 1 and press **Enter**. Enter **y** and press **Enter** at the Confirmation Prompt, then press Enter again to continue. Note that the Hostname **must** be in lower case letters (e.g., “ov2” **not** “OV2”). The Configure Peer Node’s Information Screen appears.



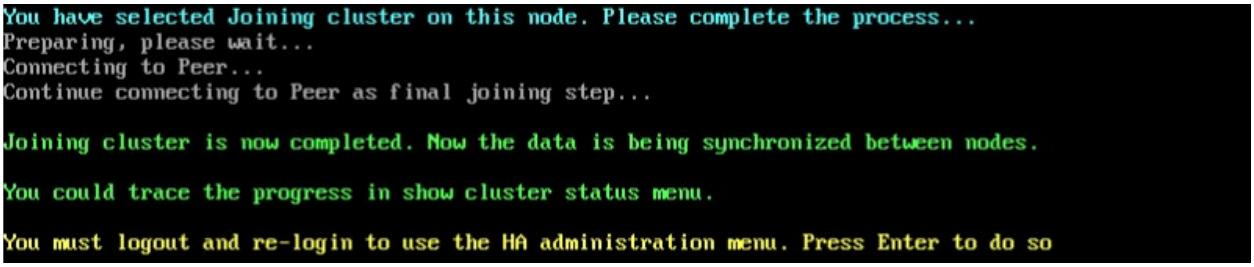
6. Enter the IP address of Node 1 (e.g., 10.255.222.97), then enter **y** and press **Enter** to confirm.

7. At the “Cluster Password” prompt, enter the “cliadmin” password for Node 1. The following Confirmation prompt will appear.

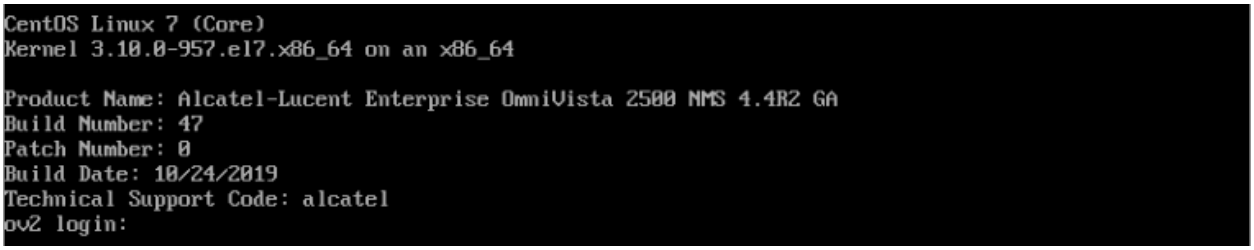
8. Press **Enter** to continue. The VM will reboot. (The screen will go black for about 10 seconds before displaying the reboot progress.) The process will continue for some time in the background while the rebooting screen is displayed (the screen may appear to be “stuck” on the reboot progress display). It can take up to 5 – 10 minutes for the process to complete. When it completes, the VM configuration will be displayed, followed by the Login Screen.



9. Log into the VM. The following screen will appear, showing the progress of the conversion process on Node 2.



10. When the process is complete, you will be prompted to press **Enter** to logout and login (as shown above). Press **Enter** at the prompt. The Login Screen will appear.



11. Log into the VM. The HA Virtual Appliance Menu Screen will appear.

The High-Availability Conversion Process in now complete. Verify the configuration as described below.

Verifying the Conversion

1. Verify that all services are running on Node 1:

- Go to the HA Virtual Appliance Menu of Node 1.
  - Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details.

2. Verify that all services are running on Node 2:

- Go to the HA Virtual Appliance Menu of Node 2.
  - Enter **5** (Run Watchdog Command) then press **Enter**. Enter **2** (Display Status of All Services) and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details. Note that on Node 2, all services should be running except upam and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”.

3. Check the Cluster status on Node 1.

- Go to the HA Virtual Appliance Menu of Node 1.
  - Enter **2** (Show OV Cluster Status) the press **Enter**. See Show OV Cluster Status for more information.

Logging into the OmniVista UI

1. Once all services are running, enter *https://<IPaddress of the Active Node>* in a supported browser to launch OV 2500 NMS-E 4.4R2.

Note: When you create a Layer 3 Cluster Configuration, OmniVista randomly assigns the Active Node to one of the VMs during the “Join Cluster” process (not necessarily to the first Node you configured for the Cluster). Use the “Show OV Cluster Status” command on the HA Virtual Appliance Menu to confirm the Active Cluster.

Note: If you changed the default HTTPs port (443) during VA configuration, you must enter the port after the IP address (e.g., *https://<IPaddress>:<HTTPsPort>).*

2. The first time you launch OmniVista you will be prompted to activate the OmniVista License (fresh installation) and the High-Availability License. Import the license file (.dat) or enter the license key to activate the license(s). You can also activate any additional licenses (e.g., Stellar APs, VM, BYOD) at this time.

Important Note: It is highly-recommended that you change all default user passwords (Admin, Netadmin, Writer, User) after logging into OmniVista for the first time. Go to the **User Management Screen** (Security – Users & User Groups – User) to update the passwords. **Be sure to store the password(s) in a secure place. Lost passwords cannot be retrieved**.

Upgrading from 4.4R1 to 4.4R2

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.4R1 Standalone or High-Availability Installation to an OV 2500 NMS-E 4.4R2 Standalone or High-Availability Installation.

Upgrading from 4.4R1 Standalone to 4.4R2 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.4R1 Standalone Installation to an OV 2500 NMS-E 4.4R2 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

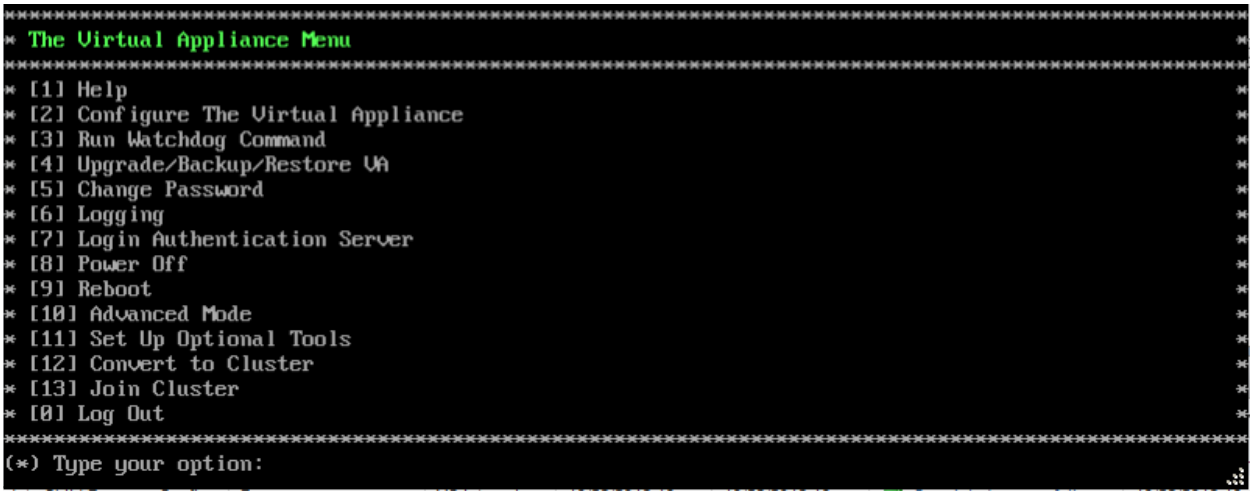
Note that OV 2500 NMS-E 4.4R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

Important Note: To perform an **Offline Upgrade, contact Customer Support**.

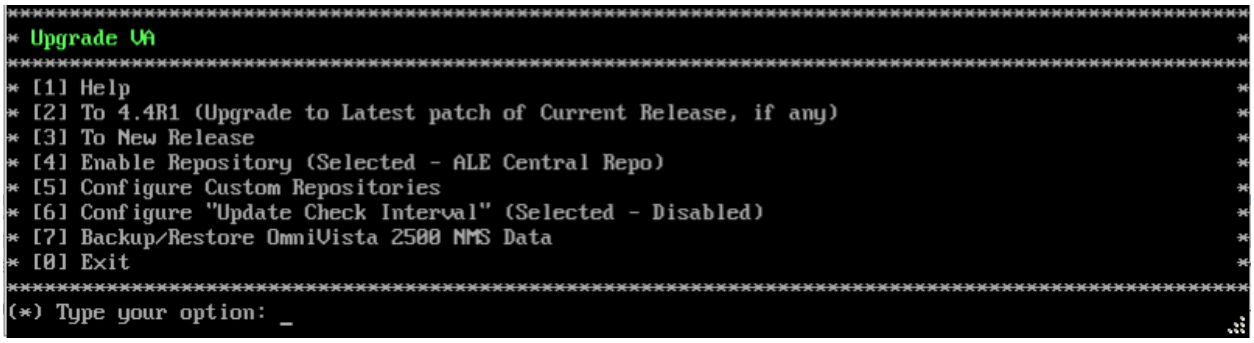
It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic "keepalive" messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

Important Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

1. Open a Console on the OV 2500 NMS-E 4.4R1 Virtual Appliance.



2. Enter **4 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.



3. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

4. Enter **1 - Upgrade to 4.4R2** and press **Enter** to bring up the Upgrade System Options Menu.

```
**********************************************************************************************************
* Upgrade System Options                                                                                 *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Download and Upgrade                                                                               *
* [3] Download Only                                                                                      *
* [4] Upgrade from downloaded package                                                                    *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option:
```

5. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R1 GA
Build Number: 58
Patch Number: 0

Checking available packages for 4.4R2 operation is in progress...
Upgrade to 4.4R2 release is available after upgrading latest to version/patch of 4.4R1 release
Do you want to continue to check upgrade for 4.4R1 release now [y|n] (n): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R2.

```
Getting upgrade information for 4.4R2...
Upgrade information for 4.4R2
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R2
Release     : 47.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R2
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R2 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

8. When the installation is complete, the following prompt will appear. Press **Enter** to continue.

9. The VM will reboot. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt. Log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
  - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See Run Watchdog Command for more details.

Launching the OmniVista UI

Once all services are running after upgrading, enter https://<OVServerIPaddress> in a supported browser to launch OV 2500 NMS-E 4.4R2.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
  1. Go to HA Virtual Appliance Menu. **Select 4 - Configure Current Node**.
  2. Select **2 - Display Current Node Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
  3. Select **16 - Configure Network Size**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
  4. At the Watchdog Service prompt, press **y**, then press **Enter** to restart Watchdog Services.

Upgrading from 4.4R1 HA to 4.4R2 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.4R1 High-Availability Installation to an OV 2500 NMS-E 4.4R2 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS-E 4.4R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

> **Important Note:** Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

High-Availability Upgrade Workflow

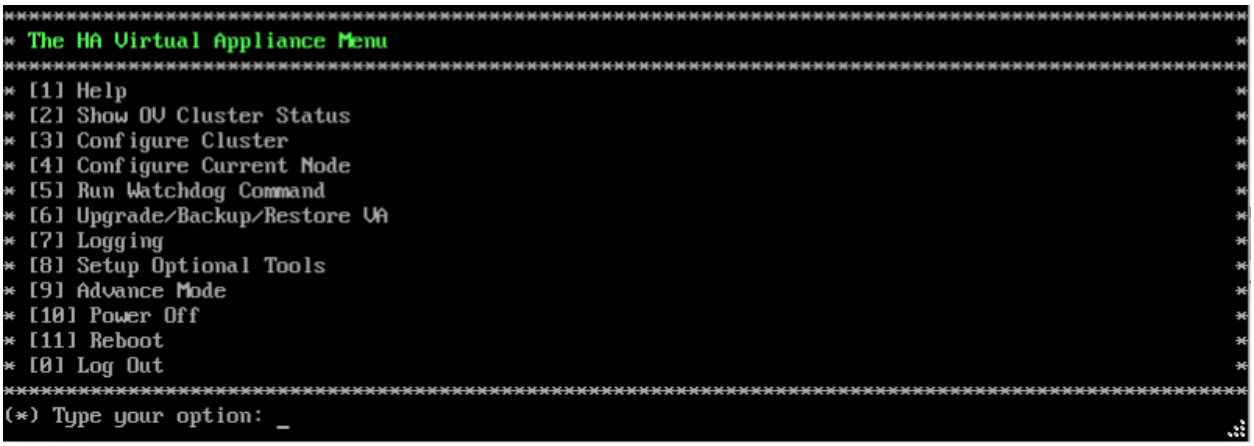
The basic steps for performing a High-Availability upgrade are:

1. Enable Maintenance Mode on the Active Node
2. Upgrade the Active Node (as part of the upgrade process, do **not** reboot the Active Node until the Standby Node is upgraded. See procedure for details.)
3. Upgrade the Standby Node
4. Disable Maintenance Mode on the Active Node

5. Verify the Upgrade.

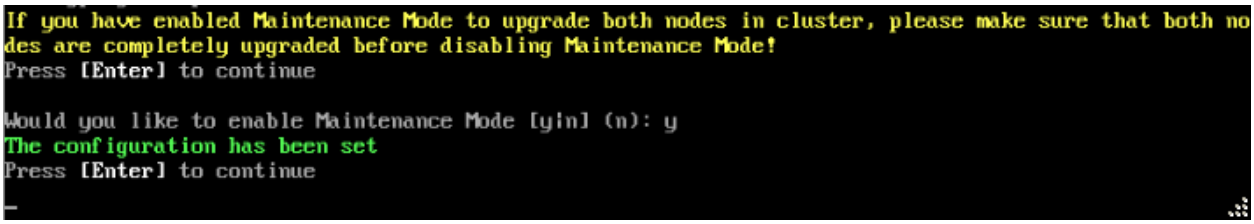
Enable Maintenance Mode on the Active Node

1. Before performing the upgrade, you must first enable Maintenance Mode on the Active Node. Open a Console on the OV 2500 NMS-E 4.4R1 Active Node. This will enable Maintenance Mode on both nodes in the Cluster.



2. Enter **3 – Configure Cluster** to bring up the Configure Cluster Menu.

3. Enter **18 – Enable Maintenance Mode** and press **Enter**. Press **Enter** to continue, then enter **y** and press **Enter** to enable Maintenance Mode. Press **Enter** again to continue and return to the Configure Cluster Menu.



4. On the Configure Cluster Menu, select **0 – Exit** to return to the HA Virtual Appliance Menu.

Upgrade the Active Node

```
**********************************************************************************************************
* The HA Virtual Appliance Menu                                                                          *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Show OV Cluster Status                                                                             *
* [3] Configure Cluster                                                                                  *
* [4] Configure Current Node                                                                             *
* [5] Run Watchdog Command                                                                               *
* [6] Upgrade/Backup/Restore VA                                                                          *
* [7] Logging                                                                                            *
* [8] Setup Optional Tools                                                                               *
* [9] Advance Mode                                                                                       *
* [10] Power Off                                                                                         *
* [11] Reboot                                                                                            *
* [0] Log Out                                                                                            *
**********************************************************************************************************
(*) Type your option: _
```

1. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

```
**********************************************************************************************************
* Upgrade VA                                                                                             *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] To 4.4R1 (Upgrade to Latest patch of Current Release, if any)                                      *
* [3] To New Release                                                                                     *
* [4] Enable Repository (Selected - ALE Central Repo)                                                    *
* [5] Configure Custom Repositories                                                                      *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                            *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                             *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option: _
```

Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

```
**********************************************************************************************************
* Upgrade to New Release                                                                                 *
**********************************************************************************************************
* [1] Upgrade to 4.4R2                                                                                   *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option:
```

3. Enter **1 - Upgrade to 4.4R2** and press **Enter** to bring up the Upgrade System Options Menu.

```
**********************************************************************************************************
* Upgrade System Options                                                                                 *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Download and Upgrade                                                                               *
* [3] Download Only                                                                                      *
* [4] Upgrade from downloaded package                                                                    *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option: _
```

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R1 GA
Build Number: 58
Patch Number: 0

Checking available packages for 4.4R2 operation is in progress...
Upgrade to 4.4R2 release is available after upgrading latest to version/patch of 4.4R1 release
Do you want to continue to check upgrade for 4.4R1 release now [y|n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R2.

```
Getting upgrade information for 4.4R2...
Upgrade information for 4.4R2
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R2
Release     : 47.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R2
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R2 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n):
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

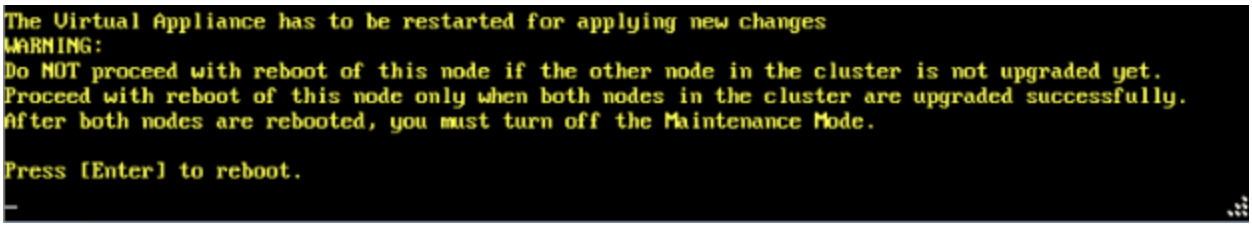
Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure Current Node Menu (from the HA Virtual Appliance Menu, select **4 - Configure Current Node** to access the menu).

7. When the installation is complete, the following prompt will appear.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
```

8. Press **Enter** to continue. The following reboot prompt will appear.

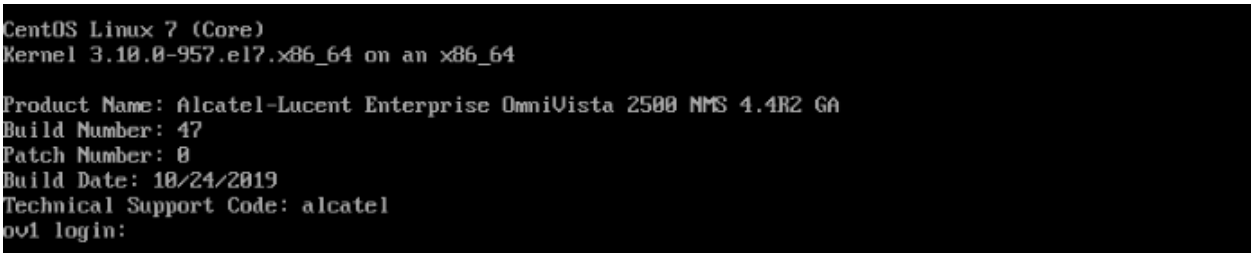


Do **not** press **Enter** at the second prompt to reboot the VM. Reboot the VM and complete the upgrade **after** upgrading the Standby Node.

9. Upgrade the Standby Node. After upgrading the Standby Node, return to this screen and continue with Step 10 below to reboot the Active Node and complete the upgrade process.

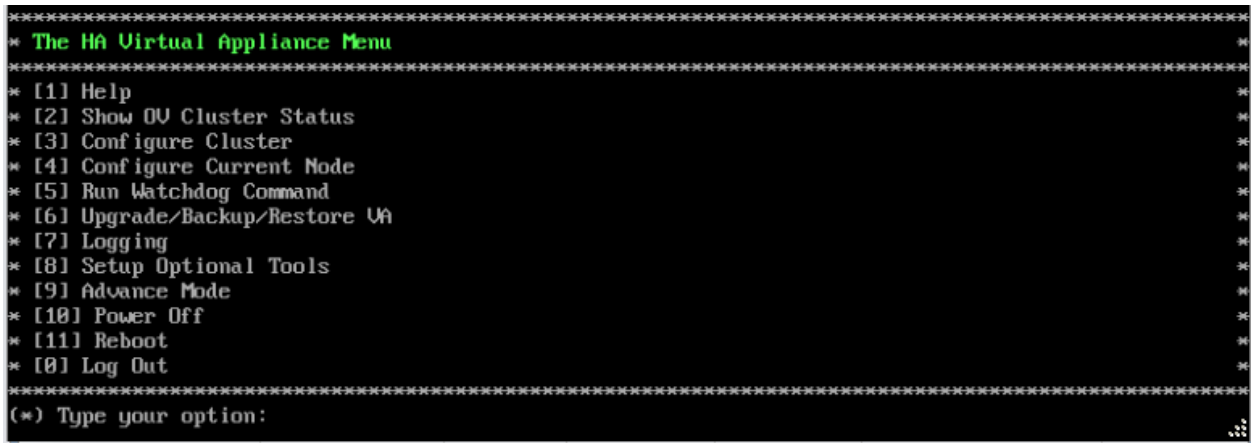
10. Press **Enter** to reboot the VM.

11. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.



12. Log into the VM. The following prompt will appear and The HA Virtual Appliance Menu is displayed.

This prompt is just a reminder. Do **not** disable Maintenance Mode at this time. You will disable Maintenance Mode after upgrading Node 2.



13. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration for more details.

Upgrade the Standby Node

```
* The HA Virtual Appliance Menu                                                *
*******************************************************************************
* [1] Help                                                                     *
* [2] Show OV Cluster Status                                                   *
* [3] Configure Cluster                                                        *
* [4] Configure Current Node                                                   *
* [5] Run Watchdog Command                                                     *
* [6] Upgrade/Backup/Restore VA                                                *
* [7] Logging                                                                  *
* [8] Setup Optional Tools                                                     *
* [9] Advance Mode                                                             *
* [10] Power Off                                                               *
* [11] Reboot                                                                  *
* [0] Log Out                                                                  *
*******************************************************************************
(*) Type your option: _
```

1. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

```
*******************************************************************************
* Upgrade VA                                                                   *
*******************************************************************************
* [1] Help                                                                     *
* [2] To 4.4R1 (Upgrade to Latest patch of Current Release, if any)            *
* [3] To New Release                                                           *
* [4] Enable Repository (Selected - ALE Central Repo)                          *
* [5] Configure Custom Repositories                                            *
* [6] Configure "Update Check Interval" (Selected - Disabled)                  *
* [7] Backup/Restore OmniVista 2500 NMS Data                                   *
* [0] Exit                                                                     *
*******************************************************************************
(*) Type your option: _
```

Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

```
*******************************************************************************
* Upgrade to New Release                                                       *
*******************************************************************************
* [1] Upgrade to 4.4R2                                                         *
* [0] Exit                                                                     *
*******************************************************************************
(*) Type your option: _
```

3. Enter **1 - Upgrade to 4.4R2** and press **Enter** to bring up the Upgrade System Options Menu.

```
*******************************************************************************
* Upgrade System Options                                                       *
*******************************************************************************
* [1] Help                                                                     *
* [2] Download and Upgrade                                                     *
* [3] Download Only                                                            *
* [4] Upgrade from downloaded package                                          *
* [0] Exit                                                                     *
*******************************************************************************
(*) Type your option: _
```

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R1 GA
Build Number: 58
Patch Number: 0

Checking available packages for 4.4R2 operation is in progress...
Upgrade to 4.4R2 release is available after upgrading latest to version/patch of 4.4R1 release
Do you want to continue to check upgrade for 4.4R1 release now [y|n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R2.

```
Getting upgrade information for 4.4R2...
Upgrade information for 4.4R2
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R2
Release     : 47.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R2
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R2 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

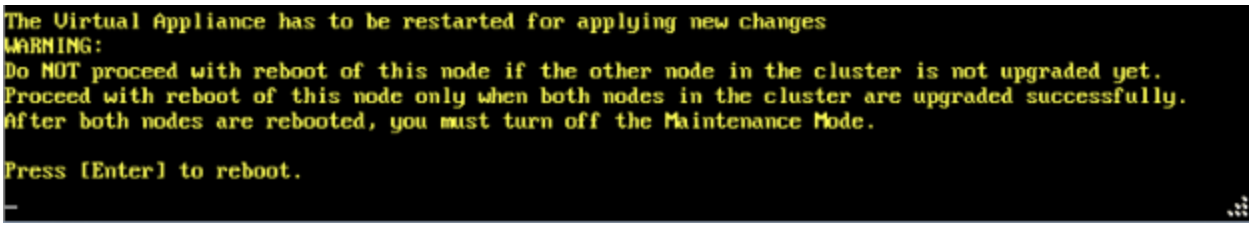
Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure Current Node Menu (from the HA Virtual Appliance Menu, select **4 - Configure Current Node** to access the menu).

7. When the installation is complete, the following prompt will appear.

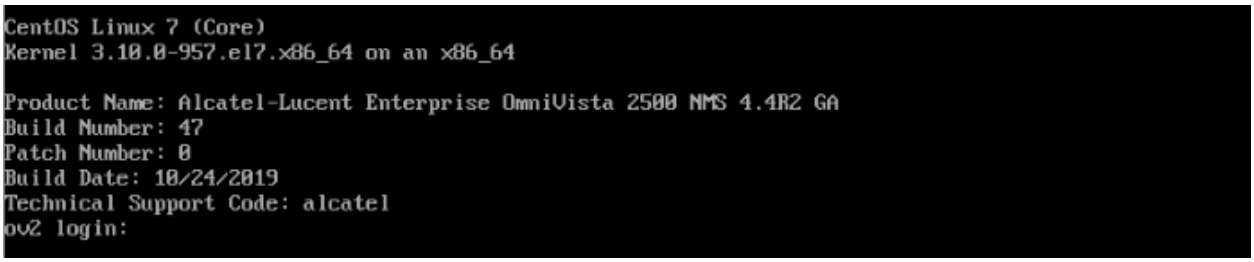
```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
```

8. Press **Enter** to continue. The following reboot prompt will appear.

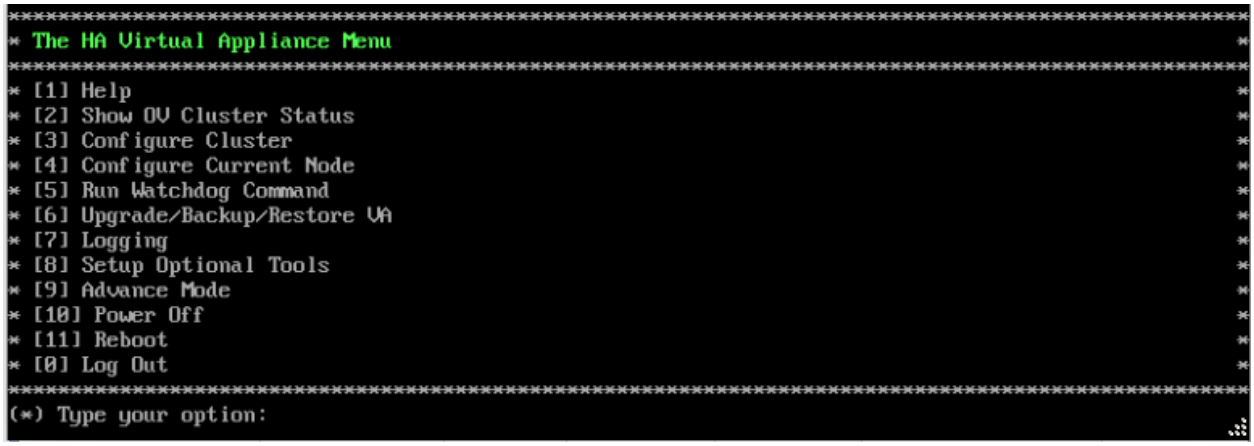


9. Press **Enter** to reboot the VM. While the Standby Node is rebooting, return to the Active Node Console Screen and reboot the Active Node (Step 10, page 53).

10. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.



11. Log into the VM. The HA Virtual Appliance Menu is displayed.



12. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration for more details.

When the upgrade is complete on **both** Nodes (including reboot and login on **both** Nodes), disable Maintenance Mode on the Active Node.

Disable Maintenance Mode on the Active Node

Open a console on the Active Node to disable Maintenance Mode.

1. Go to the HA Virtual Appliance Menu.

```
* The HA Virtual Appliance Menu                                                *
* [1] Help                                                                     *
* [2] Show OV Cluster Status                                                   *
* [3] Configure Cluster                                                        *
* [4] Configure Current Node                                                   *
* [5] Run Watchdog Command                                                     *
* [6] Upgrade/Backup/Restore VA                                                *
* [7] Logging                                                                  *
* [8] Setup Optional Tools                                                     *
* [9] Advance Mode                                                             *
* [10] Power Off                                                               *
* [11] Reboot                                                                  *
* [0] Log Out                                                                  *
(*) Type your option:
```

2. Select **3 – Configure Cluster**. The Configure Cluster Menu appears.

```
* Configure Cluster                                                            *
* [1] Help                                                                     *
* [2] Display Cluster Configuration                                            *
* [3] Configure Cluster IP                                                     *
* [4] Configure Captive Portal Virtual IP                                      *
* [5] Configure Captive Portal Virtual IP v6                                   *
* [6] Configure Additional OV Web Virtual IP                                   *
* [7] Remove peer node from cluster                                            *
* [8] Configure OV Web Ports                                                   *
* [9] Configure Portal Web Ports                                               *
* [10] Configure OV SSL Certificate                                            *
* [11] Enable/Disable AP SSL Authentication                                    *
* [12] Configure FTP Password                                                  *
* [13] Configure Login Authentication Server                                   *
* [14] Preferred Active Node                                                   *
* [15] Manual Failover                                                         *
* [16] Cluster Error Check                                                     *
* [17] Configure Peer Node's Information                                       *
* [18] Disable Maintenance Mode                                                *
* [0] Exit                                                                     *
(*) Type your option:
```

3. Enter **18 – Disable Maintenance Mode** and press **Enter**. The following prompt will appear.

```
If you have enabled Maintenance Mode to upgrade both nodes in cluster, please make sure that both no
des are completely upgraded before disabling Maintenance Mode!
Press [Enter] to continue

Would you like to disable Maintenance Mode [y|n] (n): y

Checking software version number of peer node...
The configuration has been set
Press [Enter] to continue
```

4. Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** to continue. The Configure Cluster Menu will appear.

5. Select **0 – Exit**, to return to the HA Virtual Appliance Menu.

Note: This will disable Maintenance Mode on **both** nodes in the Cluster. There is no need to repeat the steps on the Standby Node.

Verify the Upgrade

When the upgrade is complete on both nodes and Maintenance Mode is disabled, verify that all services are running on both nodes and that the Cluster Status is “Up to Date”.

- Verify that the all services are running on each node.
  - On the HA Virtual Appliance Menu select option **5 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See Run Watchdog Command for more details. Note that on the Standby Node, all services should be running except upam, and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”.
- Verify that the Cluster Status is “Up to Date”. This can be performed on either node.
  - On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See Show OV Cluster Status for more details.

You can now launch the OmniVista UI.

Launching the OmniVista UI

Enter https://<OVServerIPaddress> in a supported browser to launch OV 2500 NMS-E 4.4R2.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
  1. Go to HA Virtual Appliance Menu. **Select 4 - Configure Current Node**.
  2. Select **2 - Display Current Node Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
  3. Select **16 - Configure Network Size**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
  4. At the Watchdog Service prompt, press **y**, then press **Enter** to restart Watchdog Services.

Upgrading from 4.3R3 to 4.4R1

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R3 Standalone or High-Availability Installation to an OV 2500 NMS-E 4.4R1 Standalone or High-Availability Installation.

Upgrading from 4.3R3 Standalone to 4.4R1 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R3 Standalone Installation to an OV 2500 NMS-E 4.4R1 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

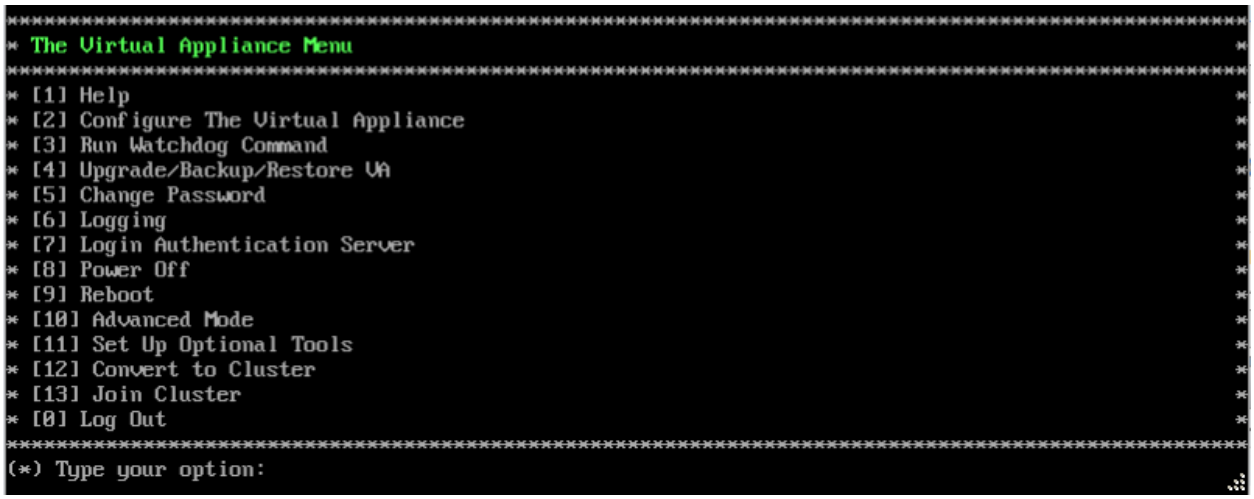
Note that OV 2500 NMS-E 4.4R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

Important Note: To perform an **Offline Upgrade, contact Customer Support**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

Important Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

1. Open a Console on the OV 2500 NMS-E 4.3R3 Virtual Appliance.



2. Enter **4 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

3. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

4. Enter **1 - Upgrade to 4.4R1** and press **Enter** to bring up the Upgrade System Options Menu.

5. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R3 GA
Build Number: 25
Patch Number: 0

Checking available packages for 4.4R1 operation is in progress...
Upgrade to 4.4R1 release is available after upgrading latest to the build of 4.3R3 release
Do you want to continue to check upgrade for 4.3R3 release now [y|n] (n): _
```

6. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R1.

```
Getting upgrade information for 4.3R3...
Current version of Virtual Appliance is the latest build of 4.3R3

Getting upgrade information for 4.4R1...
Upgrade information for 4.4R1
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R1
Release     : 55.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R1
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R1 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n):
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

8. When the installation is complete, the following prompt will appear. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

9. The reboot process will take several minutes. When the reboot is complete, the current configuration is displayed, followed by the Login Prompt. Log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
  - Select option **3 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See Run Watchdog Command for more details.

Launching the OmniVista UI

Once all services are running after upgrading, enter https://<OVServerIPaddress> in a supported browser to launch OV 2500 NMS-E 4.4R1.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
  1. Go to HA Virtual Appliance Menu. **Select 4 - Configure Current Node**.
  2. Select **2 - Display Current Node Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
  3. Select **16 - Configure Network Size**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
  4. At the Watchdog Service prompt, press **y**, then press **Enter** to restart Watchdog Services.

Upgrading from 4.3R3 HA to 4.4R1 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R3 High-Availability Installation to an OV 2500 NMS-E 4.4R1 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).

- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS-E 4.4R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

High-Availability Upgrade Workflow

The basic steps for performing a High-Availability upgrade are:

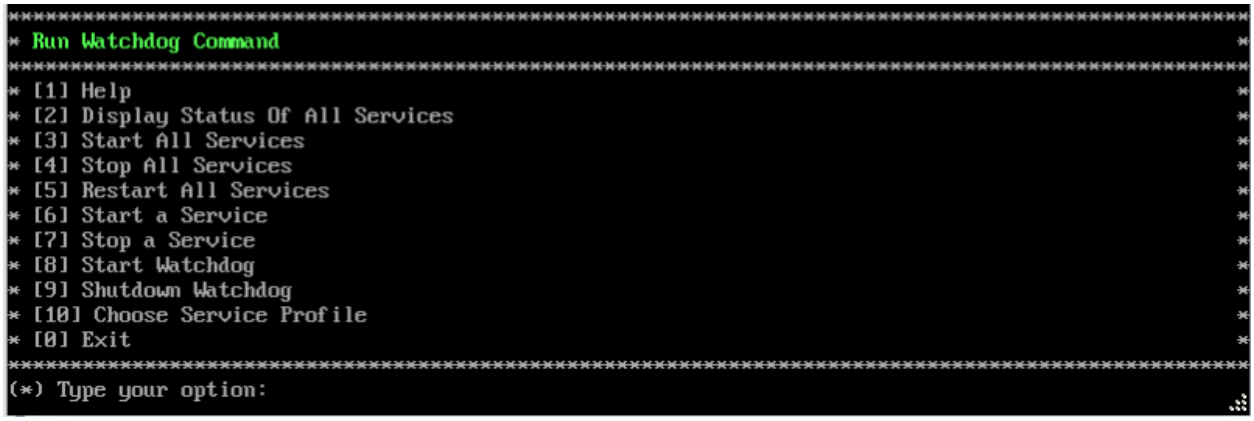
1. Stop All Watchdog Services on the Active Node
2. Enable Maintenance Mode on the Active Node
3. Shutdown the Standby Node
4. Upgrade the Active Node (upgrade must be complete before going to Step 5)
5. Startup the Standby Node
6. Stop All Watchdog Services on the Standby Node
7. Upgrade the Standby Node (upgrade must be complete before going to Step 8)
8. Disable Maintenance Mode on the Active Node
9. Verify the Upgrade.

Stop All Watchdog Services on the Active Node

Before performing the upgrade, you must first stop all services on the Active Node.

1. Open a Console on the OV 2500 NMS-E 4.3R3 Active Node.

2. Enter **5 - Run Watchdog Command** to bring up the Run Watchdog Command Menu.



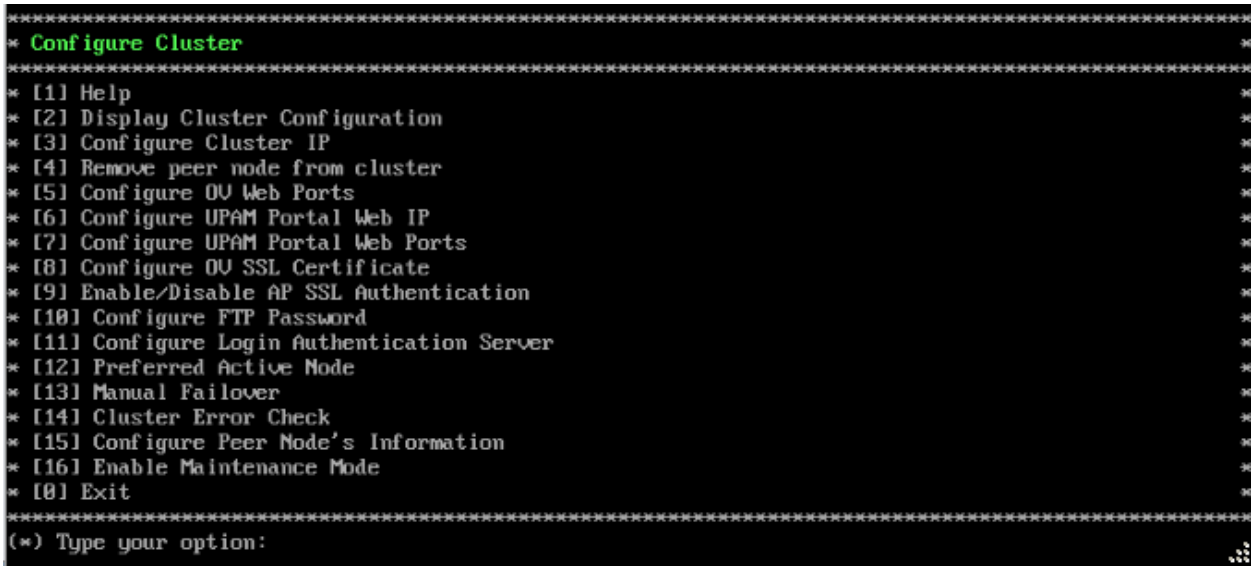
3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display “Watchdog is done stopping all services – Done” and the Run Watchdog Command Menu will appear. Enable Maintenance Mode on the Active Node.

Enable Maintenance Mode on the Active Node

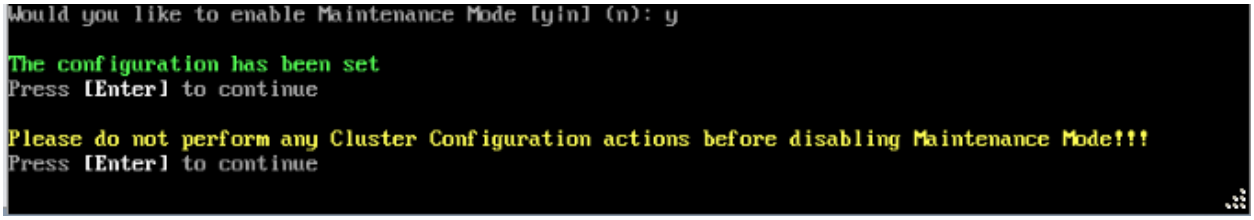
After all services have stopped on the Active Node, enable Maintenance Mode on the Node. This will enable Maintenance Mode on both nodes in the Cluster.

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.

2. Enter **3 – Configure Cluster** to bring up the Configure Cluster Menu.



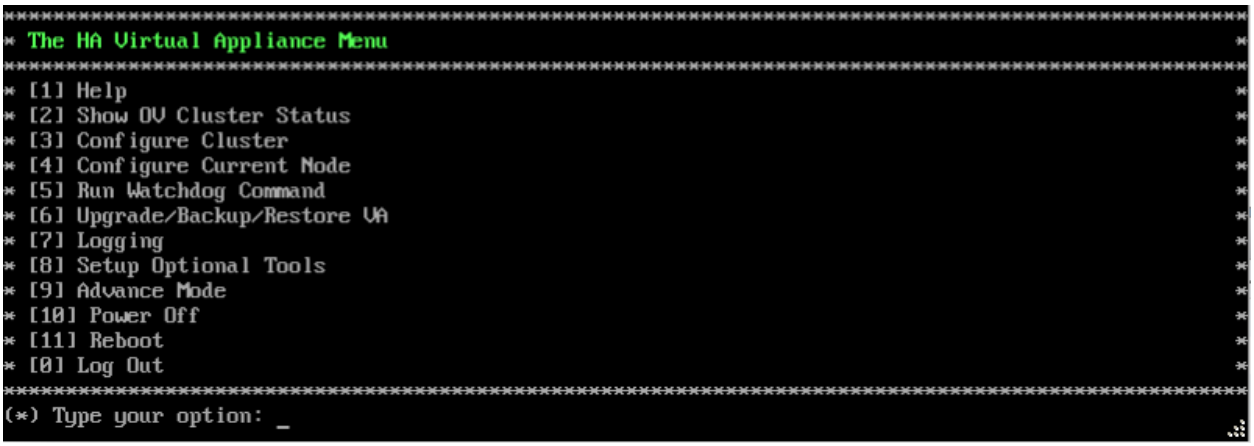
3. Enter **16 – Enable Maintenance Mode**, then enter **y** and press **Enter** to enable Maintenance Mode. Press **Enter** again to continue and return to the Configure Cluster Menu.



4. On the Configure Cluster Menu, select **0 – Exit** to return to the HA Virtual Appliance Menu. You can now shutdown the Standby Node.

Shutdown the Standby Node

1. Open a Console on the OV 2500 NMS-E 4.3R3 Standby Node VM.



2. Enter **10 – Power Off** to power off the VM. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will shut down all services and stop. When the shutdown is complete, upgrade the Active Node.

Upgrade the Active Node

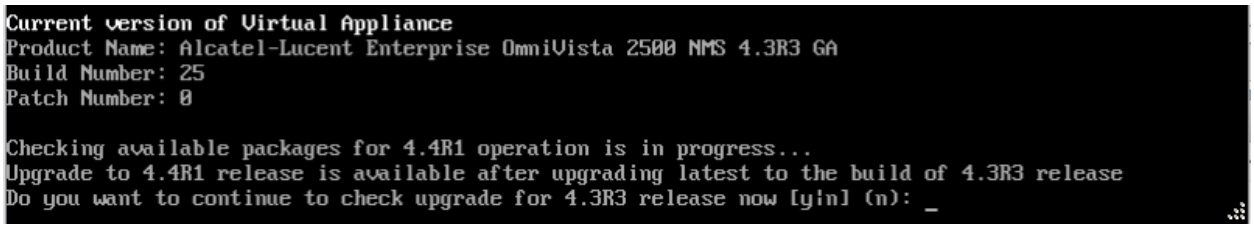
1. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

3. Enter **1 - Upgrade to 4.4R1** and press **Enter** to bring up the Upgrade System Options Menu.

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.



5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R1.

```
Getting upgrade information for 4.3R3...
Current version of Virtual Appliance is the latest build of 4.3R3

Getting upgrade information for 4.4R1...
Upgrade information for 4.4R1
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R1
Release     : 55.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R1
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R1 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n):
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

7. When the installation is complete, the following prompt will appear. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Please turn off maintenance mode after restarting.
Press [Enter] to continue
```

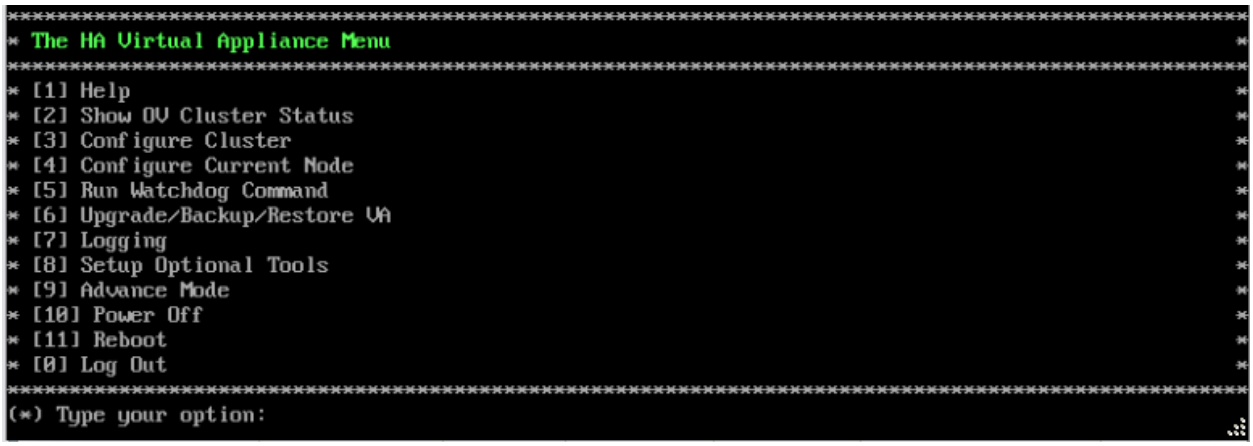
8. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R1 GA
Build Number: 56
Patch Number: 0
Build Date: 06/24/2019
Technical Support Code: alcatel
ov1 login:
```

9. Log into the VM. The following prompt will appear and The HA Virtual Appliance Menu is displayed.

This prompt is just a reminder. Do **not** disable Maintenance Mode at this time. You will disable Maintenance Mode after upgrading Node 2.



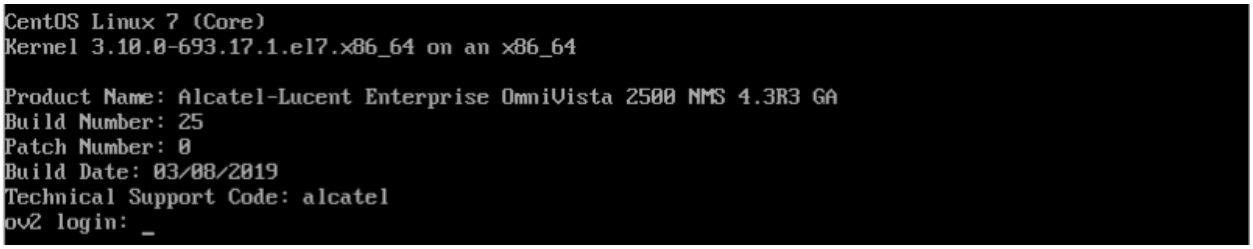
10. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration for more details.

11. After verifying the upgrade, start up the Standby Node.

Important Note: The upgrade on the Active Node must be complete, **before** you start up and upgrade the Standby Node.

Startup the Standby Node

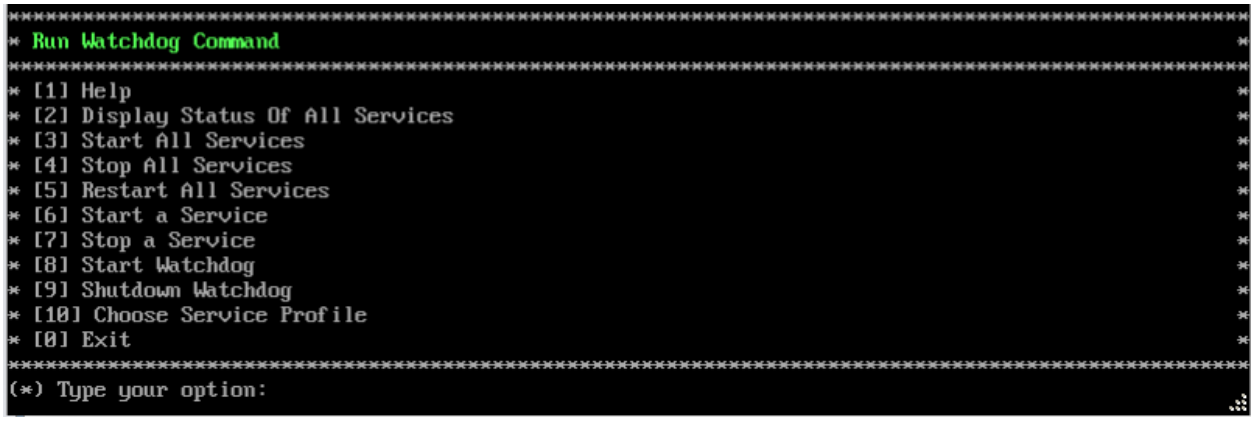
1. Power on the Standby Node.



2. Login to the VM. The HA Virtual Appliance Menu will appear. Stop all Watchdog Services on the Standby Node.

Stop All Watchdog Services on the Standby Node

2. Enter **5 - Run Watchdog Command** to bring up the Run Watchdog Command Menu.



3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display “Watchdog is done stopping all services – Done” and the Run Watchdog Command Menu will appear. Upgrade the Standby Node.

Upgrade the Standby Node

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.

```
*************************************************************************************************************
* The HA Virtual Appliance Menu                                                                             *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] Show OV Cluster Status                                                                                *
* [3] Configure Cluster                                                                                     *
* [4] Configure Current Node                                                                                *
* [5] Run Watchdog Command                                                                                  *
* [6] Upgrade/Backup/Restore VA                                                                             *
* [7] Logging                                                                                               *
* [8] Setup Optional Tools                                                                                  *
* [9] Advance Mode                                                                                          *
* [10] Power Off                                                                                            *
* [11] Reboot                                                                                               *
* [0] Log Out                                                                                               *
*************************************************************************************************************
(*) Type your option: _
```

1. Select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

```
*************************************************************************************************************
* Upgrade VA                                                                                                *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] To 4.3R3 (Upgrade to Latest patch of Current Release, if any)                                         *
* [3] To New Release                                                                                        *
* [4] Enable Repository (Selected - ALE Central Repo)                                                       *
* [5] Configure Custom Repositories                                                                         *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                               *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                                *
* [0] Exit                                                                                                  *
*************************************************************************************************************
(*) Type your option: _
```

Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

```
*************************************************************************************************************
* Upgrade to New Release                                                                                    *
*************************************************************************************************************
* [1] Upgrade to 4.4R1                                                                                      *
* [0] Exit                                                                                                  *
*************************************************************************************************************
(*) Type your option:
```

3. Enter **1 - Upgrade to 4.4R1** and press **Enter** to bring up the Upgrade System Options Menu.

```
*************************************************************************************************************
* Upgrade System Options                                                                                    *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] Download and Upgrade                                                                                  *
* [3] Download Only                                                                                         *
* [4] Upgrade from downloaded package                                                                       *
* [0] Exit                                                                                                  *
*************************************************************************************************************
(*) Type your option: _
```

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R3 GA
Build Number: 25
Patch Number: 0

Checking available packages for 4.4R1 operation is in progress...
Upgrade to 4.4R1 release is available after upgrading latest to the build of 4.3R3 release
Do you want to continue to check upgrade for 4.3R3 release now [y|n] (n): _
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.4R1.

```
Getting upgrade information for 4.3R3...
Current version of Virtual Appliance is the latest build of 4.3R3

Getting upgrade information for 4.4R1...
Upgrade information for 4.4R1
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.4R1
Release     : 55.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.4R1
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.4R1 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n):
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to begin the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size, and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

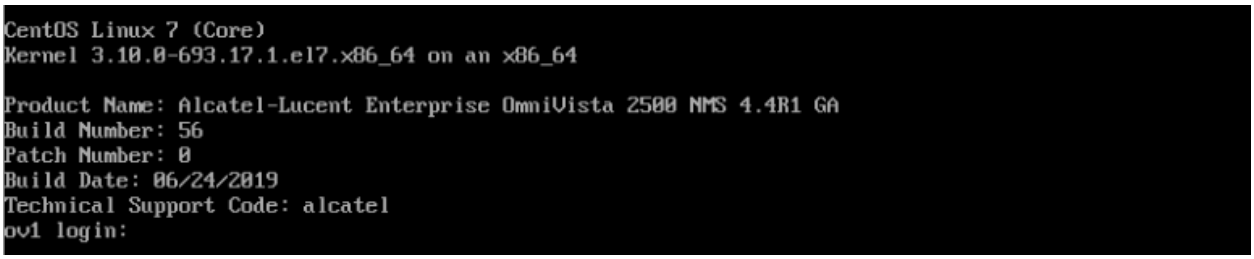
Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

7. When the installation is complete, the following prompt will appear. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Please turn off maintenance mode after restarting.
Press [Enter] to continue
```

8. The reboot process will take several minutes. When the reboot is complete, the Login Screen will appear.



9. Log into the VM. The HA Virtual Appliance Menu is displayed.

10. Verify that the Build Number is correct. On the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration for more details.

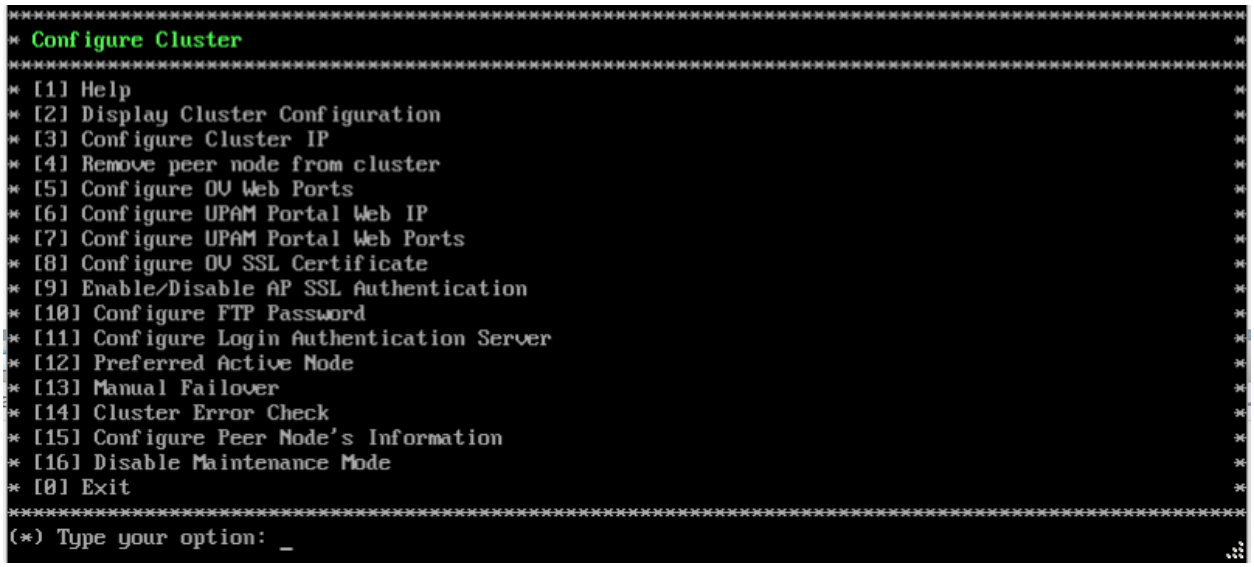
When the upgrade is complete, disable Maintenance Mode on the Active Node.

Disable Maintenance Mode on the Active Node

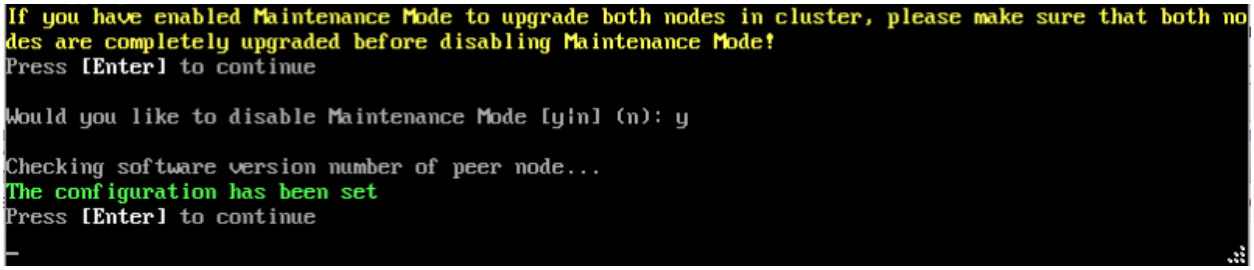
Open a console on the Active Node to disable Maintenance Mode. This will disable Maintenance Mode on both nodes in the Cluster.

1. Go to the HA Virtual Appliance Menu.

2. Select **3 – Configure Cluster**. The Configure Cluster Menu appears.



3. Enter **18 – Disable Maintenance Mode** and press **Enter**. The following prompt will appear.



4. Enter **y** and press **Enter** at the Confirmation Prompt, then press **Enter** to continue. The Configure Cluster Menu will appear.

5. Select **0 – Exit**, to return to the HA Virtual Appliance Menu.

Verify the Upgrade

When the upgrade is complete on both nodes and Maintenance Mode is disabled, verify that all services are running on both nodes and that the Cluster Status is “Up to Date”.

- Verify that the all services are running on each node.
  - On the HA Virtual Appliance Menu select option **5 – Run Watchdog Command**, then select option **2 – Display Status of All Services**. See Run Watchdog Command for more details. Note that on the Standby Node, all services should be running except upam, radius, and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”.
- Verify that the Cluster Status is “Up to Date”. This can be performed on either node.
  - On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. See Show OV Cluster Status for more details.

You can now launch the OmniVista UI.

Launching the OmniVista UI

Enter https://<OVServerIPaddress> in a supported browser to launch OV 2500 NMS-E 4.4R1.

Important Notes for Stellar APs:

- If your network includes Stellar APs, they must be running one of the certified AWOS Releases specified in the *OmniVista 2500 NMS Release Notes*. If necessary, upgrade these devices **after** the OmniVista upgrade. Use the Resource Manager Upgrade Image Screen (Configuration – Resource Manager – Upgrade Image) to upgrade Stellar APs. The AWOS Image Files are available on the Service and Support Website.
- If you are upgrading from a previous build and your network has more than 256 Stellar APs, you must re-apply your VA memory setting after completing the OmniVista upgrade as described below.
  1. Go to HA Virtual Appliance Menu. **Select 4 - Configure Current Node**.
  2. Select **2 - Display Current Node Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).
  3. Select **16 - Configure Network Size**, then select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.
  4. At the Watchdog Service prompt, press **y**, then press **Enter** to restart Watchdog Services.

Upgrading from 4.3R2 to 4.3R3

Use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R2 Standalone or High-Availability Installation to an OV 2500 NMS-E 4.3R3 Standalone or High-Availability Installation.

Upgrading from 4.3R2 Standalone to 4.3R3 Standalone

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R2 Standalone Installation to an OV 2500 NMS-E 4.3R3 Standalone Installation.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the

new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.

- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

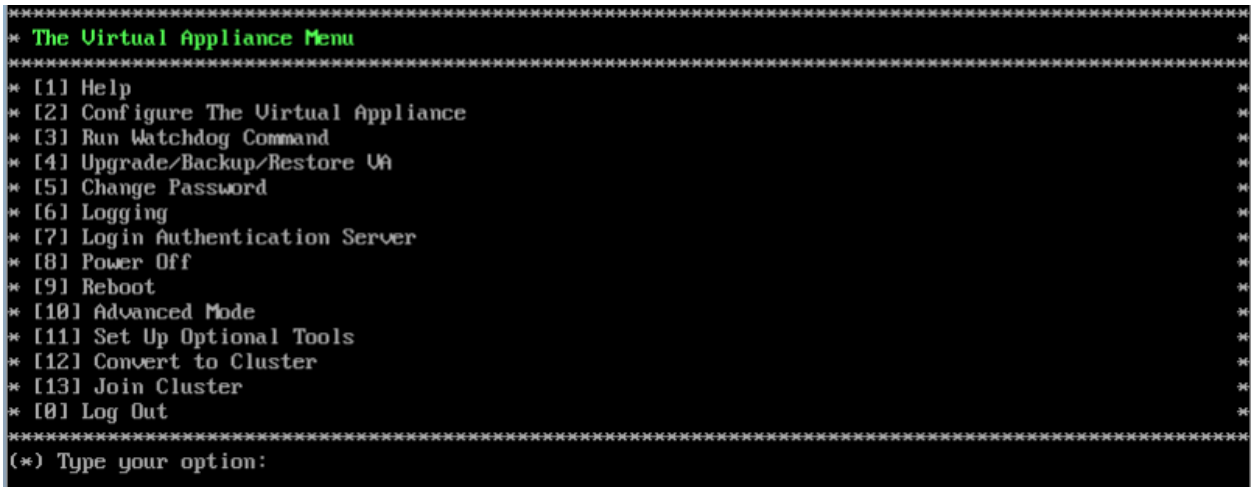
Note that OV 2500 NMS-E 4.3R3 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic "keepalive" messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

Important Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

Important Note: During the upgrade process, when presented with the prompt: "Press any key to continue the upgrade", you **must** hit a key **before the countdown expires.** If you do not, the upgrade will automatically begin at the end of the countdown, but it will fail. If this happens, start the upgrade process again and press any key when prompted before the countdown expires.

1. Open a Console on the OV 2500 NMS-E 4.3R2 Virtual Appliance.



2. Enter **4 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

3. Enter **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

Warning: If you select **3 – To New Release**, the upgrade will fail with the following error message - "/etc/yum.repos.d/ALECentral Repo.repo: Permission denied". You must select **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)**.

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

```
Checking available packages for 4.3R2 operation is in progress...
Upgrade information for 4.3R2
Available Packages
Name        : ovnmsepatchb24
Arch        : x86_64
Version     : 4.3R2
Release     : 24.1.el7
Size        : 18 M
Repo        : CustomRepo1_4.3R2
Summary     : OV Patch 1 for 4.3R2 build 24
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Patch 1 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.3R2
            : build 24
            : ------------------------------------------------------------------------------
            : OVE-3399: Could not upgrade 4.3R2 to 4.3R3 with ALE Central Repo
            :
            : OVE-3041: NO authen radius possible between UPAM and RADIUS
            : message + Too many authentication seen in OV log
            :
            : OVE-3421: Improve SNMP ping logic in OV to avoid fake
            : alaSwitchDown trap for AOS devices
            :
            : OVE-3284: Could not upgrade the switch 6350
            :
            : OVE-3639: Failure upgrade from Patch to Patch
            :
            : OVE-3832: In OV 43R2, when you input the RADIUS server 'Shared
            : Secret', it stops after 16 characters
            :
            : OVE-3778: Failed to backup-restore OV 4.3R2
            :
            : OVE-3839: Repodata messages when collecting logs in 4.3R2
            : ------------------------------------------------------------------------------

Would you like to install the package [y|n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch.

6. When the installation is complete, the following message will appear. Press **Enter** to reboot the VM.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

When the reboot is complete, the login screen will appear.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64

Technical Support Code: alcatel
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R2 GA
Build Number: 24
Patch Number: 1
Build Date: 11/08/2018
omnivista login: _
```

7. Login to the VM. The Virtual Appliance Menu will appear.

```
*************************************************************************************************
* The Virtual Appliance Menu                                                                    *
*************************************************************************************************
* [1] Help                                                                                      *
* [2] Configure The Virtual Appliance                                                           *
* [3] Run Watchdog Command                                                                      *
* [4] Upgrade/Backup/Restore VA                                                                 *
* [5] Change Password                                                                           *
* [6] Logging                                                                                   *
* [7] Login Authentication Server                                                               *
* [8] Power Off                                                                                 *
* [9] Reboot                                                                                    *
* [10] Advanced Mode                                                                            *
* [11] Set Up Optional Tools                                                                    *
* [12] Convert to Cluster                                                                       *
* [13] Join Cluster                                                                             *
* [0] Log Out                                                                                   *
*************************************************************************************************
(*) Type your option:
```

Note: Make sure all services are running before proceeding to Step 8.

8. Enter **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

```
*************************************************************************************************
* Upgrade VA                                                                                    *
*************************************************************************************************
* [1] Help                                                                                      *
* [2] To 4.3R2 (Upgrade to Latest patch of Current Release, if any)                             *
* [3] To New Release                                                                            *
* [4] Enable Repository (Selected - ALE Central Repo)                                           *
* [5] Configure Custom Repositories                                                             *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                   *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                    *
* [0] Exit                                                                                      *
*************************************************************************************************
(*) Type your option:
```

9. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

```
*************************************************************************************************
* Upgrade to New Release                                                                        *
*************************************************************************************************
* [1] Upgrade to 4.3R3                                                                          *
* [0] Exit                                                                                      *
*************************************************************************************************
(*) Type your option:
```

10. Enter **1 - Upgrade to 4.3R3** and press **Enter** to bring up the Upgrade System Options Menu.

```
*************************************************************************************************
* Upgrade System Options                                                                        *
*************************************************************************************************
* [1] Help                                                                                      *
* [2] Download and Upgrade                                                                      *
* [3] Download Only                                                                             *
* [4] Upgrade from downloaded package                                                           *
* [0] Exit                                                                                      *
*************************************************************************************************
(*) Type your option: _
```

11. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R2 GA
Build Number: 24
Patch Number: 1

Checking available packages for 4.3R3 operation is in progress...
Upgrade to 4.3R3 release is available after upgrading latest to the build of 4.3R2 release
Do you want to continue to check upgrade for 4.3R2 release now [y|n] (n): _
```

12. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.3R3.

```
Getting upgrade information for 4.3R3...
Upgrade information for 4.3R3
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R3
Release     : 21.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.3R3
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.3R3 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (14s)...
```

13. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R3.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

14. When the installation is complete, the following prompt will appear. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

15. The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
  - Select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details.

Once all services are running, upgrade to OmniVista 4.4R2 Standalone.

Upgrading from 4.3R2 HA to 4.3R3 HA

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from an OV 2500 NMS-E 4.3R2 High-Availability Installation to an OV 2500 NMS-E 4.3R3 High-Availability Installation. You must upgrade **both** the Active and Standby Nodes.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.
- Make sure the data sync between the two Nodes are up to date using the **Show Cluster Status** command in the HA Virtual Appliance Menu and make sure all services are running on both nodes.
- Make sure you can access OmniVista through the Web interface.

Note that OV 2500 NMS-E 4.3R3 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 -**

Configure The Virtual Appliance on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic "keepalive" messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

> **Important Note:** During the upgrade process, when presented with the prompt: "Press any key to continue the upgrade", you **must** hit a key **before the countdown expires.** If you do not, the upgrade will automatically begin at the end of the countdown, but it will fail. If this happens, start the upgrade process again and press any key when prompted before the countdown expires.

High-Availability Upgrade Workflow

There are two (2) upgrades required when upgrading from 4.3R2 HA to 4.3R3 HA. You must first upgrade from 4.3R2 to 4.3R2 (Patch 1); then upgrade from 4.3R2 (Patch 1) to 4.3R3.

Upgrade from 4.3R2 to 4.3R2 (Patch 1)

The basic steps for performing the upgrade to 4.3R2 (Patch 1) are:

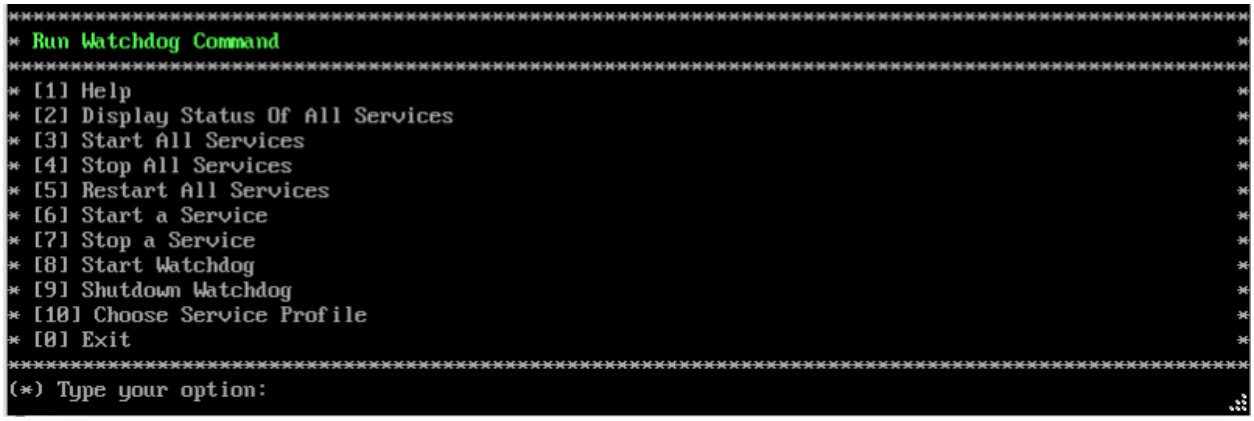
1. Stop All Watchdog Services on the Active Node
2. Enable Maintenance Mode on the Active Node
3. Shutdown the Standby Node
4. Upgrade the Active Node (upgrade must be complete before going to Step 5)
5. Startup the Standby Node
6. Stop All Watchdog Services on the Standby Node
7. Upgrade the Standby Node (upgrade must be complete before going to Step 8)
8. Disable Maintenance Mode on the Active Node
9. Verify the Upgrade.

Stop All Watchdog Services on the Active Node

Before performing the upgrade, you must first stop all services on the Active Node.

1. Open a Console on the OV 2500 NMS-E 4.3R2 Active Node VM.

2. On the HA Virtual Appliance Menu, enter **5 – Run Watchdog Command** to bring up the Run Watchdog Command Menu.



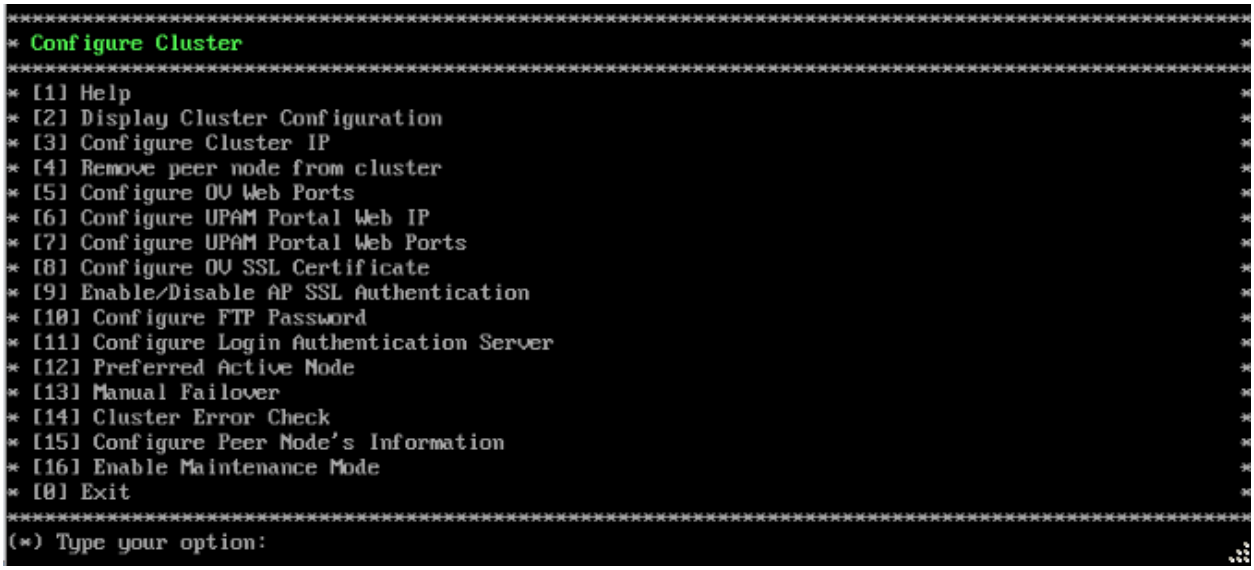
3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display the following message: “Watchdog is done stopping all services – Done”, and the Run Watchdog Command Menu will appear. Enable Maintenance Mode on the Active Node.

Enable Maintenance Mode on the Active Node

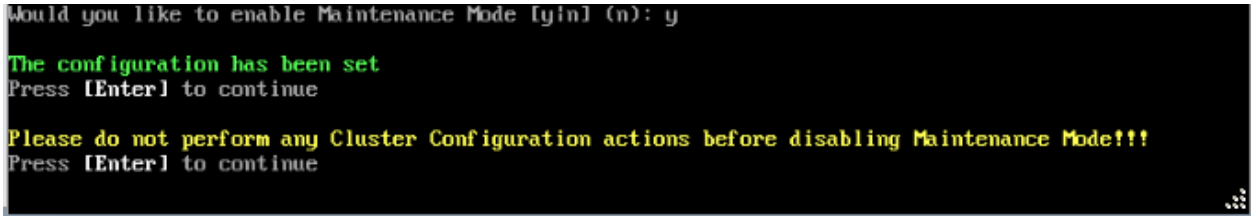
Enable Maintenance Mode on the Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.

2. Enter **3 – Configure Cluster** to bring up the Configure Cluster Menu.



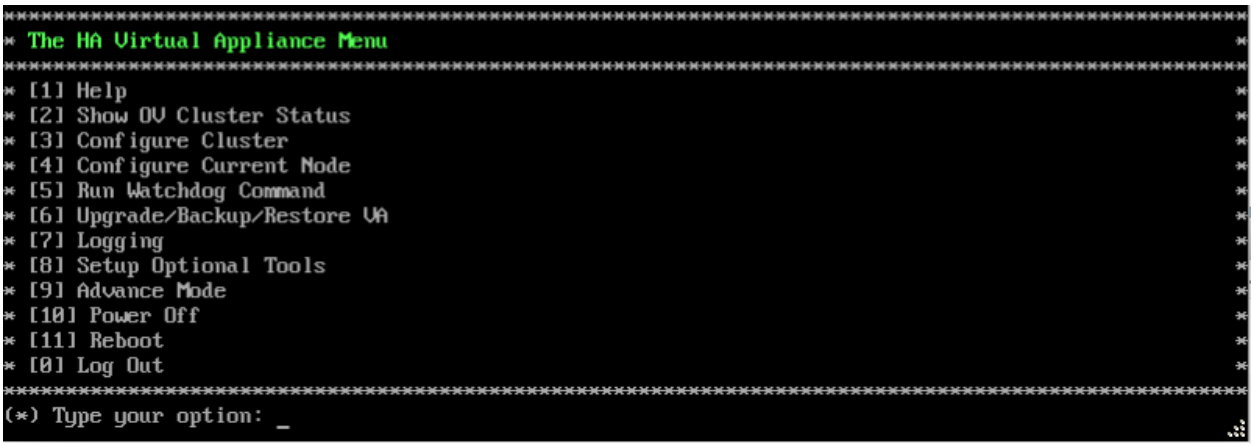
3. Enter **16 – Enable Maintenance Mode**, then enter **y** and press **Enter** to enable Maintenance Mode. Press **Enter** again to continue and return to the Configure Cluster Menu.



4. On the Configure Cluster Menu, select **0 – Exit** to return to the HA Virtual Appliance Menu. You can now shutdown the Standby Node.

Shutdown the Standby Node

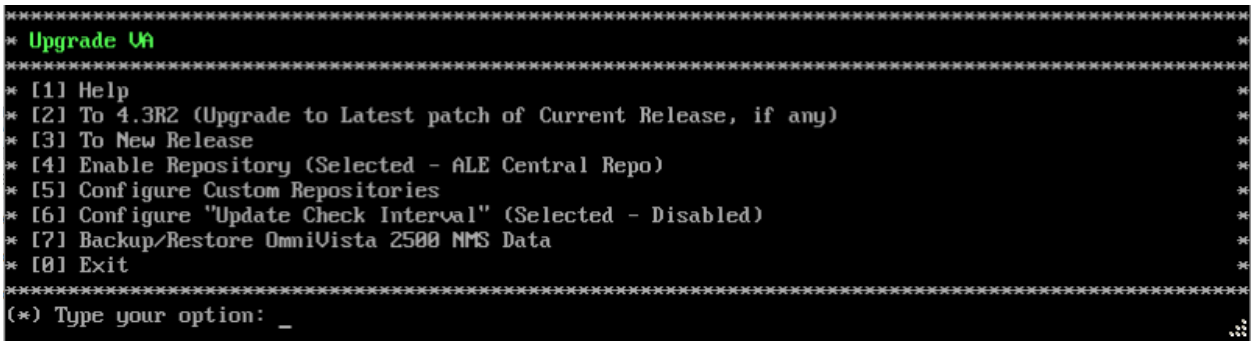
1. Open a Console on the OV 2500 NMS-E 4.3R2 Standby Node VM.



2. Enter **10 – Power Off** to power off the VM. Enter **y** and press **Enter** at the Confirmation Prompt. When the shutdown is complete, upgrade the Active Node.

Upgrade the Active Node

1. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.

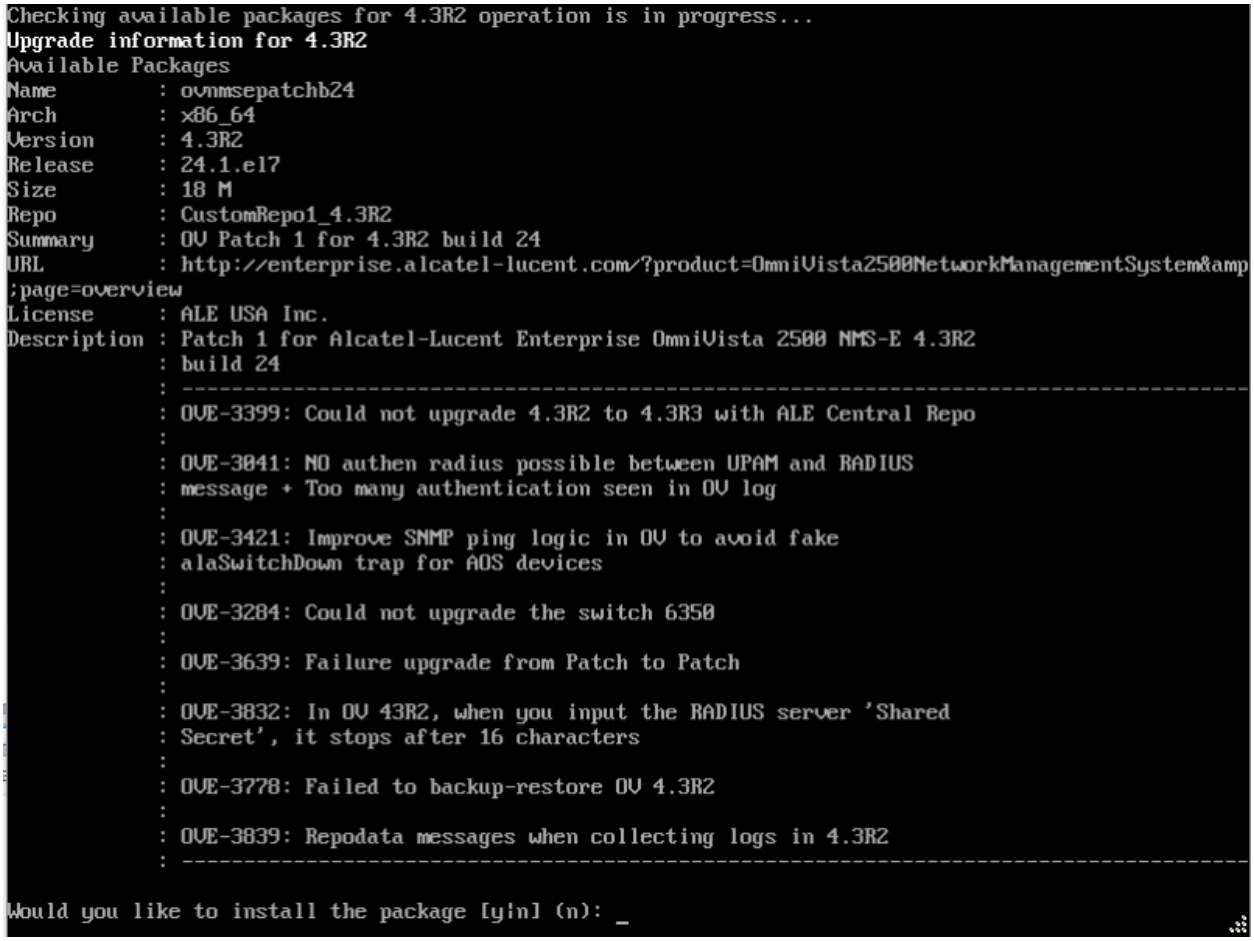


Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

Warning: If you select **3 – To New Release**, the upgrade will fail with the following error message - "/etc/yum.repos.d/ALECentral Repo.repo: Permission denied". You **must** select **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)**.

3. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt. The Upgrade Information Screen (shown below) will appear.



4. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch. When the installation is complete, the following prompt will appear.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
```

5. Press **Enter** to continue. The following prompt will appear.

```
The Virtual Appliance has to be restarted for applying new changes
Please turn off maintenance mode after restarting.
Press [Enter] to continue
```

6. Press **Enter** to reboot the VM. When the reboot is complete, the login screen will appear. Note that the screen indicates Build 24, Patch 1.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64

Technical Support Code: alcatel
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R2 GA
Build Number: 24
Patch Number: 1
Build Date: 11/08/2018
ov1 login:
```

7. Login to the VM. The HA Virtual Appliance Menu will appear.

```
*************************************************************************************************************
* The HA Virtual Appliance Menu                                                                             *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] Show OV Cluster Status                                                                                *
* [3] Configure Cluster                                                                                     *
* [4] Configure Current Node                                                                                *
* [5] Run Watchdog Command                                                                                  *
* [6] Upgrade/Backup/Restore VA                                                                             *
* [7] Logging                                                                                               *
* [8] Setup Optional Tools                                                                                  *
* [9] Advance Mode                                                                                          *
* [10] Power Off                                                                                            *
* [11] Reboot                                                                                               *
* [0] Log Out                                                                                               *
*************************************************************************************************************
(*) Type your option:
```

8. Make sure that the upgrade is complete and all services have started **before** you start up the Standby Node.

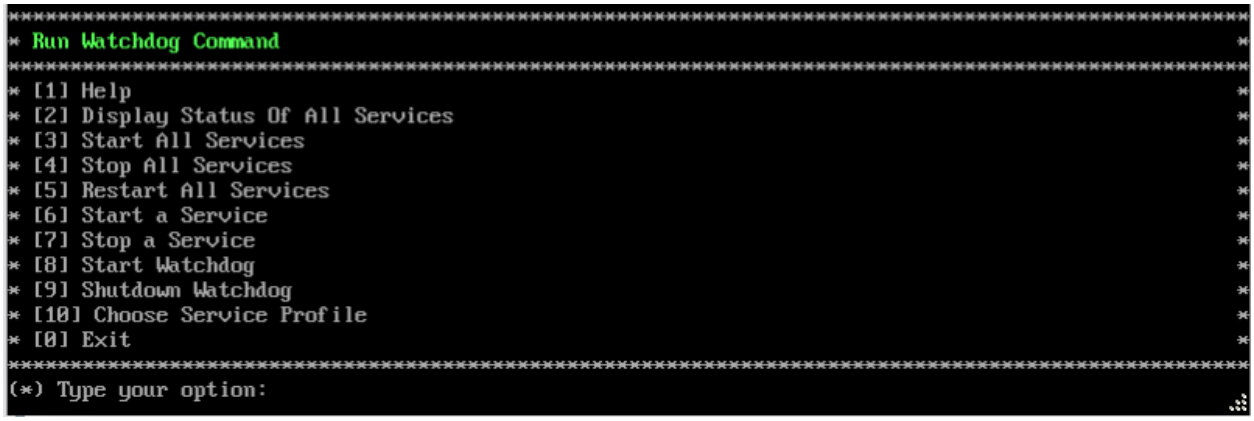
Startup the Standby Node

1. Power on the Standby Node and log into the VM. The HA Virtual Appliance Menu will appear. Once the Standby Node is powered up (all services are running), stop all Watchdog Services on the Standby Node.

Stop All Watchdog Services on the Standby Node

1. Open a Console on the OV 2500 NMS-E 4.3R2 Standby Node.

2. On the HA Virtual Appliance Menu, enter **5 - Run Watchdog Command** to bring up the Run Watchdog Command Menu.

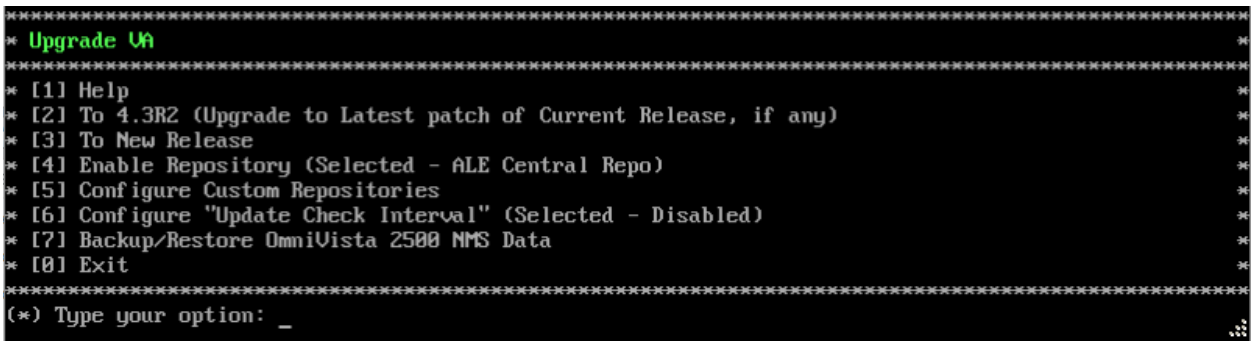


3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display “Watchdog is done stopping all services – Done” and the Run Watchdog Command Menu will appear. Upgrade the Standby Node.

Upgrade the Standby Node

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.

2. Select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.



Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

3. Enter **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

Warning: If you select **3 – To New Release**, the upgrade will fail with the following error message - "/etc/yum.repos.d/ALECentral Repo.repo: Permission denied". You **must** select **2 – To 4.3R2 (Upgrade to Latest patch of Current Release, if any)**.

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt. The Upgrade Information Screen (shown below) will appear.

```
Checking available packages for 4.3R2 operation is in progress...
Upgrade information for 4.3R2
Available Packages
Name        : ovnmsepatchb24
Arch        : x86_64
Version     : 4.3R2
Release     : 24.1.el7
Size        : 18 M
Repo        : CustomRepo1_4.3R2
Summary     : OV Patch 1 for 4.3R2 build 24
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Patch 1 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E 4.3R2
            : build 24
            : ------------------------------------------------------------------------------
            : OVE-3399: Could not upgrade 4.3R2 to 4.3R3 with ALE Central Repo
            :
            : OVE-3041: NO authen radius possible between UPAM and RADIUS
            : message + Too many authentication seen in OV log
            :
            : OVE-3421: Improve SNMP ping logic in OV to avoid fake
            : alaSwitchDown trap for AOS devices
            :
            : OVE-3284: Could not upgrade the switch 6350
            :
            : OVE-3639: Failure upgrade from Patch to Patch
            :
            : OVE-3832: In OV 43R2, when you input the RADIUS server 'Shared
            : Secret', it stops after 16 characters
            :
            : OVE-3778: Failed to backup-restore OV 4.3R2
            :
            : OVE-3839: Repodata messages when collecting logs in 4.3R2
            : ------------------------------------------------------------------------------

Would you like to install the package [y|n] (n): _
```

5. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch. When the installation is complete, the following prompt will appear.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue
```

6. Press **Enter** to continue. The following prompt will appear.

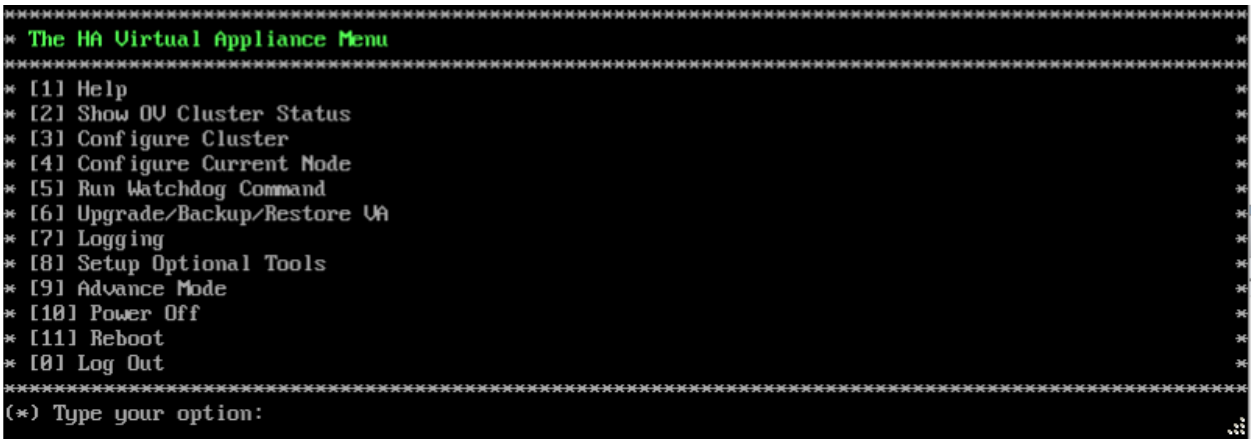
```
The Virtual Appliance has to be restarted for applying new changes
Please turn off maintenance mode after restarting.
Press [Enter] to continue
```

7. Press **Enter** to reboot the VM. When the reboot is complete, the login screen will appear. Note that the screen indicates Build 24, Patch 1.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64

Technical Support Code: alcatel
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R2 GA
Build Number: 24
Patch Number: 1
Build Date: 11/08/2018
ov1 login:
```

8. Login to the VM. The HA Virtual Appliance Menu will appear.

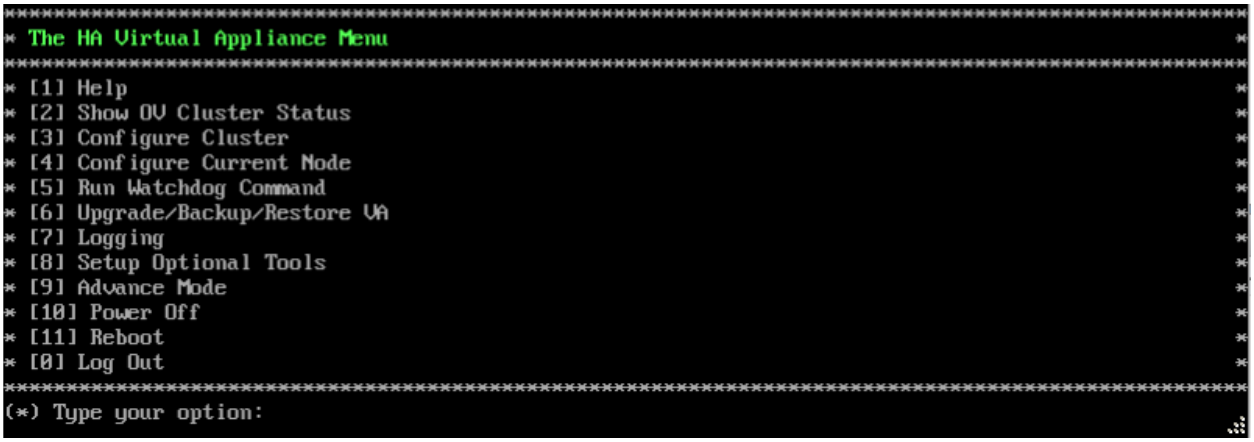


9. Make sure that the upgrade is complete and all services have started **before** you disable Maintenance Mode on the Active Node.

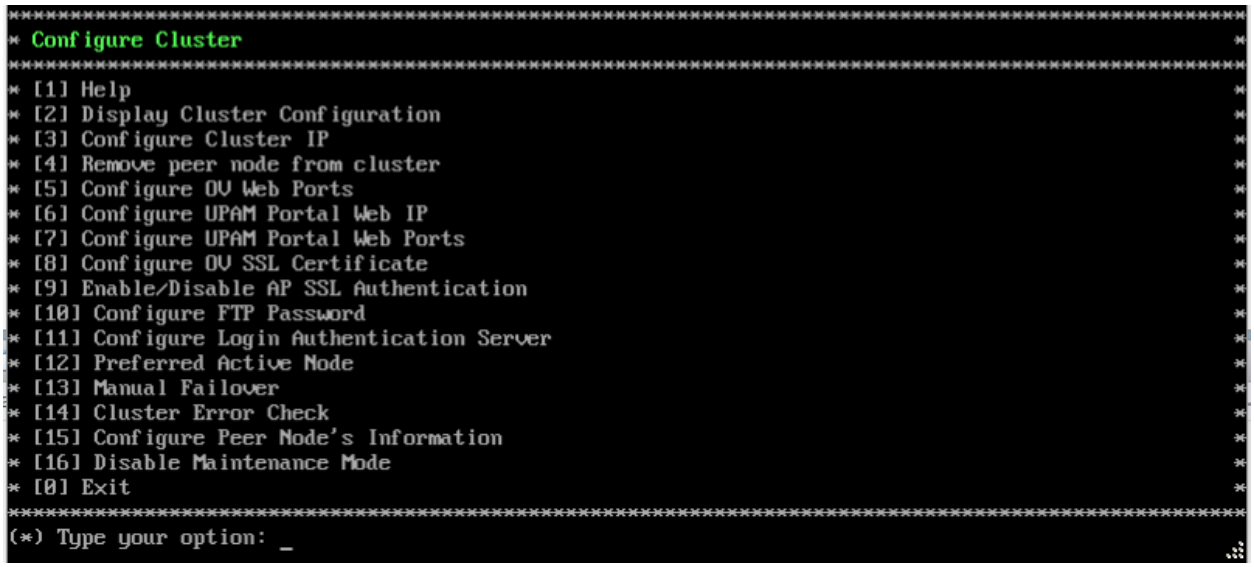
Disable Maintenance Mode on the Active Node

Open a console on the Active Node to disable Maintenance Mode. This will disable Maintenance Mode on both nodes in the Cluster.

1. Go to the HA Virtual Appliance Menu.



2. Select **3 – Configure Cluster**. The Configure Cluster Menu appears.



3. Enter **16 – Disable Maintenance Mode**, then enter **y** and press **Enter**. The Configure Cluster Menu will appear. Select **0 – Exit**, to return to the HA Virtual Appliance Menu. Verify the Upgrade.

Verify the Upgrade

When the upgrade to Patch 1 is complete on both nodes and Maintenance Mode is disabled, perform the following tasks to verify the upgrade.

- Verify that the all services are running on each node.
  - On the HA Virtual Appliance Menu select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details. Note that on the Standby Node, all services should be running except upam, radius, and nginx. It is the expected behavior on the Standby Node that these services will be "Stopped".
- Verify that the Cluster Status is "Up to Date" and that the node roles (Active/Standby) are correct. This can be performed on either node. If the roles changed, remember which node is the Active node for the upgrade to 4.3R3.
  - On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate "Up to Date". If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. The command also displays the role for node you are logged into – "Active" or "Standby". See Show OV Cluster Status for more details.
- Take a configuration snapshot without selecting the option "Snapshot virtual machine's memory". This will help with reverting the VM if the upgrade to 4.3R3 fails.

Once all services are running, upgrade from 4.3R2 (Patch 1) to 4.3R3.

Upgrade from 4.3R2 (Patch 1) to 4.3R3

The basic steps for performing the upgrade to 4.3R3 are:

1. Stop All Watchdog Services on the Active Node
2. Enable Maintenance Mode on the Active Node
3. Shutdown the Standby Node
4. Upgrade the Active Node (upgrade must be complete before going to Step 5)
5. Startup the Standby Node
6. Stop All Watchdog Services on the Standby Node
7. Upgrade the Standby Node (upgrade must be complete before going to Step 8)
8. Shutdown the Standby Node (shutdown must be complete before going to Step 9)
9. Disable Maintenance Mode on the Active Node
10. Startup the Standby Node
11. Verify the Upgrade.

Important Note: Make sure you are beginning the upgrade process on the Active Node. To view the Node Roles (Active/Standby), go to the HA Virtual Appliance Menu and select option **2 – Show OV Cluster Status**. As shown below, the command displays the role for each node – "Active" or "Standby". See Show OV Cluster Status for more details.

```
Cluster Status:
Node     Hostname  Ip Address      Role    Status
Current  ov1       10.255.222.203  Active  Online
Peer     ov2       10.255.222.98           Online
Data sync: Up to Date
```

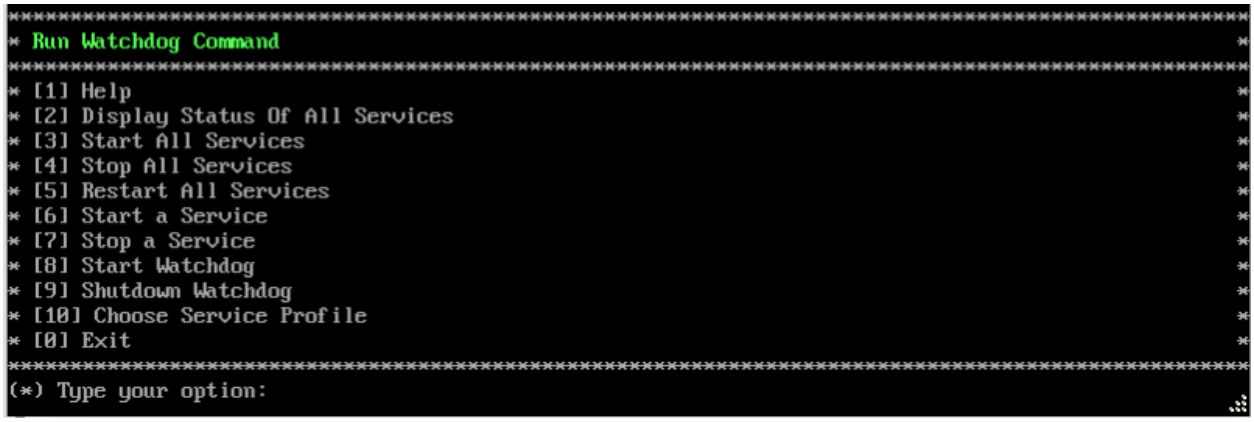
Stop All Watchdog Services on the Active Node

Before performing the upgrade, you must first stop all services on the Active Node.

1. Open a Console on the OV 2500 NMS-E 4.3R2 Active Node.

```
**********************************************************************************************************
* The HA Virtual Appliance Menu                                                                          *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Show OV Cluster Status                                                                             *
* [3] Configure Cluster                                                                                  *
* [4] Configure Current Node                                                                             *
* [5] Run Watchdog Command                                                                               *
* [6] Upgrade/Backup/Restore VA                                                                          *
* [7] Logging                                                                                            *
* [8] Setup Optional Tools                                                                               *
* [9] Advance Mode                                                                                       *
* [10] Power Off                                                                                         *
* [11] Reboot                                                                                            *
* [0] Log Out                                                                                            *
**********************************************************************************************************
(*) Type your option: _
```

2. On the HA Virtual Appliance Menu, enter **5 – Run Watchdog Command** to bring up the Run Watchdog Command Menu.



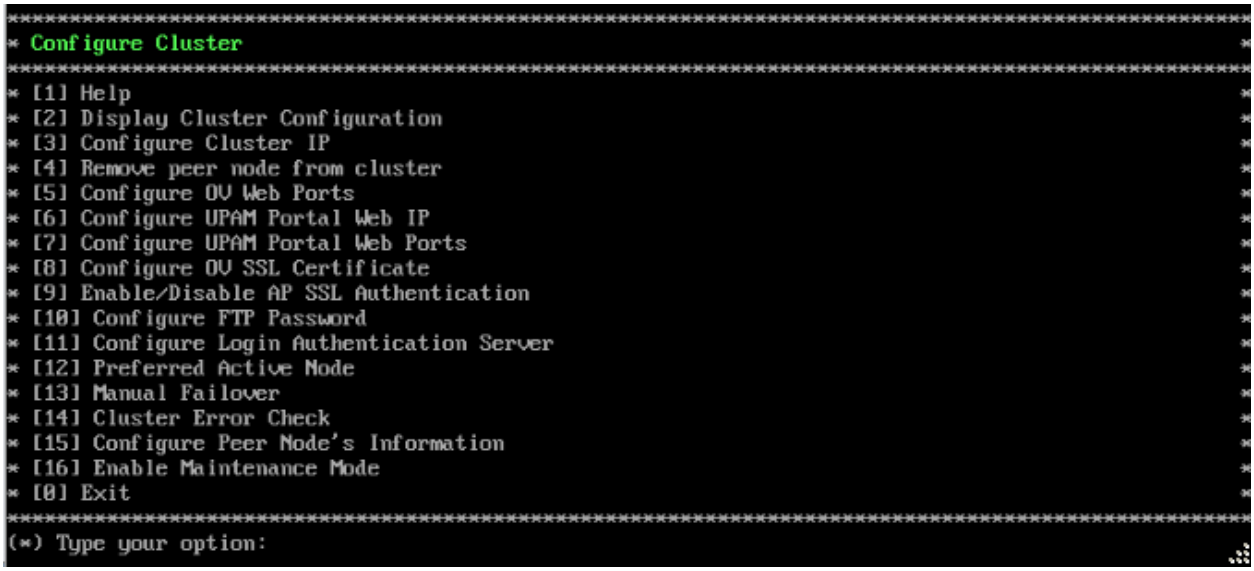
3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display "Watchdog is done stopping all services – Done" and the Run Watchdog Command Menu will appear. Enable Maintenance Mode on the Active Node.

Enable Maintenance Mode on the Active Node

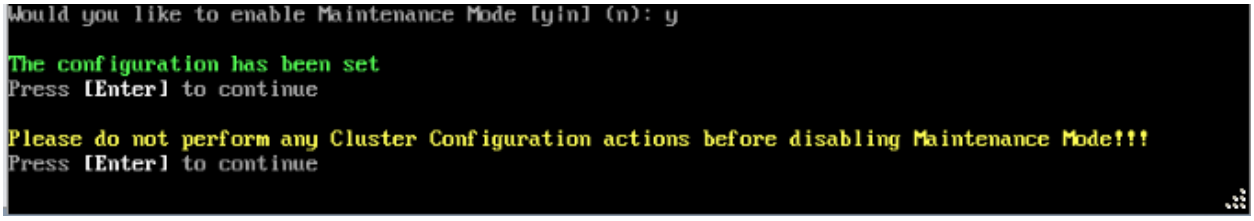
Enable Maintenance Mode on the Active Node. This will enable Maintenance Mode on both nodes in the Cluster.

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.

2. Enter **3 – Configure Cluster** to bring up the Configure Cluster Menu.



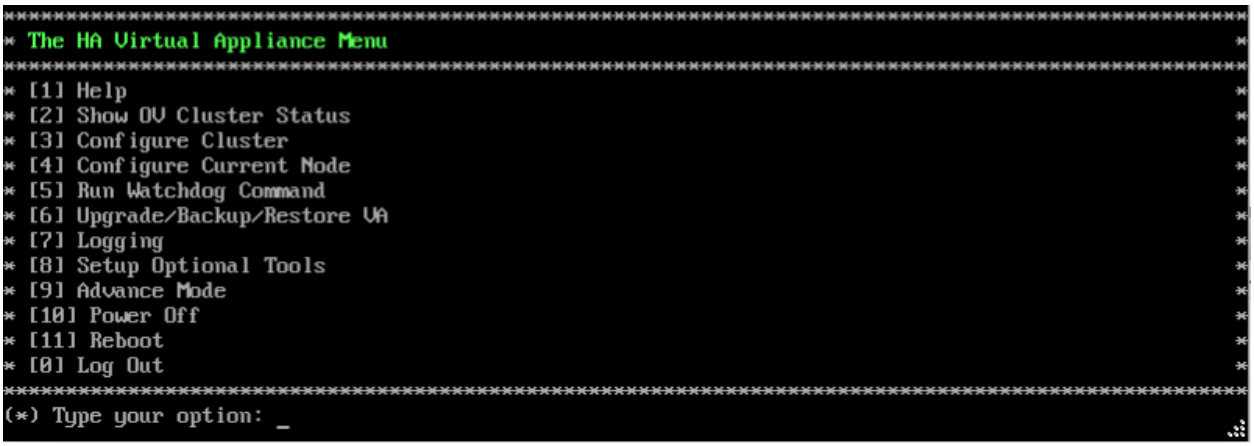
3. Enter **16 – Enable Maintenance Mode**, then enter **y** and press **Enter** to enable Maintenance Mode. Press **Enter** again to continue and return to the Configure Cluster Menu.



4. On the Configure Cluster Menu, select **0 – Exit** to return to the HA Virtual Appliance Menu. You can now shutdown the Standby Node.

Shutdown the Standby Node

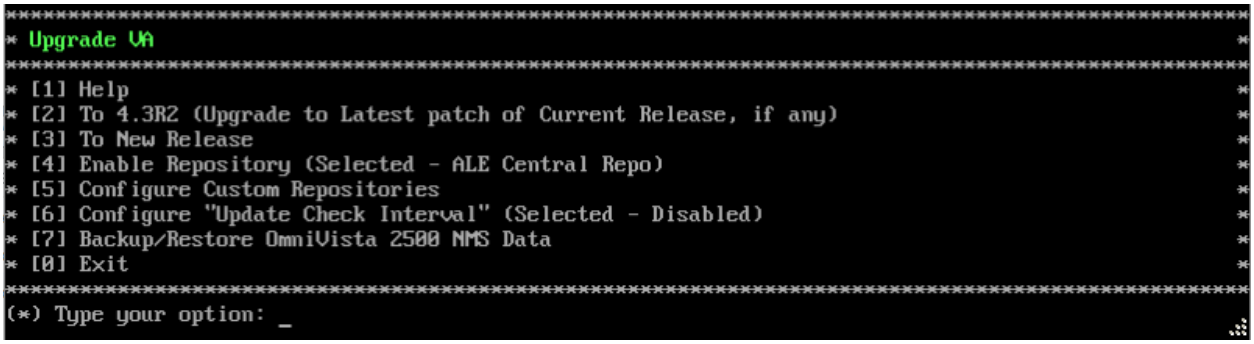
1. Open a Console on the OV 2500 NMS-E 4.3R2 Standby Node VM.



2. Enter **10 – Power Off** to power off the VM. Enter **y** and press **Enter** at the Confirmation Prompt. When the shutdown is complete, upgrade the Active Node.

Upgrade the Active Node

1. On the HA Virtual Appliance Menu, select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.



Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

2. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu.

Warning: If you select **2 – To 4.3R2** (Upgrade to Latest patch of Current Release, if any), the following warning message will be displayed: “No package available” as you are at latest patch. You must select **3 – To New Release**.

3. Enter **1 - Upgrade to 4.3R3** and press **Enter** to bring up the Upgrade System Options Menu.

```
**********************************************************************************************************
* Upgrade System Options                                                                                 *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Download and Upgrade                                                                               *
* [3] Download Only                                                                                      *
* [4] Upgrade from downloaded package                                                                    *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option: _
```

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R2 GA
Build Number: 24
Patch Number: 1

Checking available packages for 4.3R3 operation is in progress...
Upgrade to 4.3R3 release is available after upgrading latest to the build of 4.3R2 release
Do you want to continue to check upgrade for 4.3R2 release now [y|n] (n):
```

5. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.3R3.

```
Getting upgrade information for 4.3R3...
Upgrade information for 4.3R3
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R3
Release     : 21.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.3R3
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.3R3 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (5s)....
```

6. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R3.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the

Configure The Virtual Appliance Menu (from the HA Virtual Appliance Menu, select **4 - Configure Current Node** to access the menu).

7. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

8. The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration for more details.

9. After verifying the upgrade, start up the Standby Node.

Important Note: The upgrade on the Active Node must be complete, **before** you start up and upgrade the Standby Node.

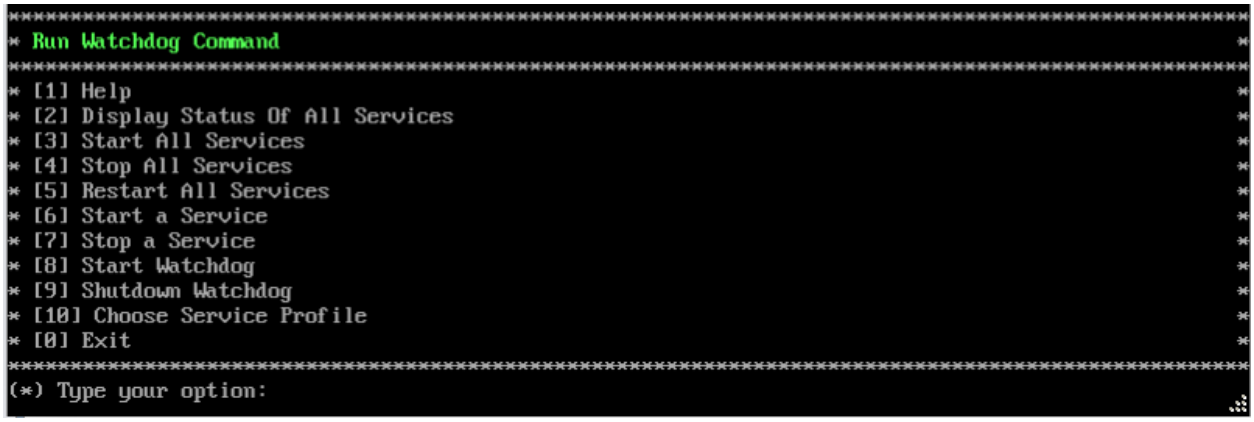
Startup the Standby Node

1. Power on the Standby Node and log into the VM. The HA Virtual Appliance Menu will appear. Once the Standby Node is powered up (all services are running), stop all Watchdog Services on the Standby Node.

Stop All Watchdog Services on the Standby Node

1. Open a Console on the OV 2500 NMS-E 4.3R2 Standby Node.

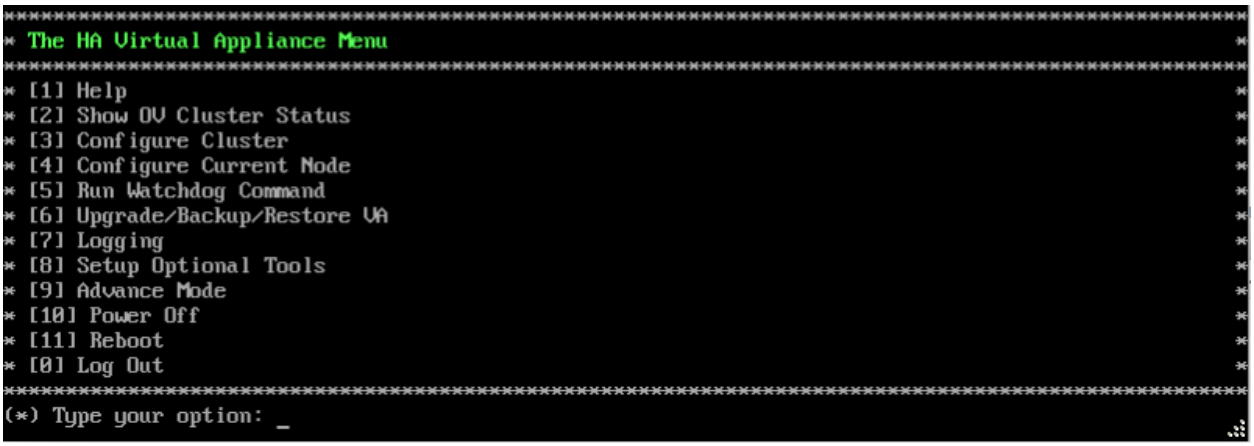
2. On the HA Virtual Appliance Menu, enter **5 - Run Watchdog Command** to bring up the Run Watchdog Command Menu.



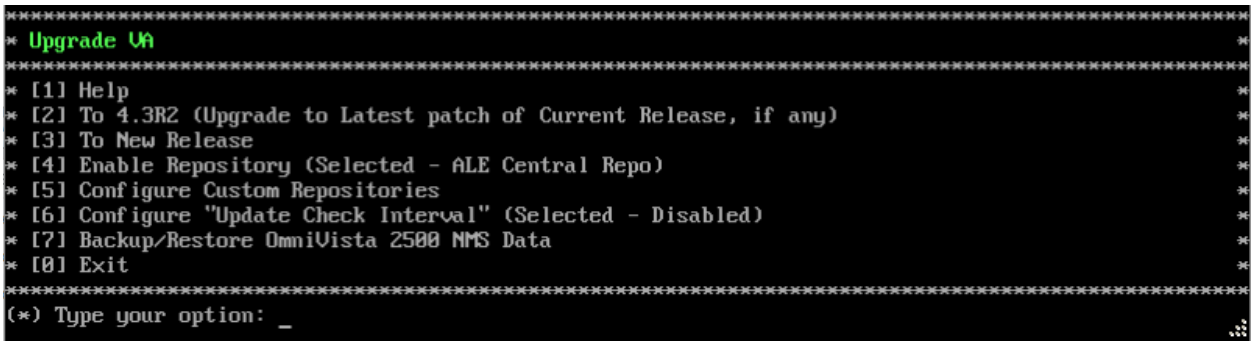
3. Enter **4 – Stop All Services**, then enter **y** and press **Enter** at the Confirmation Prompt. After about a minute, OmniVista will begin stopping services and display the progress. When all services have stopped, OmniVista will display "Watchdog is done stopping all services – Done" and the Run Watchdog Command Menu will appear. Upgrade the Standby Node.

Upgrade the Standby Node

1. On the Run Watchdog Command Menu, enter **0 – Exit** to return to the HA Virtual Appliance Menu.



2. Select **6 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu.



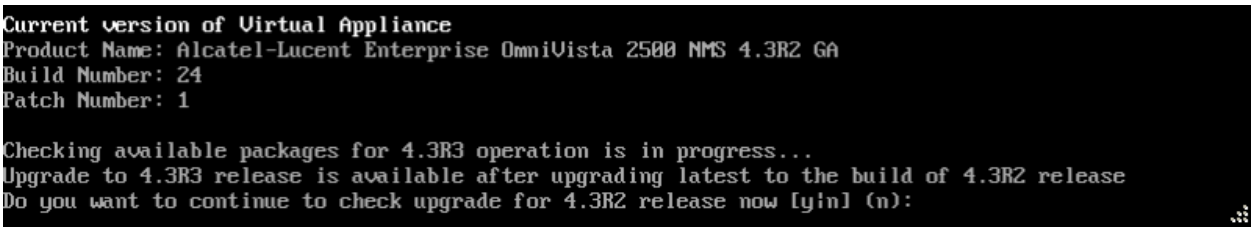
Note: It is recommended that you use the default ALE Central Repo in Option 4 above. If you already have a different repository name, you can use it, and continue with the next step.

3. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu.

Warning: If you select **2 – To 4.3R2** (Upgrade to Latest patch of Current Release, if any), the following warning message will be displayed: “No package available” as you are at latest patch. You must select **3 – To New Release**.

4. Enter **1 - Upgrade to 4.3R3** and press **Enter** to bring up the Upgrade System Options Menu.

5. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.



6. Enter **y** and press **Enter** at the Confirmation Prompt. OmniVista will retrieve and display upgrade information for 4.3R3.

```
Getting upgrade information for 4.3R3...
Upgrade information for 4.3R3
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R3
Release     : 21.0.el7
Size        : 1.3 G
Repo        : CustomRepo1_4.3R3
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.3R3 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (5s)....
```

7. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R3.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the HA Virtual Appliance Menu, select **4 - Configure Current Node** to access the menu).

8. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
You can safely ignore any warnings that may have been displayed above
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Please turn off maintenance mode after restarting.
Press [Enter] to continue
```

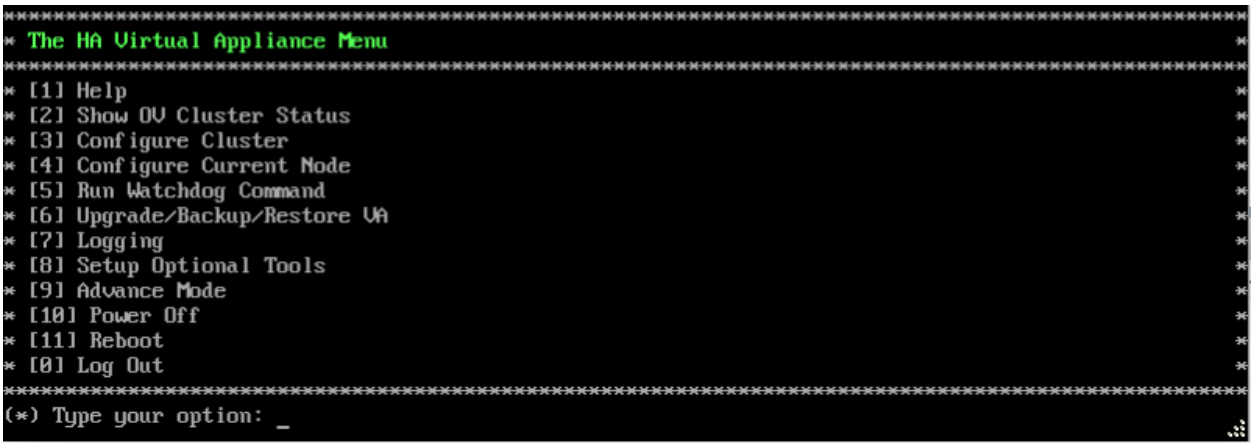
9. The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the HA Virtual Appliance Menu and select option **4 – Configure Current Node**, then select option **2 – Display Current Node Configuration** to view the current Build Number. See Display Current Node Configuration

When the upgrade is complete, shutdown the Standby Node.

Shutdown the Standby Node

1. Open a Console on the OV 2500 NMS-E 4.3R2 Standby Node VM.

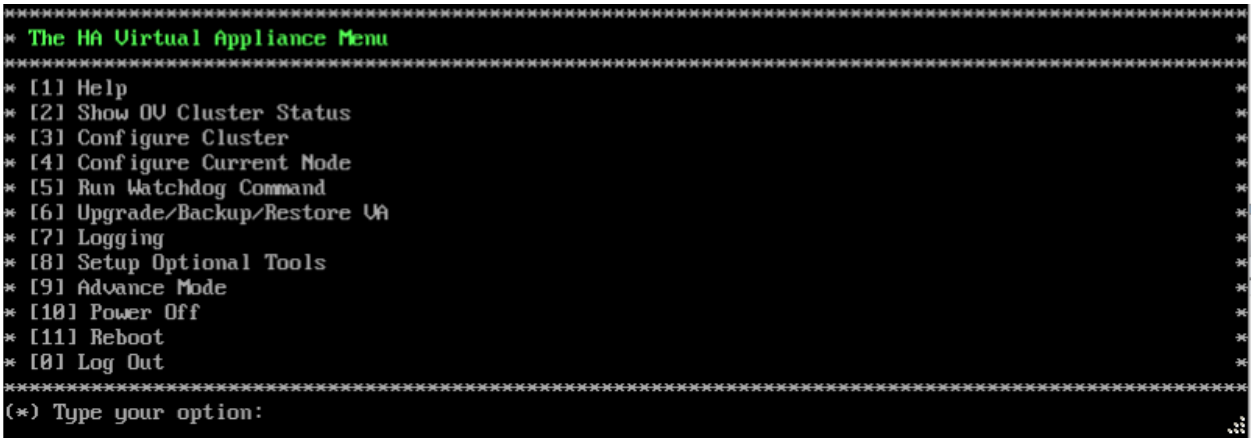


2. Enter **10 – Power Off** to power off the VM. Enter **y** and press **Enter** at the Confirmation Prompt. When the shutdown is complete, disable Maintenance Mode on the Active Node.

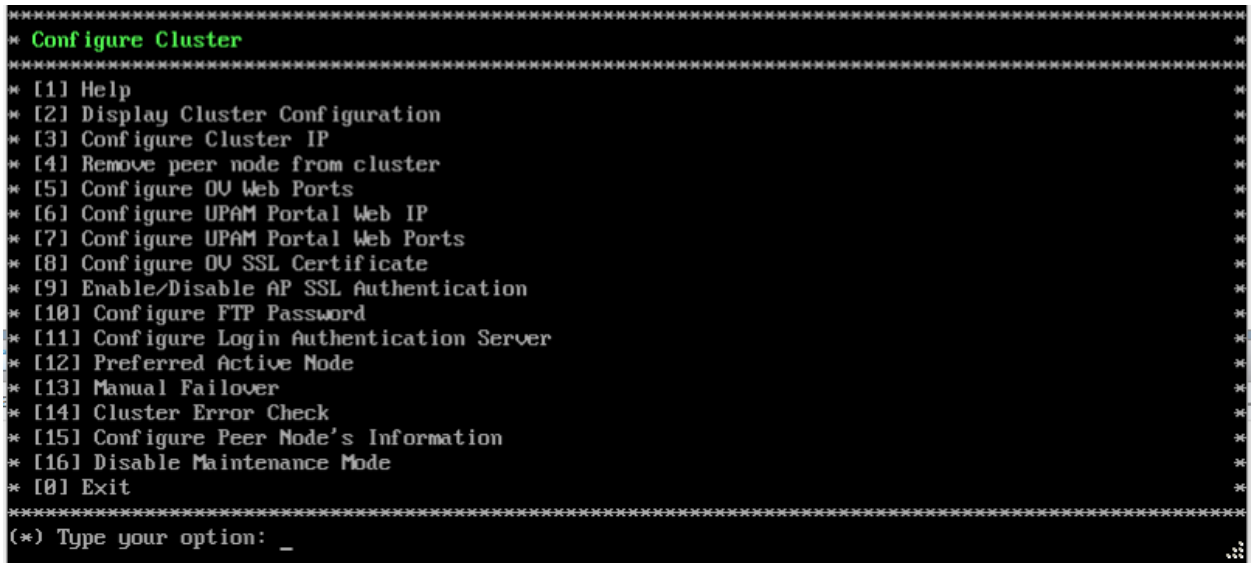
Disable Maintenance Mode on the Active Node

Open a console on the Active Node to disable Maintenance Mode. This will disable Maintenance Mode on both nodes in the Cluster.

1. Go to the HA Virtual Appliance Menu.



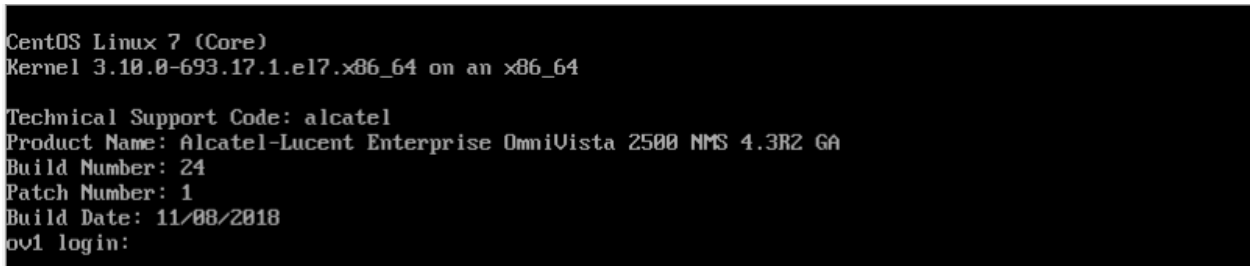
2. Select **3 – Configure Cluster**. The Configure Cluster Menu appears.



3. Enter **16 – Disable Maintenance Mode**, then enter **y** and press **Enter**. The Configure Cluster Menu will appear. Select **0 – Exit**, to return to the HA Virtual Appliance Menu. Startup the Standby Node.

Startup the Standby Node

1. Power on the Standby Node.



2. Login to the VM. The HA Virtual Appliance Menu will appear. When the Standby Node is powered up, verify the upgrade.

Verify the Upgrade

When the upgrade is complete on both nodes and Maintenance Mode is disabled, verify that all services are running on both nodes, that the Cluster Status is “Up to Date”, and that the node roles are correct. And take a configuration snapshot.

- Verify that the all services are running on each node.
  - On the HA Virtual Appliance Menu select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details. Note that on the Standby Node, all services should be running except upam, radius, and nginx. It is the expected behavior on the Standby Node that these services will be “Stopped”.
- Verify that the Cluster Status is “Up to Date” and that the node roles (Active/Standby) are correct. This can be performed on either node.
  - On the HA Virtual Appliance Menu select option **2 – Show OV Cluster Status**. The data sync status indicates whether the data between two nodes is in sync. If it is, the

field will indicate “Up to Date”. If it is in the process of syncing, a percentage will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes. The command also displays the role for node you are logged into – “Active” or “Standby”. See Show OV Cluster Status for more details.

- Take a configuration snapshot without selecting the option “Snapshot virtual machine’s memory”. This will help with reverting the VM if the next upgrade path fails.

Once all services are running, upgrade to OmniVista 4.4R1 HA.

Upgrading from 4.3R1 (Fresh Installation) to 4.3R2

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from fresh installation of OV 2500 NMS-E 4.3R1 to OV 2500 NMS-E 4.3R2, before upgrading to 4.3R3.

If you are upgrading from an OV 2500 NMS-E 4.3R1 Standalone Installation you can only upgrade to an OV 4.3R2 Standalone Installation. If you are planning on configuring a High-Availability Installation, you must perform a fresh installation of OV 2500 NMS-E 4.3R2.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

Note that OV 2500 NMS-E 4.3R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

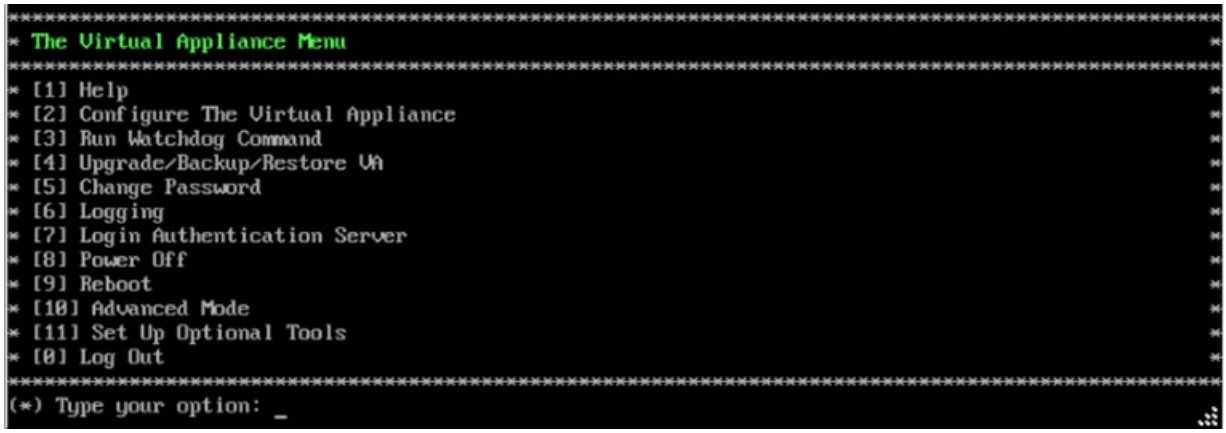
It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured**

to keep the session alive by sending periodic "keepalive" messages. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

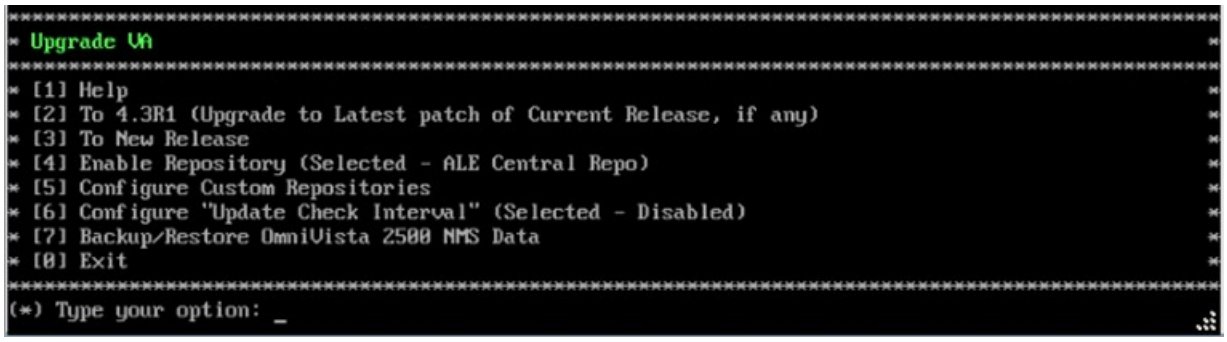
Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

Important Note: During the upgrade process, when presented with the prompt: "Press any key to continue the upgrade", you **must** hit a key **before the countdown expires.** If you do not, the upgrade will automatically begin at the end of the countdown, but it will fail. If this happens, start the upgrade process again and press any key when prompted before the countdown expires.

1. Open a Console on the OV 2500 NMS-E 4.3R1 Virtual Appliance.



2. On the Virtual Appliance Menu, enter **4 – Upgrade/Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

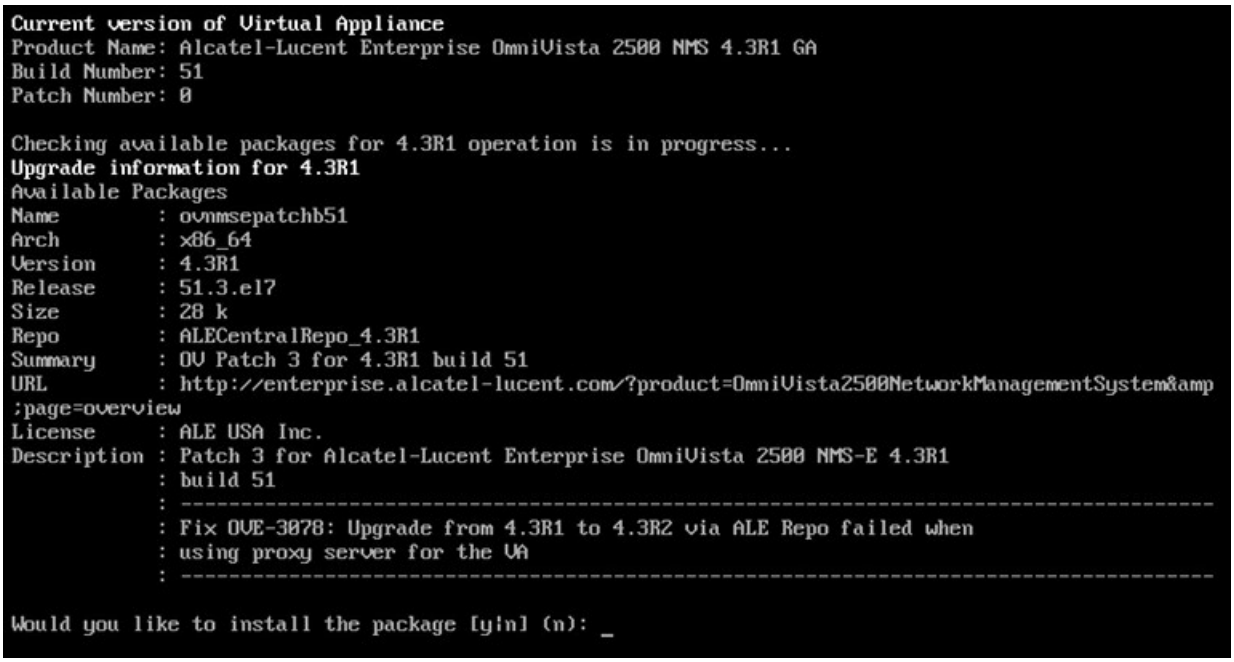


Note: It is not necessary to use the ALE Central Repo in Option 4 above. If you already have a different repository name, you should not change it, and continue with the next step.

3. Enter **2 – To 4.3R1 (Upgrade to Latest patch of Current Release, if any)** and press **Enter** to bring up the Upgrade System Options Menu.

Warning: If you select **3 – To New Release**, the upgrade will fail with the following error message - "/etc/yum.repos.d/ALECentral Repo.repo: Permission denied". You must select **2 – To 4.3R1 (Upgrade to Latest patch of Current Release, if any)**.

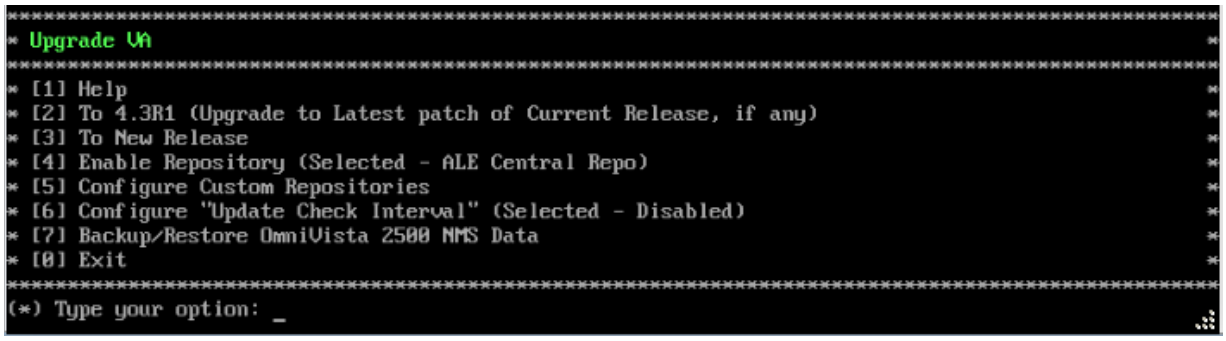
4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.



5. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch.

6. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to reboot the VM.

7. After OmniVista comes up, on the Virtual Appliance Menu, enter **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

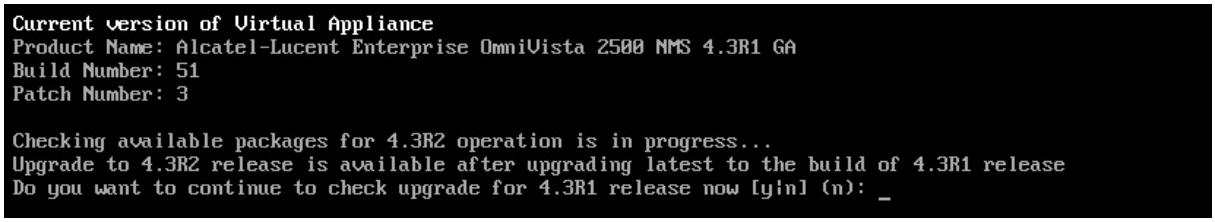


8. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

Warning: If you select **2 – To 4.3R1** (Upgrade to Latest patch of Current Release, if any), the following warning message will be displayed: “No package available” as you are at latest patch. You must select **3 – To New Release**.

9. Enter **1 - Upgrade to 4.3R2** and press **Enter** to bring up the Upgrade System Options Menu.

10. Enter 2 – Download and Upgrade and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.



OmniVista will retrieve and display upgrade information for 4.3R2.

```
Getting upgrade information for 4.3R2...
Upgrade information for 4.3R2
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R2
Release     : 24.0.el7
Size        : 1.3 G
Repo        : ALECentralRepo_4.3R2
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.3R2 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (18s)...
```

11. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R2.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select 2 - Configure The Virtual Appliance to access the menu).

12. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press Enter to continue, then press Enter to reboot the VM.

```
Complete!
Operation is successful
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

13. The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.

- Select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details.

Once all services are running, upgrade to OmniVista 4.3R3.

Upgrading from 4.2.2.R01 (MR2) (Fresh Installation) to 4.3R2

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from OV 2500 Fresh NMS-E 4.2.2.R01 (MR 2) to OV 2500 NMS-E 4.3R2, before upgrading to 4.3R3.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

Note that OV 2500 NMS-E 4.3R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

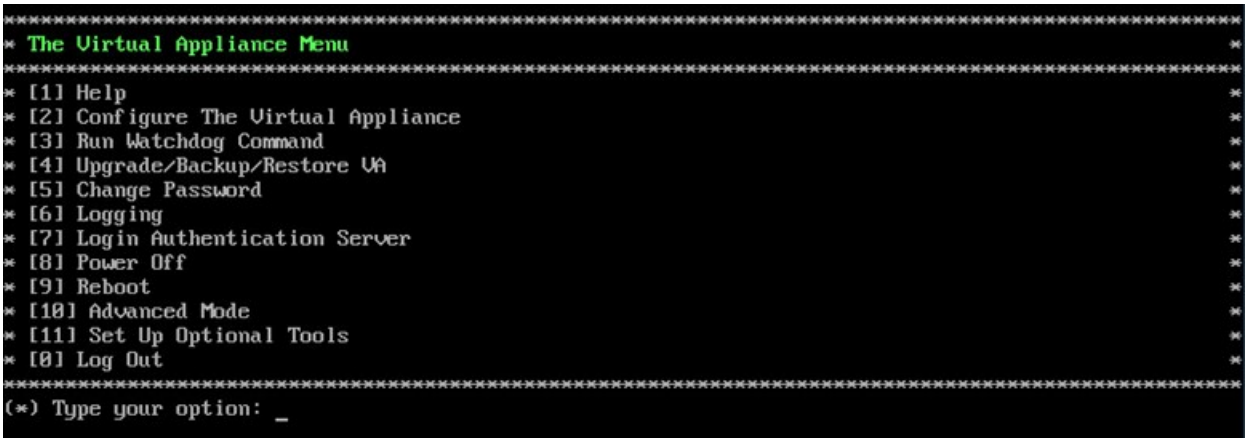
It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

Important Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

Important Note: During the upgrade process, when presented with the prompt: “Press any key to continue the upgrade”, you **must** hit a key **before the countdown expires.** If you do not, the upgrade will automatically begin at the end of the countdown, but it will fail. If this

happens, start the upgrade process again and press any key when prompted before the countdown expires.

1. Open a Console on your existing Virtual Appliance (OV 2500 NMS-E 4.2.2.R01 MR 2).



2. On the Virtual Appliance Menu, enter **4 – Upgrade/Backup/Restore VA**.

3. Enter **2 – To 4.2.2 (Upgrade to Latest patch of Current Release, if any)** and Press **Enter** to bring up the Upgrade System Options Menu.

Warning: If you select **3 – To 4.3R1**, you will receive the following error message: “ovnmsepatchb51-4.3R1-51.3.e17 available, but not installed. No packages marked for update”, and the VA will reboot. After rebooting, you are still at the 4.2.2 MR2 release level. You must select **2 – To 4.2.2 (Upgrade to Latest patch of Current Release, if any)**.

4. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

```
* [2] Download and Upgrade
* [3] Download Only
* [4] Upgrade from downloaded package
* [0] Exit
********************************************************************************************************
(*) Type your option: 2

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.2.R01 MR-2
Build Number: 115
Patch Number: 0

Checking available packages for 4.2.2.R01 operation is in progress...
Upgrade information for 4.2.2.R01
Available Packages
Name        : ovnmsepatchb115
Arch        : x86_64
Version     : 4.2.2.R01
Release     : 115.3.el7
Size        : 38 k
Repo        : ALECentralRepo_4.2.2.R01
Summary     : OV Patch 3 for 4.2.2.R01 build 115
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSy
;page=overview
License     : ALE USA Inc.
Description : Patch 3 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
            : 4.2.2.R01 build 115
            : ------------------------------------------------------------------------------
            : Fix 4.2.2.R01 patch 2 to 4.3R1 patch 3
            : ------------------------------------------------------------------------------

Would you like to install the package [y|n] (n): _
```

5. When the installation is completed, the following message will appear “Complete! Operation is successful”. Press **Enter** to reboot the VM.

```
  Verifying  : ovnmsepatchb115-4.2.2.R01-115.3.el7.x86_64                  1/1

Installed:
  ovnmsepatchb115.x86_64 0:4.2.2.R01-115.3.el7

Complete!
Operation is successful
Press [Enter] to continue
```

6. After OmniVista comes up, on the Virtual Appliance Menu, enter **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

```
********************************************************************************************************
* Upgrade VA                                                                                           *
********************************************************************************************************
* [1] Help                                                                                             *
* [2] 4.2.2 (Upgrade to Latest patch of Current Release, if any)                                       *
* [3] 4.3R1 (New Release)                                                                              *
* [4] Enable Repository (Selected - ALE Central Repo)                                                  *
* [5] Configure Custom Repositories                                                                    *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                          *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                           *
* [0] Exit                                                                                             *
********************************************************************************************************
(*) Type your option: 3
```

7. Enter **3 – To 4.3R1** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

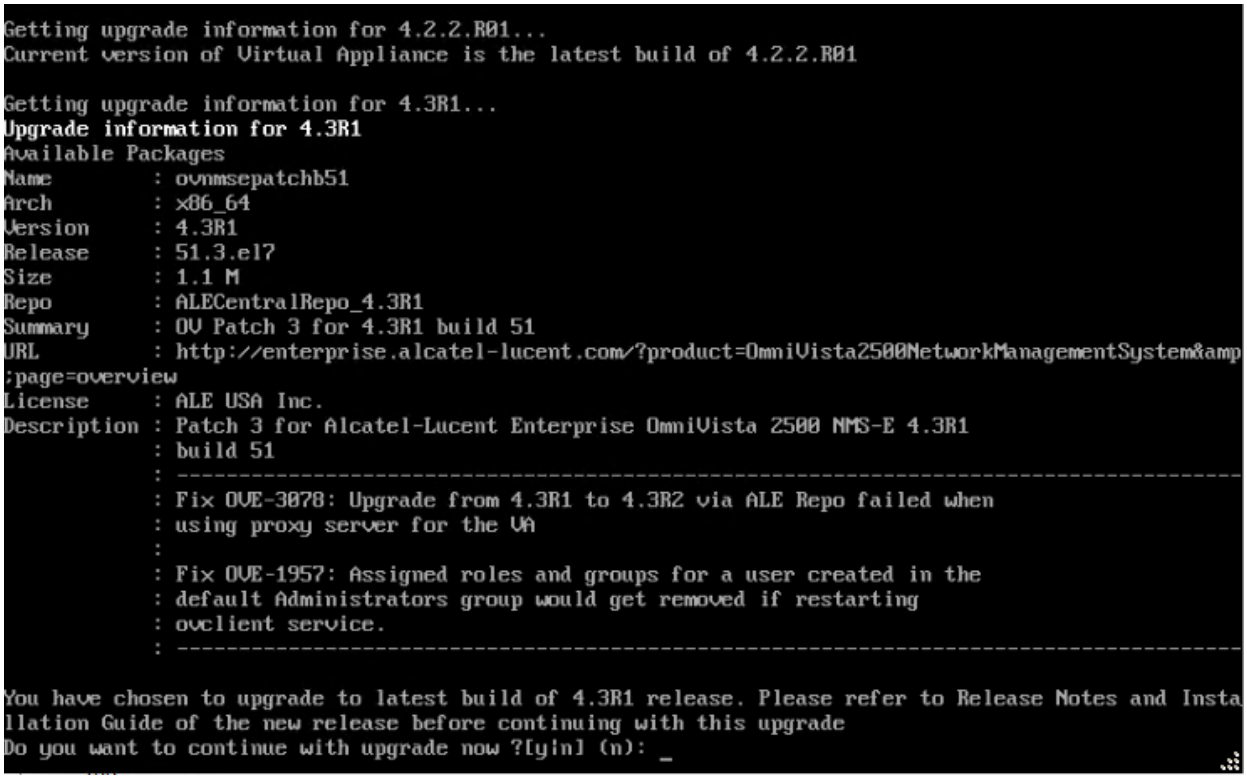
8. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size.

Note: “no such file or directory” error messages may appear during the upgrade process. These can be ignored. Allow the upgrade process to complete.

Note: If you are unable to connect to the repository, you will receive the following error message: “Please check the connectivity of your repository configuration”. Configure the Proxy and/or DNS Settings and try again. Proxy and DNS configuration is available in the Configure The Virtual Appliance Menu (from the Virtual Appliance Menu, select **2 - Configure The Virtual Appliance** to access the menu).

9. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R1 Patch 3.

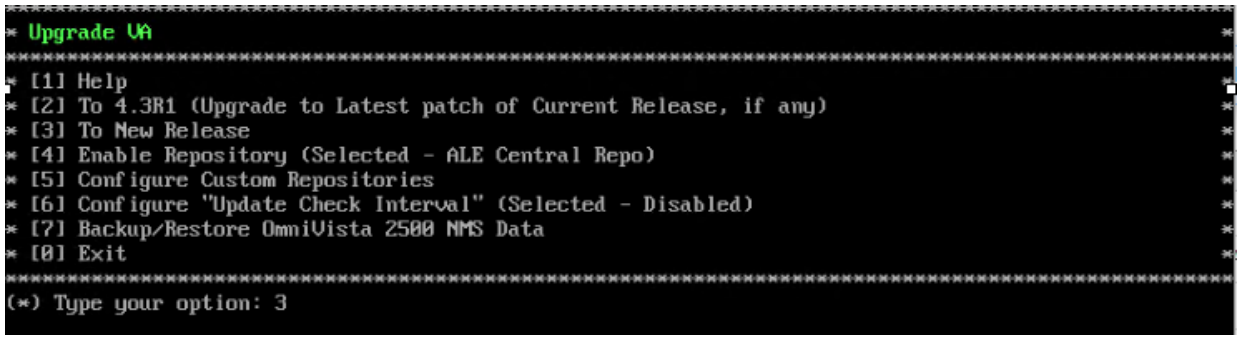


10. When the installation is completed, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

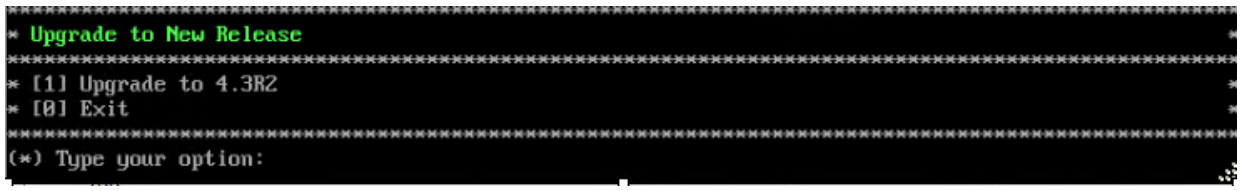
11. After OmniVista comes up, on the Virtual Appliance Menu, enter **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

12. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

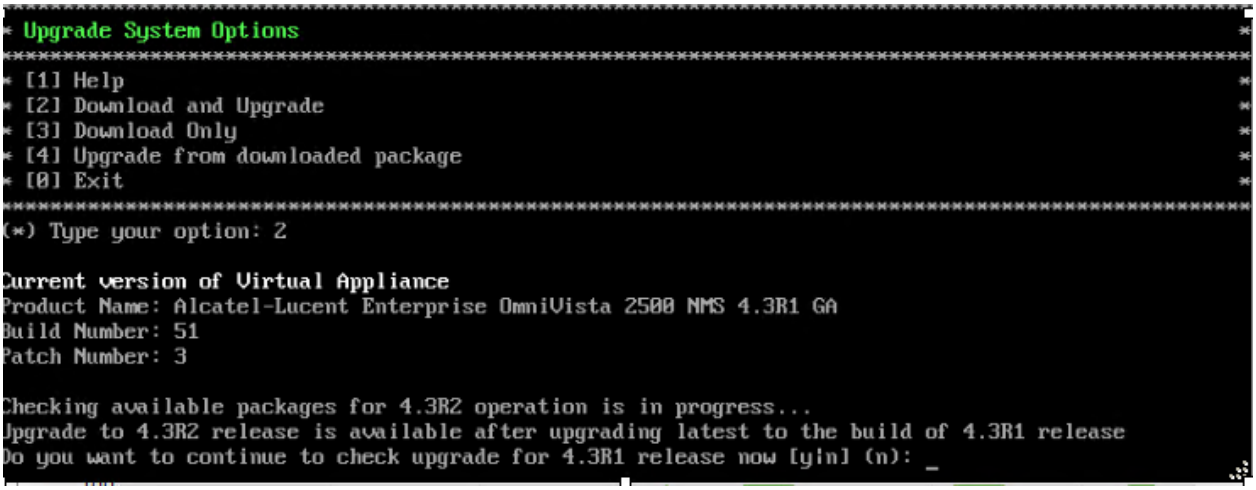
Note: If you select **2 – To 4.3R1 (Upgrade to Latest patch of Current Release, if any)**, the following warning message will be displayed: “No package available” as you are at latest patch. You **must** select **3 – To New Release**.



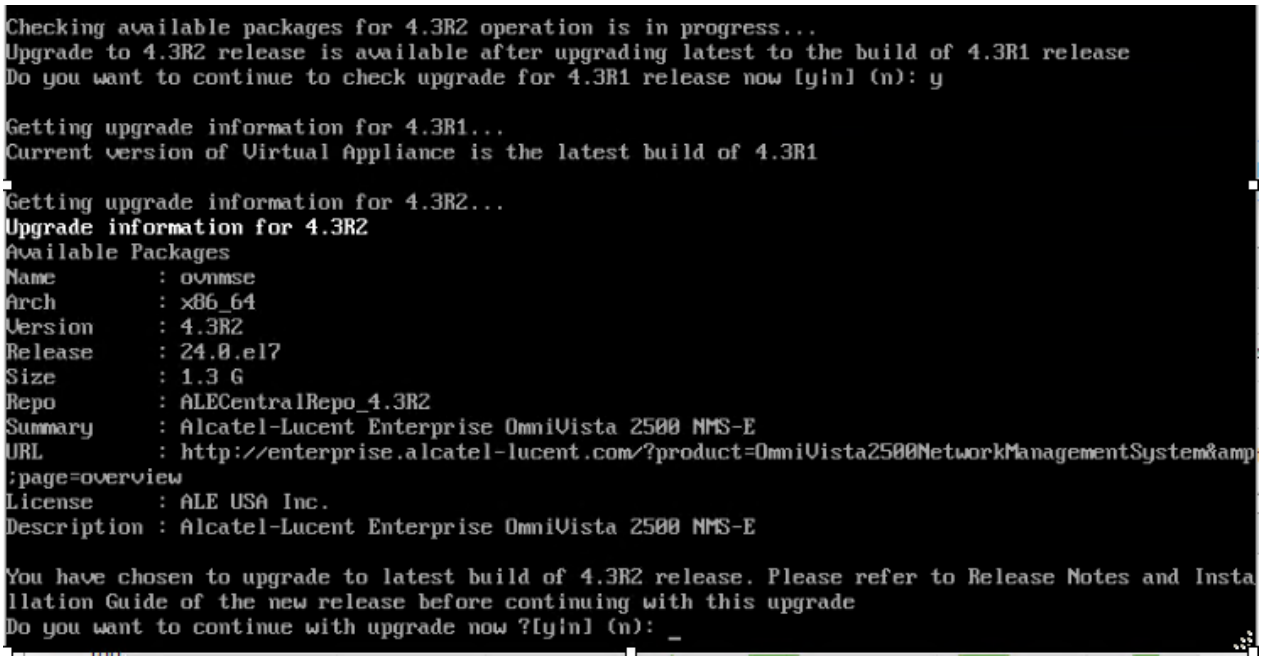
13. Enter **1 - Upgrade to 4.3R2** and press **Enter** to bring up the Upgrade System Options Menu.



14. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. **I**nformation on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.



15. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R2.



16. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

17. The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade.

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.
  - Select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details.

Once all services are running, upgrade to OmniVista 4.3R3.

Upgrading from 4.2.2.R01 (GA) or 4.2.2.R01 (MR2) (Upgrade) to 4.3R2

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from 4.2.2.R01 (GA) or 4.2.2.R01 (MR2) (upgraded from a previous version – not a fresh installation) to 4.3R2, before upgrading to 4.3R3.

Important Notes: Before beginning the upgrade:

- Take a VM Snapshot of the current OmniVista VA. Note that VM snapshots can cause performance issues on the running VM. When upgrading OmniVista, it is recommended that you delete any previous snapshots, take a new snapshot of the current VM configuration, then perform the upgrade. After OmniVista is successfully upgraded, it is recommended that you also delete the snapshot taken prior to the upgrade. For long-term VM backups, consult the virtualization software documentation for recommended procedures.
- Move old OmniVista Server Backup files to external storage (SFTP to OmniVista using port 22 and the “cliadmin” login to access the files under “backups” directory).
- Copy old switch backup files to external storage for archiving purposes if needed (SFTP to OmniVista using port 22 and use the “cliadmin” login to access the files under the “switchbackups” directory), and then delete these old switch backup files from the Resource Manager UI. You can also automatically purge old backup files by configuring a Backup Retention policy (Configuration - Resource Manager Settings). Note that the new retention policy (purging of old backup files) will take effect only when the next switch backup occurs.
- Ensure that there is enough free disk space for OmniVista.
- You can also reduce the default Analytics purge settings for Top N Ports/Switches/ Applications/Clients to free up disk space (default settings are to purge data after 6 or 12 months). The purge will not happen immediately, OmniVista many take up to a day to purge the older data, but it is recommended as a way to save disk space.

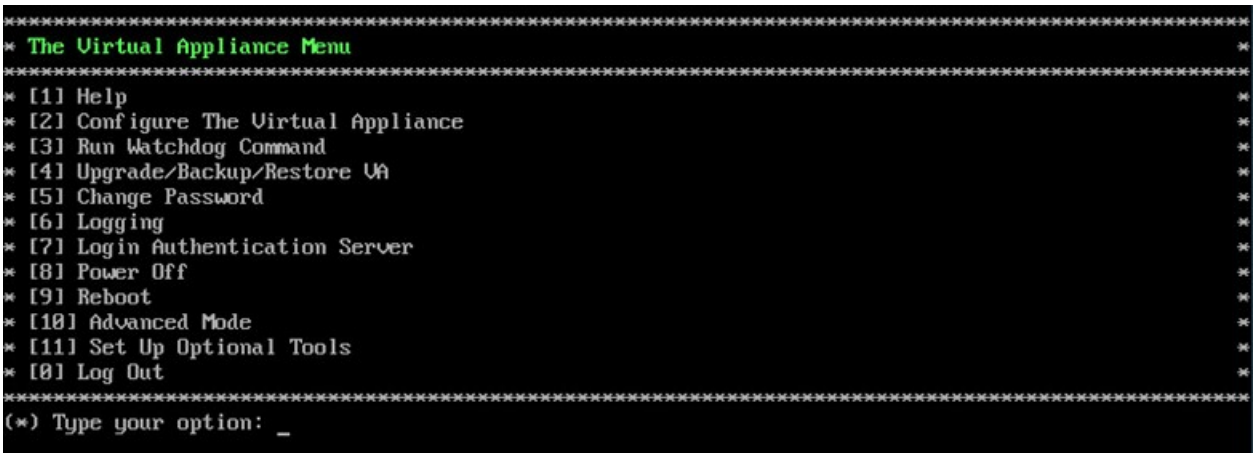
Note that OV 2500 NMS-E 4.3R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for software upgrades. If the OmniVista 2500 NMS Server has a direct connection to the Internet, a Proxy is not required. If a Proxy has not been configured, select **2 - Configure The Virtual Appliance** on the Virtual Appliance Menu, then select **15 - Configure Proxy**.

It is highly recommended that you perform the upgrade directly from the VM Console. If you access OmniVista remotely using an SSH client (e.g., putty), **the client should be configured to keep the session alive by sending periodic “keepalive” messages**. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and database size.

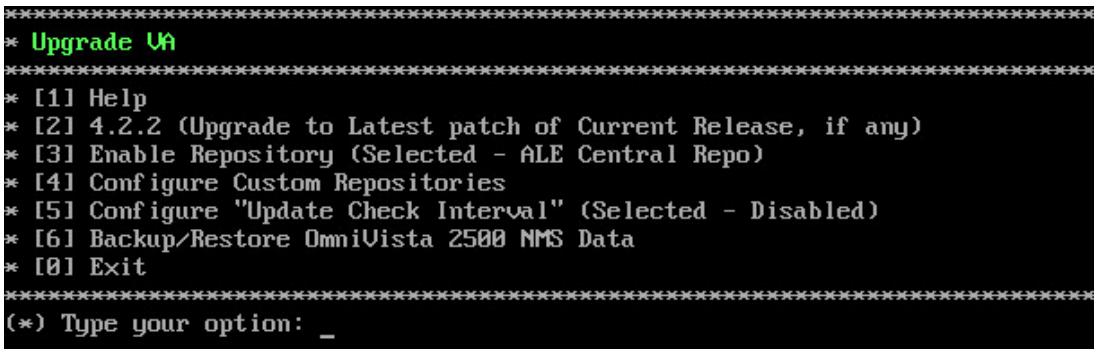
Important Note: Before beginning the upgrade, stop all Watchdog Services using the Run Watchdog Command in the VA Menu.

Important Note: During the upgrade process, when presented with the prompt: “Press any key to continue the upgrade”, you **must** hit a key **before the countdown expires.** If you do not, the upgrade will automatically begin at the end of the countdown, but it will fail. If this happens, start the upgrade process again and press any key when prompted before the countdown expires.

1. Open a Console on the OV 2500 NMS-E 4.2.2.R01 GA Virtual Appliance.



2. On the Virtual Appliance Menu, select option **4 – Upgrade/Backup/Restore VA**.



3. Enter **2 – To 4.2.2** (Upgrade to Latest patch of Current Release, if any) and Press **Enter** to bring up the Upgrade System Options Menu.

4. Enter 2 – Download and Upgrade and press **Enter** to begin the upgrade. **I**nformation on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

```
**********************************************************************************************************
* Upgrade System Options                                                                                 *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Download and Upgrade                                                                               *
* [3] Download Only                                                                                      *
* [4] Upgrade from downloaded package                                                                    *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option: 2

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.2.R01 GA
Build Number: 81
Patch Number: 0

Checking available packages for 4.2.2.R01 operation is in progress...
Upgrade information for 4.2.2.R01
Available Packages
Name        : ovnmsepatchb115
Arch        : x86_64
Version     : 4.2.2.R01
Release     : 115.3.el7
Size        : 38 k
Repo        : ALECentralRepo_4.2.2.R01
Summary     : OV Patch 3 for 4.2.2.R01 build 115
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Patch 3 for Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
            : 4.2.2.R01 build 115
            : ----------------------------------------------------------------------------------------
            : Fix 4.2.2.R01 patch 2 to 4.3R1 patch 3
            : ----------------------------------------------------------------------------------------

Would you like to install the package [y|n] (n): y
```

5. Enter **y** and press **Enter** at the Confirmation Prompts to apply the patch.

6. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to reboot the VM.

```
Complete!
Operation is successful
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

7. After OmniVista comes up, on the Virtual Appliance Menu, select option **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

```
**********************************************************************************************************
* Upgrade VA                                                                                             *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] 4.2.2 (Upgrade to Latest patch of Current Release, if any)                                         *
* [3] 4.3R1 (New Release)                                                                                *
* [4] Enable Repository (Selected - ALE Central Repo)                                                    *
* [5] Configure Custom Repositories                                                                      *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                            *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                             *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

8. Enter **5** and press Enter to configure a Custom Repository.

9. Select a Custom Repository (e.g., **2** – "Custom Repo 1" Repository) and press **Enter**.

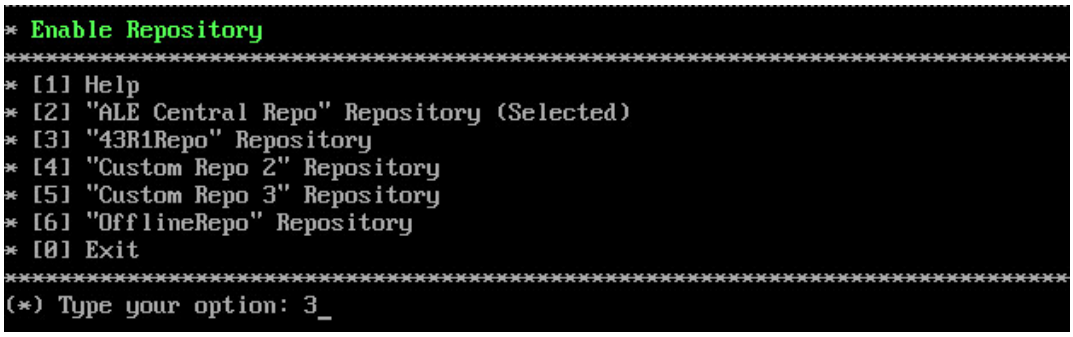
Note: The Custom Repository should be created with an **unused** custom repository from the Configure Custom Repositories Menu option (e.g. "Custom Repo 1", "Custom Repo 2" or "Custom Repo 3").

10. Configure the repository as described below, then Enter **y** and press **Enter** to confirm the configuration.

- Repository Name – 43R1Repo
- Repository URL Host – ovrepo.fluentnetworking.com
- Repository URL Location – ov

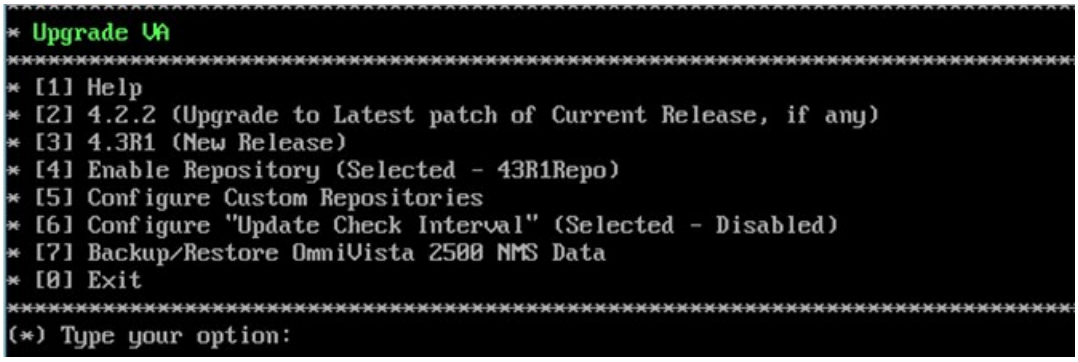
11. Enter **0** and press **Enter** to exit to the Upgrade VA Menu.

12. Enter **4** and press **Enter** to bring up the Enable Repository Menu.



13. Select the Custom Repository you just created (e.g., 3 – "43R1Repo" Repository) and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. The Custom Repository you enabled will be designated as "Selected", as shown below.

14. Enter **0** and press **Enter** to exit to the Upgrade VA Menu.

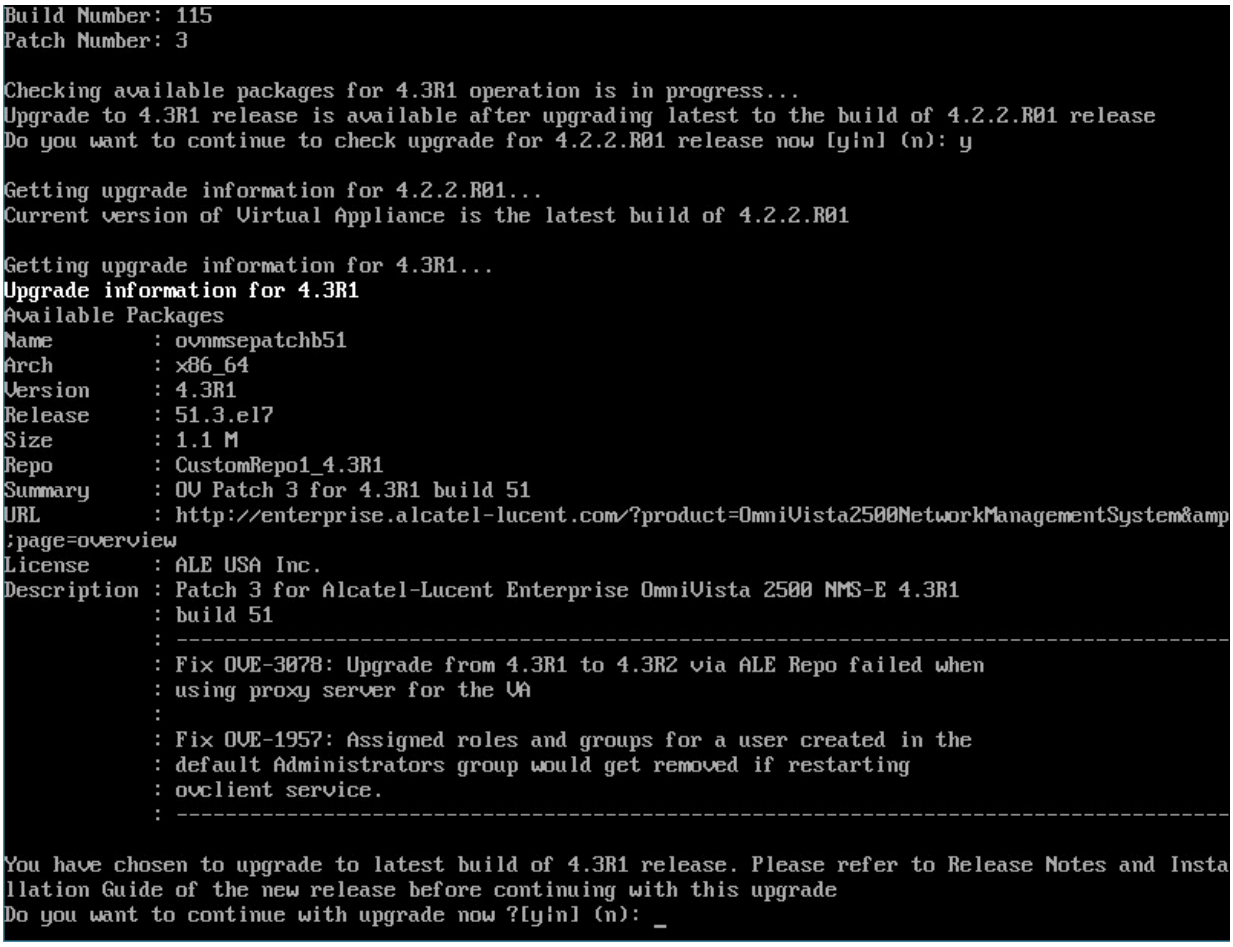


15. Enter **3 – To 4.3R1 (New Release)** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

> **Note:** If you select **2 – To 4.2.2** (Upgrade to Latest patch of Current Release, if any), the following warning message will be displayed: "No package available" as you are at latest patch. You **must** select **3 – To 4.3R1 (New Release)**.

16. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. **I**nformation on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

17. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R1 Patch 3.



18. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

19. After OmniVista comes up, on the Virtual Appliance Menu, select option **4 – Upgrade/ Backup/Restore VA** and press **Enter** to bring up the Upgrade VA Menu Screen.

20. Enter **3 – To New Release** and press **Enter** to bring up the Upgrade to New Release Menu Screen.

> **Note:** If you select **2 – To 4.3R1** (Upgrade to Latest patch of Current Release, if any), the following warning message will be displayed: “No package available” as you are at latest patch. You **must** select **3 – To New Release**.

21. Enter **1 - Upgrade to 4.3R2** and press **Enter** to bring up the Upgrade System Options Menu.

22. Enter **2 – Download and Upgrade** and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages. Enter **y** and press **Enter** at the Confirmation Prompt.

```
Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R1 GA
Build Number: 51
Patch Number: 3

Checking available packages for 4.3R2 operation is in progress...
Upgrade to 4.3R2 release is available after upgrading latest to the build of 4.3R1 release
Do you want to continue to check upgrade for 4.3R1 release now [y|n] (n): _
```

23. Enter **y** and press **Enter** at the Confirmation Prompts to upgrade to 4.3R2.

```
Getting upgrade information for 4.3R2...
Upgrade information for 4.3R2
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R2
Release     : 24.0.el7
Size        : 1.3 G
Repo        : ALECentralRepo_4.3R2
Summary     : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL         : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&amp
;page=overview
License     : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have chosen to upgrade to latest build of 4.3R2 release. Please refer to Release Notes and Insta
llation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now ?[y|n] (n): y
This operation can result in data loss or corruption. We advise taking a VM snapshot and read Instal
l guide, Release Notes of new release prior to this.
Are you ready to proceed ? [y|n] (n): y
Build download is in progress, it may take long time depending on n/w speed
Warning messages may be shown during upgrading. This is a normal case that the RPM installer tries t
o remove unexisting files. You can ignore them.
Press any key to continue the upgrade (18s)...
```

24. When the installation is complete, the following message will appear “Complete! Operation is successful”. Press **Enter** to continue, then press **Enter** to reboot the VM.

```
Complete!
Operation is successful
Press [Enter] to continue

The Virtual Appliance has to be restarted for applying new changes
Press [Enter] to continue
```

The reboot process will take several minutes. When the reboot is complete, log into the VM and verify the upgrade

- Verify that the Build Number is correct.
  - Go to the Virtual Appliance Menu and select option **2 – Configure the Virtual Appliance**, then select option **2 – Display the Current Configuration** to view the current Build Number. See Display Current Configuration for more details.
- Verify that all services have started.
  - From the Configure the Virtual Appliance Menu, select option **0 – Exit** to go to The Virtual Appliance Menu.

- Select option **3 – Run Watchdog Command**, then select option **3 – Display Status of All Services**. See Run Watchdog Command for more details.

Once all services are running, upgrade to OmniVista 4.3R3.

Appendix A – Installing Virtual Box

If you are deploying OV 2500 NMS-E 4.3R3 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download.

Go to https://www.virtualbox.org/wiki/Downloads. Click on the applicable download link (e.g., Windows Hosts). The sections below provide procedures for installing Virtual Box on Windows or Linux Hosts. See the Oracle VM Virtual Box documentation for additional information.

Supported Hosts

Virtual Box runs on the following host operating systems:

- **Windows Hosts:**
  - Windows Vista SP1 and later (32-bit and 64-bit).
  - Windows Server 2008 (64-bit)
  - Windows Server 2008 R2 (64-bit)
  - Windows 7 (32-bit and 64-bit)
  - Windows 8 (32-bit and 64-bit)
  - Windows 8.1 (32-bit and 64-bit)
  - Windows 10 RTM build 10240 (32-bit and 64-bit)
  - Windows Server 2012 (64-bit)
  - Windows Server 2012 R2 (64-bit).
- **Linux Hosts (32-bit and 64-bit):**
  - Ubuntu 10.04 to 15.04
  - Debian GNU/Linux 6.0 ("Squeeze") and 8.0 ("Jessie")
  - Oracle Enterprise Linux 5, Oracle Linux 6 and 7
  - Redhat Enterprise Linux 5, 6 and 7
  - Fedora Core / Fedora 6 to 22
  - Gentoo Linux
  - openSUSE 11.4, 12.1, 12.2, 13.1
  - Mandriva 2011.

Installing Virtual Box on Windows Hosts

The Virtual Box installation can be started by double-clicking on the downloaded executable file (contains both 32- and 64-bit architectures), **or** by entering:

```
VirtualBox.exe –extract
```

on the command line. This will extract both installers into a temporary directory in which you will find the usual .MSI files. You can then perform the installation by entering:

```
msiexec /i Virtual Box-<version>-MultiArch_<x86|amd64>.msi
```

In either case, this will display the installation welcome dialog and allow you to choose where to install Virtual Box to and which components to install. In addition to the Virtual Box application, the following components are available:

- USB Support:
  - This package contains special drivers for your Windows host that Virtual Box requires to fully support USB devices inside your virtual machines.
- Networking
  - This package contains extra networking drivers for your Windows host that Virtual Box needs to support Bridged Networking (to make your VM's virtual network cards accessible from other machines on your physical network).
- Python Support
  - This package contains Python scripting support for the Virtual Box API. For this to work, a working Windows Python installation on the system is required.

The Virtual Box 5.2.x Setup Wizard will guide you through the installation. Depending on your Windows configuration, you may see warnings about "unsigned drivers", etc. Please allow these installations as otherwise Virtual Box might not function correctly after installation.

With standard settings, Virtual Box will be installed for all users on the local system; and the installer will create a "Virtual Box" group in the Windows "Start" menu which allows you to launch the application and access its documentation.

Installing Virtual Box on Linux Hosts

Virtual Box is available in a number of package formats native to various common Linux distributions. In addition, there is an alternative generic installer (.run) which should work on most Linux distributions.

Note: If you want to run the Virtual Box graphical user interfaces, the following packages must be installed before starting the Virtual Box installation (some systems will do this for you automatically when you install Virtual Box):

- Qt 4.8.0 or higher;
- SDL 1.2.7 or higher (this graphics library is typically called `libsdl` or similar).

Specifically, Virtual Box, the graphical Virtual Box manager, requires both Qt and SDL. VBoxSDL, our simplified GUI, requires only SDL. If you only want to run VBoxHeadless, neither Qt nor SDL are required.

Installing Virtual Box From a Debian/Ubuntu Package

Download the appropriate package for your distribution. The following examples assume that you are installing to a 32-bit Ubuntu Raring system. Use `dpkg` to install the Debian package:

```
sudo dpkg -i virtualbox-5.0_5.2.x_Ubuntu_raring_i386.deb
```

You will be asked to accept the Virtual Box Personal Use and Evaluation License. Unless you answer "yes" here, the installation will be aborted.

The installer will also search for a Virtual Box kernel module suitable for your kernel. The package includes pre-compiled modules for the most common kernel configurations. If no suitable kernel module is found, the installation script tries to build a module itself. If the build process is not successful, a warning is displayed and the package will be left unconfigured. In this case, check `/var/log/vbox-install.log` to find out why the compilation failed. You may have to install the appropriate Linux kernel headers.

After correcting any problems, enter `sudo rcvboxdrv setup` to start a second attempt to build the module. If a suitable kernel module was found in the package or the module was successfully built, the installation script will attempt to load that module.

Once Virtual Box has been successfully installed and configured, you can start it by selecting "Virtual Box" in your start menu or from the command line.

Using the Alternative Installer (VirtualBox.run)

The alternative installer performs the following steps:

- It unpacks the application files to the target directory, `/opt/Virtual Box/`, which cannot be changed.
- It builds the Virtual Box kernel modules (`vboxdrv, vboxnetflt` and `vboxnetadp`) and installs them.
- It creates `/sbin/rcvboxdrv`, an init script to start the Virtual Box kernel module.
- It creates a new system group called `vboxusers`.
- It creates symbolic links in `/usr/bin` to a shell script (`/opt/Virtual Box/VBox`) which does some sanity checks and dispatches to the actual executables, `Virtual Box`, `VBoxSDL`, `VBoxVRDP`, `VBoxHeadless` and `VboxManage`.
- It creates `/etc/udev/rules.d/60-vboxdrv.rules`, a description file for udev, if that is present, which makes the USB devices accessible to all users in the `vboxusers` group.
- It writes the installation directory to `/etc/vbox/vbox.cfg`.

The installer must be executed as root with either `install` or `uninstall` as the first parameter.

```
sudo ./VirtualBox.run install
```

If you do not have the "sudo" command available, run the following as root instead:

```
./VirtualBox.run install
```

Then put every user requiring access to USB devices from Virtual Box guests into the group `vboxusers`, either through the GUI user management tools or by running the following command as root:

```
sudo usermod -a -G vboxusers username
```

> **Note:** The `usermod` command of some older Linux distributions does not support the `-a` option (which adds the user to the given group without affecting membership of other groups). In this case, determine the current group memberships using the `groups` command and add these groups in a comma-separated list to the command line after the `-G` option (e.g., `usermod -G group1,group2,vboxusers username`.)

Performing a Manual Installation

If, for any reason, you cannot use the shell script installer described previously, you can also perform a manual installation. Invoke the installer by entering:

```
./VirtualBox.run --keep --noexec
```

This will unpack all the files needed for installation in the `install` directory under the current directory. The Virtual Box application files are contained in `VirtualBox.tar.bz2` which you can unpack to any directory on your system. For example:

```
sudo mkdir /opt/Virtual Box
sudo tar jxf ./install/VirtualBox.tar.bz2 -C /opt/Virtual Box
```

or as root:

```
mkdir /opt/Virtual Box
tar jxf ./install/VirtualBox.tar.bz2 -C /opt/Virtual Box
```

The sources for VirtualBox's kernel module are provided in the `src` directory. To build the module, change to the directory and issue the following command:

```
make
```

If everything builds correctly, issue the following command to install the module to the appropriate module directory:

```
sudo make install
```

If you do not have sudo, switch the user account to root and enter:

```
make install
```

The Virtual Box kernel module needs a device node to operate. The above make command will tell you how to create the device node, depending on your Linux system. The procedure is slightly different for a classical Linux setup with a `/dev` directory, a system with the now deprecated `devfs` and a modern Linux system with `udev`.

On certain Linux distributions, you might experience difficulties building the module. You will have to analyze the error messages from the build system to diagnose the cause of the problems. In general, make sure that the correct Linux kernel sources are used for the build process. Note that the `/dev/vboxdrv` kernel module device node must be owned by root:root and must be read/writable only for the user.

Next, you will have to install the system initialization script for the kernel module:

```
cp /opt/Virtual Box/vboxdrv.sh /sbin/rcvboxdrv
```

(assuming you installed Virtual Box to the `/opt/Virtual Box` directory) and activate the initialization script using the right method for your distribution, you should create VirtualBox's configuration file:

```
mkdir /etc/vbox
echo INSTALL_DIR=/opt/Virtual Box > /etc/vbox/vbox.cfg
```

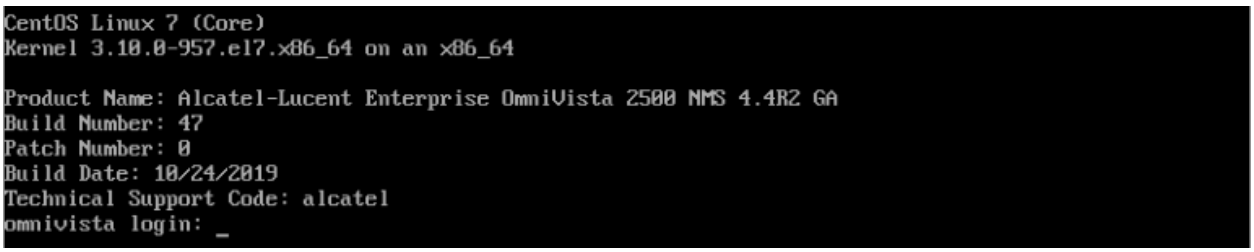
and, for convenience, create the following symbolic links:

```
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/Virtual Box
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxManage
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxHeadless
ln -sf /opt/Virtual Box/VBox.sh /usr/bin/VBoxSDL
```

Appendix B – Using the Virtual Appliance Menu

To access the Virtual Appliance Menu for a VM, launch the Hypervisor Console. The login prompt is displayed.

> **Note:** You can also access the Virtual Appliance Menu by connecting via SSH using port 2222, user **cliadmin,** and password set when deploying VA (e.g., ssh cliadmin@192.160.70.230 –p 2222).



1. Enter the login (**cliadmin**) and press **Enter**.

2. Enter the password and press **Enter**. The password is the one you created when you first launched the VM Console at the beginning of the installation process. The Virtual Appliance Menu is displayed.

The Virtual Appliance Menu provides the following options:

- 1 - Help
- 2 - Configure the Virtual Appliance
- 3 - Run Watchdog Command
- 4 - Upgrade/Backup/Restore VA
- 5 - Change Password
- 6 - Logging
- 7 - Login Authentication Server
- 8 - Power Off
- 9 - Reboot
- 10 - Advanced Mode
- 11 - Set Up Optional Tools

- 12 - Convert to Cluster
- 13 - Join Cluster
- 0 - Log Out

For information on these menu options, refer to the sections below.

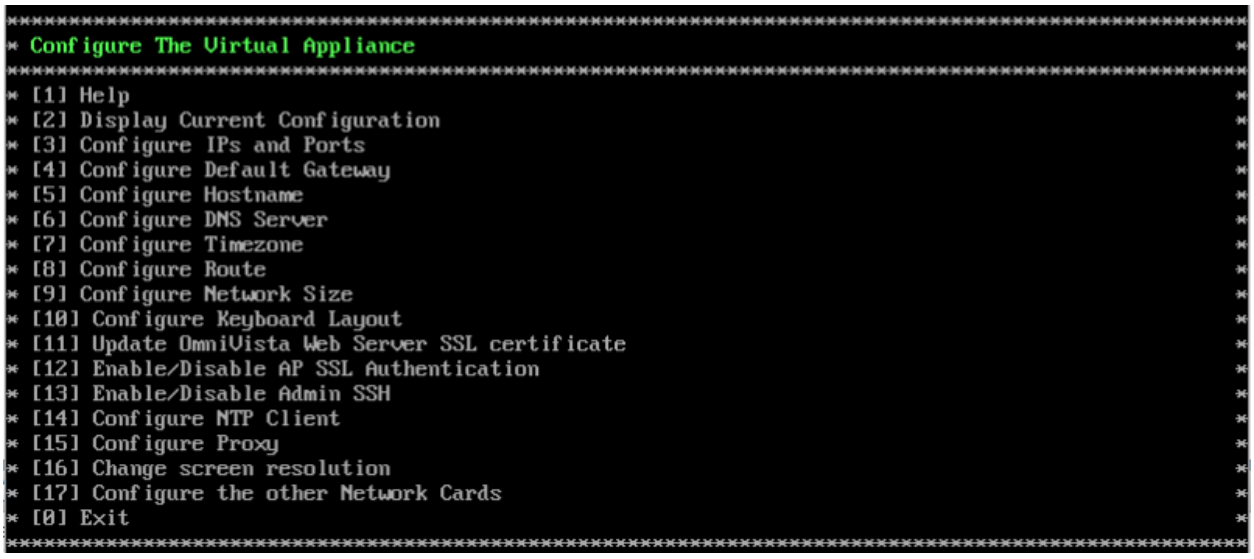
Help

Enter **1** and press **Enter** to bring up help for the Virtual Appliance Menu.

Configure the Virtual Appliance

The “Configure the Virtual Appliance” menu provides the following options:

- 1 - Help
- 2 - Display Current Configuration
- 3 - Configure IPs & Ports
- 4 - Configure Default Gateway
- 5 - Configure Hostname
- 6 - Configure DNS Server
- 7 - Configure Timezone
- 8 - Configure Route
- 9 - Configure Network Size
- 10 - Configure Keyboard Layout
- 11 - Update OmniVista Web Server SSL Certificate
- 12 - Enable/Disable AP SSL Authentication
- 12 - Enable/Disable Admin SSH
- 14 - Configure NTP Client
- 15 - Configure Proxy
- 16 - Change Screen Resolution
- 17 - Configure the Other Network Cards
- 0 - Exit

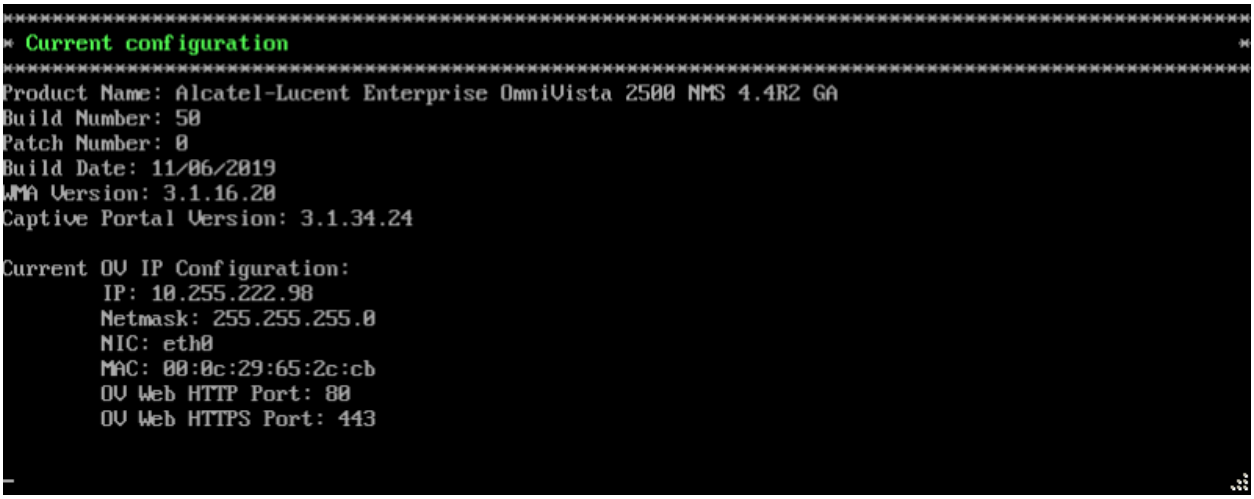


Help

Enter **1** and press **Enter** to bring up help for the Configure The Virtual Appliance Menu.

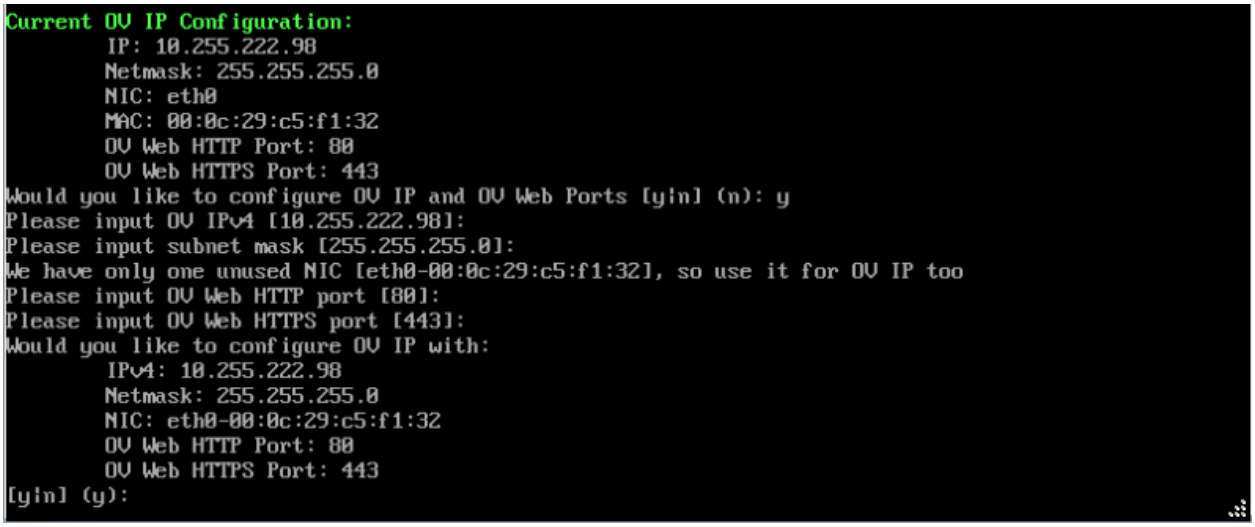
Display Current Configuration

Enter **2** and press **Enter** to display the current VA configuration. Press **Enter** to return to the Configure The Virtual Appliance Menu.



Configure IPs and Ports

1. If you want to re-configure the current OV IP, Captive Portal IP and Ports, and optional Additional Web OV IP, enter **3** and press **Enter**. The current configuration will be displayed. Enter **y** and press **Enter** at the first confirmation prompt to re-configure the OV IP and Web Ports.



2. Enter an IPv4 IP address and subnet mask.

3. Enter **y** at the confirmation prompt and press **Enter** to confirm the settings.

4. After configuring the OV IP address, configure the OV ports.

5. At the prompt, enter an HTTP value and press **Enter**. Enter an HTTPS value and press **Enter**.

- HTTP Port (Valid range: 1024 to 65535, Default = 80)
- HTTPS Port (Valid range: 1024 to 65535, Default = 443)

  Note: You can press **Enter** to accept default values. New port values must be unique (i.e., they must differ from any previously-configured ports).

6. Enter **y** and press **Enter** to confirm the settings.

7. At the Captive Portal Configuration Prompt, enter **y** and press **Enter** to configure the Captive Portal Ports, otherwise press **Enter** to continue. The Captive Portal IP address can be the same as the OV IP address or different. However, if you use a different IP address for Captive Portal it is recommended that you use the default ports. If you do not use the default ports, the ports should be >1024.

- HTTP Port (Valid range: 1024 to 65535, Default = 8080)
- HTTPS Port (Valid range: 1024 to 65535, Default = 8443)

Note: The default Captive Portal FQDN is "ov2500-upam-cportal.al-enterprise.com". If you want to replace it with your own FQDN you must:

1. Log into the OmniVista UI.
2. Go to the UPAM – Captive Portal Certificates page (U PAM – Settings – Captive Portal Certificates).
   - Create a Custom Certificate.
   - Activate the certificate.

8. At the Additional OV Web IP Prompt, enter **y** and press **Enter** to configure an Additional OV Web IP, otherwise press **Enter** to continue. An additional OV Web IP address provides you with another way of accessing the OmniVista UI. It is optional. The OV Web IP address must be

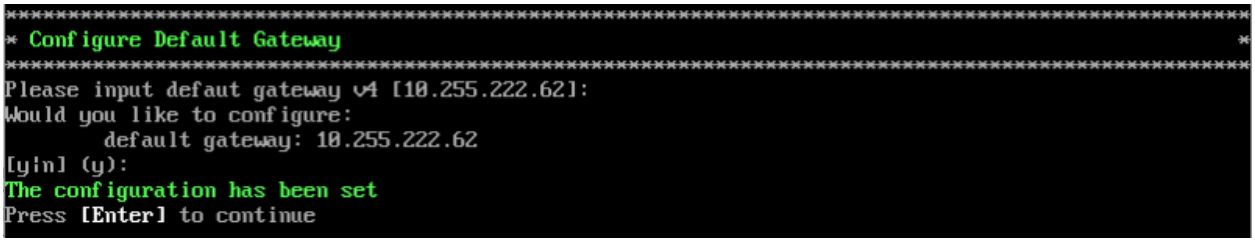
configured on a different NIC and different subnet than the OmniVista IP and Captive Portal IP. If an additional NIC is not available, it cannot be enabled.

After entering values and confirming, you must restart all services for the changes to take effect. Use the **Restart All Services** option in the **Run Watchdog** command in the Virtual Appliance Menu.

> **Important Note:** If you change the OV IP address in the VA Menu, the network is NOT touched. For wired devices, you must reconfigure the sFlow receiver, policy server, and SNMP trap station. After changing the IP Address of the OV Server, you must manually push configurations from various applications (Analytics, Policy View QoS, and Notification applications respectively) to inform the network about the new location of the OV Server. For Stellar APs, you must reconfigure the DHCP Server, and reapply WLAN Services and Global Configurations in Unified Access.
>
> **Note:** If OmniVista is unreachable after you change the OmniVista Server IP address, reboot the OmniVista Server.

Configure Default Gateway

1. Enter **4** and press **Enter** to configure default gateway settings.



2. Enter an IPv4 default gateway.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Hostname

1. The default Hostname is **omnivista**. If you want to change the default Hostname, enter **5** and press **Enter**.

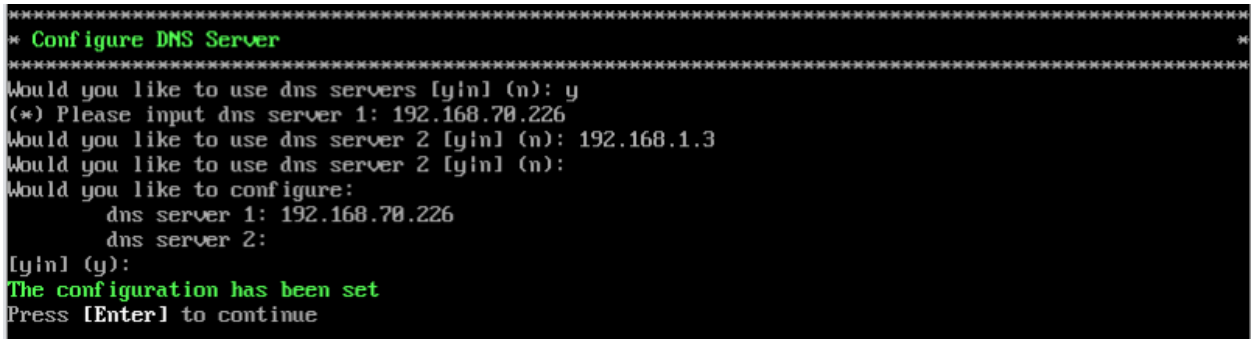
2. Enter a hostname (maximum of 15 characters).

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure DNS Server

1. Enter **6** to specify whether the VM will use a DNS Server.

2. If the VM will use a DNS server, enter **y**, then press **Enter**. Enter the IPv4 address for Server 1 and Server 2, if applicable.

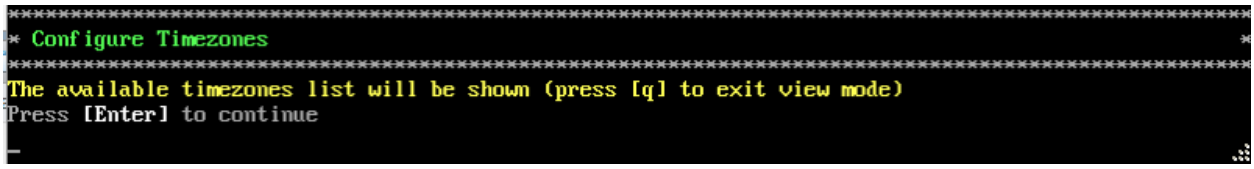


Note: If **n** (No) is selected, all DNS Servers will be disabled.

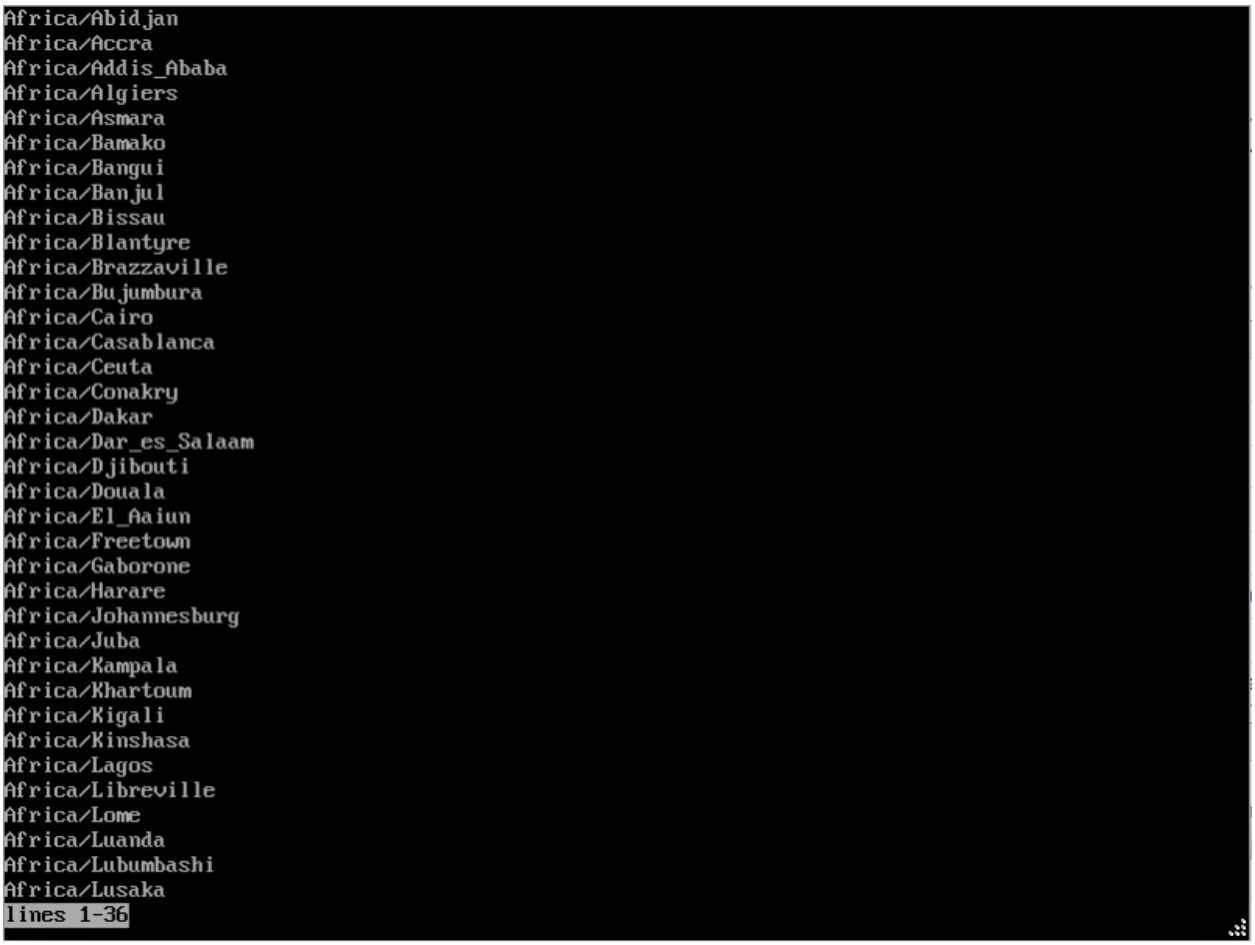
3. Enter **y** and press **Enter** to confirm the settings. You will be prompted to restart the OV Client Service for the change to take effect. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Timezone

1. Enter **7** and press **Enter** to begin setting up the timezone.



2. Press **Enter** to display timezones.



2. Press **Enter** to scroll through the list. After locating your timezone, press **q** and enter your timezone at the prompt (e.g., America/Los_Angeles). Then press **Enter** to set the timezone and return to the Configure Current Node Menu.

You can verify the change using the **2 - Display Current Configuration** command.

Configure Route

1. If you want to add a static route from the VM to another network enter **8** and press **Enter**.

2. Add an IPv4 route by entering **3** at the command prompt.

3. Enter the subnet, netmask and gateway.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Network Size

1. At the Main Menu prompt, enter **9** and press **Enter** to begin configuring a Network Size.

2. You can re-configure OV 2500 NMS-E 4.4R2 memory settings by selecting option **2**. Select an option (e.g., Low, Medium, High, Very High) based on the number of devices being managed and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the Watchdog Service for the change to take effect. See Recommended System Configurations for more information.

3. Configure Swap file by selecting option **3**.

- **1 - Show Current Swap Files -** Enter **1** and press **Enter** to display information about any configured Swap Files.
- **2 - Add Swap File -** Enter the size of the Swap File in MB (Range = 1 - 4096). Enter **y** and press **Enter** at the confirmation prompt.
- **3 - Delete Swap File -** Select the Swap File you want to delete and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.

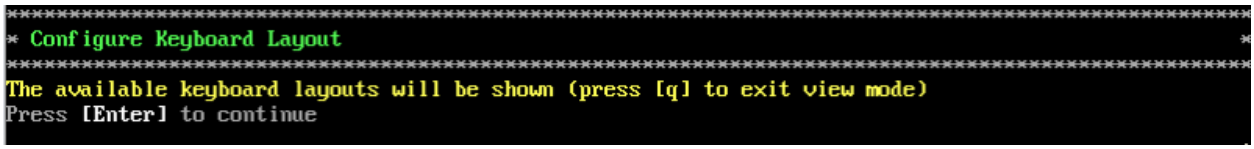
4. Configure Data Partition by selecting option **4**.

By default, OV 2500 NMS-E 4.4R2 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you increase the provisioned hard disk.

> **Important Note:** Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, HDD Provisioning) is adequate for the number of devices you are managing; and make sure the appropriate memory and disk space for the selected network size have been allocated to the OmniVista VA. Insufficient memory or disk space for the chosen network size may cause OV instability. OmniVista will not allow you to configure a network size that cannot be supported by the VA configuration. For example, if you allocate 16GB of memory for the OmniVista VA, OmniVista will only allow you to configure a Low network size (fewer than 500 devices). Refer to Recommended System Configurations for details.

Configure Keyboard Layout

1. Enter **10** and press **Enter** to specify a keyboard layout.



2. Press **Enter** to see the list of keyboard layouts.

3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Enter **y** at the confirmation prompt and press **Enter**. Press **Enter** to return to The Virtual Appliance Menu.

The table below lists all supported keyboard layouts.

amiga-de	amiga-us	atari-uk-falcon	atari-se
atari-us	atari-de	pt-olpc	es-olpc
sg-latin1	hu	sg	fr_CH
de-latin1-nodeadkeys	fr_CH-latin1	de-latin1	de_CH-latin1
cz-us-qwertz	sg-latin1-lk450	croat	slovene
sk-prog-qwertz	sk-qwertz	de	cz
wangbe	wangbe2	fr-latin9	fr-old
azerty	fr	fr-pc	be-latin1
fr-latin0	fr-latin1	tr_f-latin5	trf-fgGIod
backspace	ctrl	applkey	keypad
euro2	euro	euro1	windowkeys
unicode	se-latin1	cz-cp1250	il-heb
ttwin_cplk-UTF-8	pt-latin1	ru4	ruwin_ct_sh-CP1251
ruwin_alt-KOI8-R	no-latin1	pl1	cz-lat2
nl2	mk	es-cp850	bg-cp855
by	uk	pl	ua-cp1251
pt-latin9	sk-qwerty	se-lat6	bg_bds-cp1251
ruwin_cplk-UTF-8	br-abnt	la-latin1	sr-cy
ruwin_ctrl-CP1251	ua	dk	ru-yawerty
mk-cp1251	ruwin_cplk-KOI8-R	kyrgyz	defkeymap_V1.0
se-fi-lat6	ruwin_ctrl-UTF-8	ro	fi
sk-prog-qwerty	trq	fi-latin9	gr
ru3	us	ruwin_ct_sh-KOI8-R	nl
ro_std	ttwin_alt-UTF-8	trf	ruwin_alt-UTF-8
it-ibm	il	by-cp1251	it
emacs	fi-latin1	pc110	bg_bds-utf8
tralt	defkeymap	bg_pho-utf8	ua-ws
cf	hu101	bg_pho-cp1251	se-ir209
ttwin_ctrl-UTF-8	cz-lat2-prog	br-latin1-us	mk-utf

cz-qwerty	ruwin_cplk-CP1251	ttwin_ct_sh-UTF-8	ru1
ruwin_ctrl-KOI8-R	ru-ms	no	us-acentos
pl2	sv-latin1	br-latin1-abnt2	et
ru-cp1251	ruwin_alt-CP1251	ru	it2
lt.l4	ua-utf	bywin-cp1251	bg-cp1251
ru_win	emacs2	dk-latin1	kazakh
br-abnt2	es	pl4	mk0
is-latin1	is-latin1-us	il-phonetic	fi-old
et-nodeadkeys	jp106	lt	ru2
ruwin_ct_sh-UTF-8	pt	se-fi-ir209	gr-pc
lt.baltic	tr_q-latin5	pl3	ua-utf-ws
bashkir	no-dvorak	dvorak-r	dvorak
ANSI-dvorak	dvorak-l	mac-euro	mac-euro2
mac-fr_CH-latin1	mac-us	mac-de-latin1	mac-be
mac-es	mac-pl	mac-se	mac-dvorak
mac-fi-latin1	mac-template	mac-dk-latin1	mac-de-latin1-nodeadkeys
mac-fr	mac-pt-latin1	mac-uk	mac-it
mac-de_CH	sunt4-no-latin1	sunt5-cz-us	sundvorak
sunt5-de-latin1	sunt5-us-cz	sunt5-es	sunt4-fi-latin1
sunkeymap	sunt4-es	sunt5-ru	sunt5-uk
sun-pl	sunt5-fr-latin1	sunt5-fi-latin1	sun-pl-altgraph

4. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Update OmniVista Web Server SSL Certificate

To update the OmniVista Web Server SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VA. Make sure the destination directory is “keys”.

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>
- **SFTP Port:** 22

1. Enter **11** and press **Enter**.

2. Choose a certificate file (.crt) and enter **y** and press **Enter**. Choose a private key file (.key) and enter **y** and press **Enter**.

```
**********************************************************************************************************
* Update OmniVista Web Server SSL certificate
**********************************************************************************************************
**********************************************************************************************************
* Available certificate(s)
**********************************************************************************************************
* [1] ov_server.crt
* [0] Exit
**********************************************************************************************************
(*) Type your option: 1
Would you like to use this certificate?
       [1] ov_server.crt
[y|n] (n): y

**********************************************************************************************************
* Available private key(s)
**********************************************************************************************************
* [1] ov_server.key
* [0] Exit
**********************************************************************************************************
(*) Type your option: 1
Would you like to use this private key?
       [1] ov_server.key
[y|n] (n):
```

Enable/Disable AP SSL Authentication

Enables/Disables AP SSL Authentication. By default, AP SSL Authentication is enabled. However, you may want to disable it if there is a problem with the SSL Certificate. Enter **12** and press **Enter**. The current status will be displayed (Enabled/Disabled). Follow the prompts to enable or disable AP SSL Authentication. Once services have started/stopped, press **Enter** to return to the Configure the Virtual Appliance Menu.

Enable/Disable Admin SSH

Enter **13** and press **Enter** to enable/disable OmniVista Admin SSH. If enabled, you can log into the OmniVista VM via SSH. If disabled, you can only log in using the Hypervisor Console. Admin SSH is enabled by default.

Configure NTP Client

1. Enter **13** and press **Enter** to configure an NTP Server.

```
**********************************************************************************************************
* Configure NTP Client                                                                                   *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Configure NTP Server IP                                                                            *
* [3] Status NTP Client                                                                                  *
* [4] Disable NTP Client                                                                                 *
* [5] Enable NTP Client                                                                                  *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

2. Enter **2** and press **Enter**.

3. Enter the IP address of the NTP Server and press **Enter**.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu. You can enable the server when you create it, or enable it at a later time using option **5**.

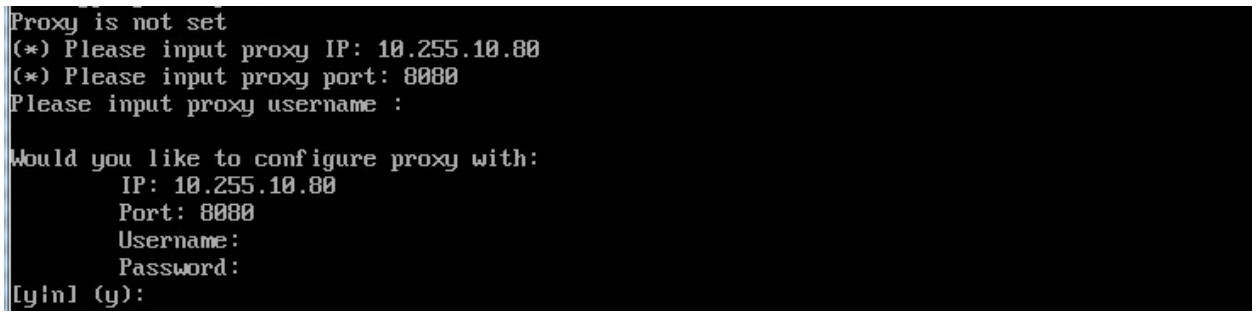
Configure Proxy

OV 2500 NMS-E 4.4R2 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management (PALM). If the OV 2500 NMS-E 4.3R3 Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.3R3 to connect to these external sites (Port 443):

- **ALE Central Repository -** ovrepo.fluentnetworking.com
- **AV Repository -** ep1.fluentnetworking.com
- **PALM -** palm.enterprise.alcatel-lucent.com
- **Call Home Backend -** us.fluentnetworking.com
- **Device Fingerprinting Service -** api.fingerbank.org.

1. Enter **154** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **2** and press **Enter** to configure a Proxy Server.

2. If the VM will use a proxy server, enter the Proxy Server IP address, along with the port (e.g., 8080).



15

Note: If **n** (No) is selected, all proxy servers will be disabled.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

4. Enter **3** and press **Enter** to enable the Proxy.

Change Screen Resolution

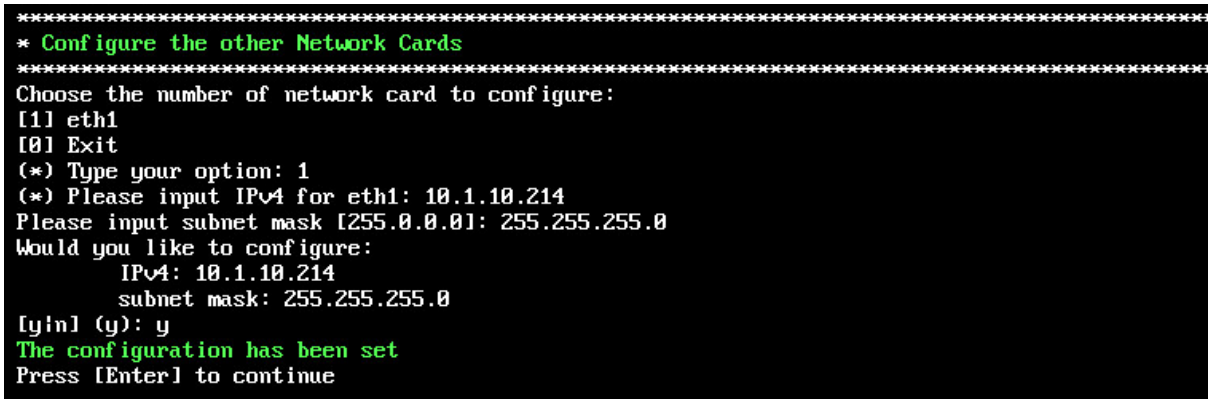
1. Enter **15** and press **Enter** to configure the VA screen resolution.

2. Select a screen resolution and press **Enter**. Enter **y** and press Enter **y** at the confirmation prompt. You will be prompted to restart the VA for the settings to take effect.

3. Enter **y** and press **Enter** at the confirmation prompt to restart the VA.

Configure the Other Network Cards

1. Enter **16** and press **Enter** to configure additional Network Cards on the Virtual Appliance.



2. Enter the number of the network card you want to configure (e.g., **1** eth1) and press **Enter**.

3. Enter an IPv4 IP address and mask.

4. Enter **y** and press **Enter** at the confirmation prompt.

To add another network card using the VA Menu, the card must exist in the Hypervisor. If necessary, add a new Network Adapter in the VM Settings in the Hypervisor.

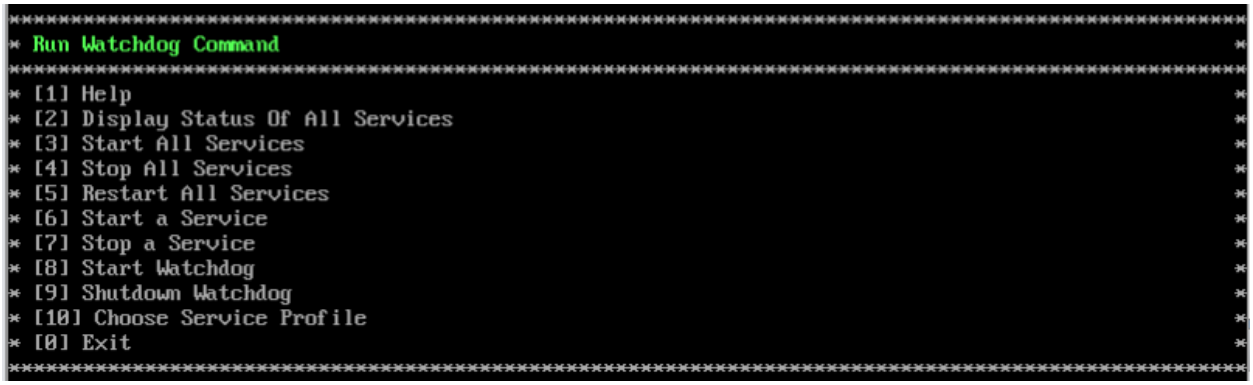
> **Important Note:** The new adapter **must** be the same Adapter Type as first NIC. In other words, eth1, eth0 should be same type.

Exit

Enter **0** and press **Enter** to return to the Virtual Appliance Menu.

Run Watchdog Command

The Watchdog command set is used to start and stop managed services used by OV 2500 NMS-E 4.4R2. If you stop certain framework services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services. To access the Watchdog Command Menu, enter **3** at the command prompt.



The following options are available:

- **Display Status Of All Services -** Displays the status of all of the services used by OmniVista (Running/Stopped). To display the status for all services just once (Default), Enter **n** and press **Enter** at the "Continuous Status" Prompt (or just press **Enter**). The status will be displayed and you will be returned to the Run Watchdog Command Menu. To run and display continuous status checks for all services, enter **y** then press **Enter** at the "Continuous Status" Prompt. To stop the display and return to the Run Watchdog Command Menu, enter **Ctrl C**.
- **Start All Services -** Starts all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Stop All Services** - Stop all services. Enter y and press **Enter** at the confirmation prompt.
- **Restart All Services -** Stop and restart all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Start a Service -** Starts a single service. Enter the service name at the prompt and press **Enter**. At the "Start Tree" option, enter **y** and press **Enter** to start all dependent services; enter **n** if you do not want to start dependent services. Press **Enter** at the confirmation prompt to start the service(s).
- **Stop a Service -** Stops a single service. Enter the service name at the prompt and press **Enter**. At the "Stop Tree" option, enter **y** and press **Enter** to stop all dependent services; enter **n** if you do not want to stop dependent services. Press **Enter** at the confirmation prompt to stop the service(s).
- **Start Watchdog -** Starts the Watchdog Service, which starts all services.
- **Shutdown Watchdog -** Stops the Watchdog Service, which stops all services.
- **Choose Service Profile -** Used to save memory if certain services are not required for your network (e.g., you are not using Stellar APs in your network or you are not using the Application Visibility application). Note that when you change a service profile, all Watchdog Services will be restarted.
  - **All Features (Default) -** All services are started.
  - **No Stellar, No UPAM -** Services required for Stellar APs and UPAM will not be started.
  - **No Application Visibility -** Services required for the Application Visibility application will not be started.
  - **No Stellar, No UPAM, No Application Visibility -** Services required for Stellar APs, UPAM, and Application Visibility will not be started.

Upgrade VA

The Upgrade VA command set is used to display information about the currently-installed OmniVista 2500 NMS software, upgrade OmniVista software, configure the OV Build Repository, and backup/restore OV software. OV software and updates are stored on an external repository (ALE Central Repository). By default, the OV Virtual Appliance points to the ALE Central Repository, which contains the latest builds and software updates. If a proxy has been configured, make sure to configure the proxy to connect to the external repository.

Note: If you have configured and enabled a Custom Repository, you must select option **4 – Enable Repository**, and enable the **ALE Custom Repository** to access the latest software.

To access the Upgrade VA Menu, enter **4** at the command prompt. The following options are available:

- **To 4.4R2 (Upgrade to Latest Patch of Current Release, if any) -** Displays information about the currently-installed OmniVista NMS software (e.g., Release Number, Build Number). It also checks for, and displays information about, any available updates. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. Select an option and press **Enter** to display information about the currently-installed OmniVista NMS software and download/upgrade an available update.
  - **Download and Upgrade -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available. (If you are using an Offline Repo, this is the only upgrade option supported. “Download Only” and “Upgrade from a Download Package” are not supported.)
  - **Download Only -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads the update, if available.
  - **Upgrade from a Download Package -** If you have previously downloaded an update but have not yet installed it, OV will install the downloaded update.

    Note: You can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available.
- **To New Release -** Upgrade to a new release. The options and processes are the same as above (“To 4.4R2 Upgrade to Latest Patch of Current Release, if any”). Note that if a new version of the current release is available, you will be prompted to install the latest version of the current release before upgrading to the new release.
- **Enable Repository -** Enable an OV Build Repository. This is the repository that OmniVista 2500 NMS will use to retrieve OV upgrade software. Select a repository from

the list, enter **y** and press **Enter** at the confirmation prompt to enable the repository. Only one (1) repository can be enabled at a time.

- **Configure Custom Repositories -** Configure a custom repository. By default, the OV Virtual Appliance points to the external ALE Central Repository, which contains the latest OV software. However, you can configure up to three (3) custom repositories. Select a repository (e.g., [1] "Custom Repo 1" Repository) and press **Enter**. Complete the fields as described below, then enter **y** and press **Enter** at the confirmation prompt:
  - **Repository Name -** User-configured repository name.
  - **Repository URL -** The URL of the custom repository (e.g., 192.168.70.10/repo/centos). Enter the URL only. There is no need to enter the "https://" prefix.

  Only one (1) repository can be enabled at a time. The user is responsible for ensuring that the custom repository contains the latest OV software.
- **Configure Update Check Interval -** Configure how often the OmniVista 2500 NMS Server will check the OV Build Repository for updates. You can perform a check immediately or schedule the check to be performed at regular intervals. The results of the scheduled checks are displayed on the Welcome Screen.
  - **Check Now -** Run the Update Check Task immediately and displays the results. Enter **2** and press **Enter**. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade. Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new release is available (e.g., R01 to R02), and do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.
  - **Check Daily/Weekly/Monthly -** Run the Update Check Task at the configured intervals and displays the results on the Welcome Screen. Select an interval and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
  - **Disable (Default) -** Disable the Update Check Task. Enter **6** and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
- **Backup/Restore OV2500 NMS Data -** Backup/Restore OmniVista 2500 NMS data. The following options are available:
  - **Configure Backup Retention Policy -** Configure the maximum number of days that you want to retain backups (Range = 1 – 30, Default = 7), and the maximum number of backups that you want to retain (Range = 1 – 30, Default = 5). Backup files are automatically deleted based on the Backup Retention Policy.
  - **Backup Now -** Perform an immediate backup. Enter an optional name for the backup (default = ov2500nms) and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. When the backup is complete, it will be stored in the "backups" Directory with the backup name and the date and time of the backup (<base name>_<yyyy-MM-dd--HH-mm>.bk). If you do not enter a name, the backup will be stored as ov2500nms- yyyy-MM-dd--HH-mm>.bk. (e.g., ov2500nms-2018-11-16--16-21.bk).
  - **Schedule Backup -** You can schedule an automatic backup to begin at a specific time and repeat at a specific daily interval. Enter a time for the backup to begin (HH:mm format) and press **Enter**. Enter the time between backups (Range = 1 – 30

Days, Default = 1) and press **Enter**. You can change the backup schedule at any time.

Note: Scheduled backups utilize the Task Scheduler (Windows) and Cron Job (Linux) utilities. If necessary, these utilities can be used to modify a scheduled backup.

Note: Backup files are automatically deleted based on the Backup Retention Policy. Monitor and maintain the Backup Directory to optimize disk space.

- **Restore -** Select a backup and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt and press **Enter**.

  Note: You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.4R2 configuration using a 4.4R2 Backup File). OmniVista will not allow you to perform a restore using a backup from a previous release.

  Note: If you want to perform a restore using a 4.4R2 Backup File residing on a different system, you must change the OV IP address/ports and UPAM IP address/ports of the system on which you are performing the restore to match the OV IP address/ports and UPAM IP address/ports of the system from which the backup file was taken before performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu (Option 4 - Configure OV IP & OV Ports) to return the restored system to its original OV IP address/ports and UPAM IP address/ports.

  For example, if you want to use a backup file on System A to perform a restore on the System B, you must change the OV IP address/ports and UPAM IP address/ports of System B to the OV IP address/ports and UPAM IP address/ports of System A before performing the restore. After the restore is complete, you can use the Configure The Virtual Appliance Menu (Option 4 - Configure OV IP & OV Ports) to change the OV IP address/ports and UPAM IP address/ports on System B back to their original configuration.

- **View Backup Configurations -** View the backup retention policies. The policies are configured using Option **2 – Configure Backup Retention Policy**. Note that if you have not configured a Backup Retention Policy, the “Maximum Backup Retention Days” and Maximum Backup Retention Files” fields will show “-1”.

Change Password

You can change the Virtual Appliance cliadmin password and/or mongo database password. Enter **5** and press **Enter** to bring up the Change Password Menu.

To change the VA cliadmin password, enter **2**, then press **Enter**. At the prompts, enter the current password, then enter the new password.

To change the mongo database password, enter **3**, then press **Enter**. You have two options when changing the mongo database password.

```
(*) Type your option: 3
You must remember the new passwords in order to manage the Mongodb.
Press [Enter] to continue

Would you like to change password for
        [1] Mongo administrator
        [2] Ngnms application user
Provide your option [1 OR 2]:
```

Enter **1** to change the mongo administrator password. Enter **2** to change the application user password. At the prompts, enter the current password, then enter the new password.

To change the Technical Support Code (used by Support to access the VM) enter **4**, then press **Enter**. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

To change the password of the “ftp” user of the VA, enter **5**, then press **Enter**. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

Logging

You can view OV 2500 NMS-E 4.4R2 Logs using the “Logging” option. Enter **6**, then press **Enter**.

```
**********************************************************************************************************
* Configure Logging                                                                                      *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Change Log Level                                                                                   *
* [3] Collect Log Files                                                                                  *
* [4] Collect JVM Information                                                                            *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

The following options are available:

- **Change Log Level -** Changes the logging level for OV services. Enter the number corresponding to the OV service for which you want to change the logging level (e.g. 13 - ovsip) and press **Enter**. Enter the number corresponding to the package for which you want to change the logging level (e.g., 1 - com.alu.ov.ngms.sip.service) and press **Enter**. Enter the number corresponding to the log level you want to set (e.g., 2 - DEBUG) and press **Enter**.
- **Collect Log Files -** Collects all log files from a specific date to the current date. Enter the date from which you want to collect log files in dd-MM-yyyy format (e.g., 10-15-2018) and press **Enter**. When finished, a "Collecting completed" message is displayed. The log files are stored in a zip file in the "logs" Directory with the date and time the logs were collected appended to the file name (e.g., ovlogs-15-10-2018_12-04-18.zip). SFTP to the VA using the "cliadmin" username and password to view the log files (Port 22).
- **Collect JVM Information -** Collects and archives Java Virtual Machine (JVM) information. Enter **y** and press **Enter** at the confirmation prompt to collect JVM information. When finished, a "Collecting completed" message is displayed along with the JVM information file name. The file is stored in the "jvm-info" directory with date and time the file was created collected appended to the file name (e.g., jvm -info-02018-10-

15-12-08-43.jar). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).

Login Authentication Server

The Login Authentication Server is used to view/change the OV 2500 NMS-E 4.4R2 Login Authentication Server. Enter **7** and press **Enter** to bring up the Login Authentication Server Menu.

Enter **2** and press **Enter** to display the current Login Authentication Server. If the server is remote, the IP address is displayed. If the server is local, "local" is displayed.

If the current Login Authentication Server is a remote server, enter **3** and press **Enter** to change the Login Authentication Server to "local". Enter **y** and press **Enter** at the confirmation prompt.

Power Off

Before powering off the VM, you must stop all OmniVista services using the **Stop All Services** option in the **Run Watchdog Command**. After all the services are stopped, enter **8** at the command line to power off the VM. Confirm the power is off by entering **y**. The power off may take several minutes to complete.

> **Note:** OV 2500 NMS-E 4.4R2 functions stop running following power off. The VM must be powered back on via the VMware client software and you must log back into the VM via the console.

Reboot

Before rebooting the VM, you must stop all OmniVista services using the **Stop All Services** option in the **Run Watchdog Command**. After all services are stopped, enter **9** at the command line to reboot the VM. Confirm reboot by entering **y**. The reboot may take several minutes to complete. When rebooted, you will be prompted to log in through the cliadmin user and password prompts. Note that OV 2500 NMS-E 4.4R2 functions continue following reboot.

Advanced Mode

Advanced Mode enables you to use read-only UNIX commands for troubleshooting. Enter **9**, then press **Enter** to bring up the CLI prompt. Enter **exit** and press **Enter** to return to the Virtual Appliance Menu. The following commands are supported:

- /usr/bin/touch
- /usr/bin/mktemp
- /usr/bin/dig
- /usr/bin/cat
- /usr/bin/nslookup
- /usr/bin/which
- /usr/bin/less

- /usr/bin/tail
- /usr/bin/vi
- /usr/bin/tracepath
- /usr/bin/tty
- /usr/bin/systemctl
- /usr/bin/grep
- /usr/bin/egrep
- /usr/bin/fgrep
- /usr/bin/dirname
- /usr/bin/readlink
- /usr/bin/locale
- /usr/bin/ping
- /usr/bin/traceroute
- /usr/bin/netstat
- /usr/bin/id
- /usr/bin/ls
- /usr/bin/mkdir
- /usr/sbin/ifconfig
- /usr/sbin/route
- /usr/sbin/blkid
- /usr/sbin/sshd-keygen
- /usr/sbin/consoletype
- /usr/sbin/ntpdate
- /usr/sbin/ntpq
- /usr/bin/ntpstat
- /usr/bin/abrt-cli
- /usr/sbin/init
- /usr/sbin/tcpdump
- /bin/mountpoint

Set Up Optional Tools

The Setup Optional Tools command set is used to install/upgrade Hypervisor Optional Tools Packages. Enter **11** and Press **Enter** to bring up the Optional Tool Menu.

Enter the number corresponding to the Hypervisor you are using (**2 - VMWare**, **3 - Virtual Box**, **4 - Hyper-V**) and press **Enter**. Information about available packages is displayed. If a new package is available, enter **y** and press **Enter** at the "Would you like to install the package" prompt. The package will automatically be downloaded from the OV Repository and installed (this may take several minutes). When the "Installation Complete" messaged is displayed, press **Enter** to continue. Press **Enter** again to restart the Virtual Appliance.

Convert to Cluster

Enter **12** and press **Enter** to convert the Node to a Cluster (High-Availability) Installation. This command prepares the VM to be configured in a Cluster configuration. After selecting this option and confirming the operation, the VM will reboot. When the reboot is complete, log into the VM to complete the conversion.

```
(*) Type your option: 12
OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed converting to cluster?[y|n] (n):
```

See Converting to a High-Availability Installation for detailed instructions on configuring a High-Availability installation.

Join Cluster

Enter **13** and press **Enter** to have this VM join in a Cluster (High-Availability) Installation. After selecting this option and confirming the operation, the VM will reboot. When the reboot is complete, log into the VM to complete the conversion.

```
All data on this node will be lost and OV will restart if you continue.
Backing up this OV installation before continue is strongly recommended.
Are you sure want to proceed joining cluster?[y|n] (n):
```

See Converting to a High-Availability Installation for detailed instructions on configuring a High-Availability installation.

Log Out

To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OV 2500 NMS-E 4.4R2 functions continue following logout.

Appendix C – Using the HA Virtual Appliance Menu

To access the High-Availability (HA) Virtual Appliance Menu for a VM, launch the Hypervisor Console. The login prompt is displayed.

> **Note:** You can also access the Virtual Appliance Menu by connecting via SSH using port 2222, user **cliadmin,** and password set when deploying VA (e.g., ssh cliadmin@192.160.70.230 –p 2222).

The menus are the same for both Nodes in the Cluster. With the exception of the specific Cluster Menus (Show OV Cluster Status, Configure Cluster and Configure Current Node), any configurations you perform (e.g., Watchdog commands, Upgrade/Backup/Restore commands) are executed on the Node you are logged into.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.4R2 GA
Build Number: 47
Patch Number: 0
Build Date: 10/24/2019
Technical Support Code: alcatel
ov1 login:
```

1. Enter the login (**cliadmin**) and press **Enter**.

2. Enter the password and press **Enter**. The password is the one you created when you first launched the VM Console at the beginning of the installation process. The Virtual Appliance Menu is displayed.

```
**********************************************************************************************************
* The HA Virtual Appliance Menu                                                                          *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Show OV Cluster Status                                                                             *
* [3] Configure Cluster                                                                                  *
* [4] Configure Current Node                                                                             *
* [5] Run Watchdog Command                                                                               *
* [6] Upgrade/Backup/Restore VA                                                                          *
* [7] Logging                                                                                            *
* [8] Setup Optional Tools                                                                               *
* [9] Advance Mode                                                                                       *
* [10] Power Off                                                                                         *
* [11] Reboot                                                                                            *
* [0] Log Out                                                                                            *
**********************************************************************************************************
```

The HA Virtual Appliance Menu provides the following options:

- 1 – Help
- 2 – Show OV Cluster Status
- 3 – Configure Cluster
- 4 – Configure Current Node
- 5 – Run Watchdog Command
- 6 – Upgrade/Backup/Restore VA
- 7 – Logging
- 8 – Setup Optional Tools
- 9 – Advance Mode

- 10 – Power Off
- 11 – Reboot
- 0 – Log Out

For information on these menu options, refer to the sections below.

Help

Enter **1** and press **Enter** to bring up help for the HA Virtual Appliance Menu.

Show OV Cluster Status

The Cluster Status Screen displays information about the High-Availability Cluster, including Node IP address, Role, and Status. The status will display and the HA Virtual Appliance Menu will return.

```
Cluster Status:
Node     Hostname  Ip Address      Role    Status
Current  ov1       10.255.222.203  Active  Online
Peer     ov2       10.255.222.98           Online
Data sync: Up to Date
```

The data sync status indicates whether the data between two nodes is in sync. If it is, the field will indicate “Up to Date”. If it is in the process of syncing, a progress will be displayed as a percentage. The speed of a data sync depends on the amount of data and the network speed between the two Nodes.

> **Important Note:** If a data sync is in progress, it is highly recommended to wait for a data sync to complete before doing performing any configuration on a Node.

Configure Cluster

Enter **3** and press **Enter** to configure the Cluster. The settings you configure in this menu are applied to both Nodes in the Cluster. Note that Cluster settings (Menu Items 3 – 8) can only be configured on the Active Node.

```
**********************************************************************************************************
* Configure Cluster                                                                                      *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Display Cluster Configuration                                                                      *
* [3] Configure Cluster IP                                                                               *
* [4] Configure Captive Portal Virtual IP                                                                *
* [5] Configure Captive Portal Virtual IP v6                                                             *
* [6] Configure Additional OV Web Virtual IP                                                             *
* [7] Remove peer node from cluster                                                                      *
* [8] Configure OV Web Ports                                                                             *
* [9] Configure UPAM Portal Web Ports                                                                    *
* [10] Configure OV SSL Certificate                                                                      *
* [11] Enable/Disable AP SSL Authentication                                                              *
* [12] Configure FTP Password                                                                            *
* [13] Configure Login Authentication Server                                                             *
* [14] Preferred Active Node                                                                             *
* [15] Manual Failover                                                                                   *
* [16] Cluster Error Check                                                                               *
* [17] Configure Peer Node's Information                                                                 *
* [18] Enable Maintenance Mode                                                                           *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

The following options are available:

Help

Enter **1** and press **Enter** to bring up help for the Configure Cluster Menu.

Display Cluster Configuration

Enter **2** and press **Enter** to view information about the Cluster, including Node information, HTTP/HTTPS port information and proxy information.

```
**********************************************************************************************************
* Cluster Configuration                                                                                  *
**********************************************************************************************************
Cluster name: ovcluster
OV Virtual IP: 10.255.222.97
Captive Portal Virtual IP: 198.168.0.3
Captive Portal Virtual IPv6: (disabled)
Additional OV Web Virtual IP: (disabled)

Current node IP: 10.255.222.203
Current node hostname: ov1
Peer node IP: 10.255.222.98
Peer node hostname: ov2
Current Preferred Node:

OV Web HTTP Port: 80
OV Web HTTPS Port: 443

Captive Portal Web HTTP Port: 80
Captive Portal Web HTTPS Port: 443
```

Configure Cluster IP

Enter **3** and press **Enter** to configure the Cluster IP address and subnet. You will be prompted to restart services for the change to take effect. Note that if you reconfigure the Cluster IP address you will have to make the applicable network updates. The Cluster IP is only applicable for a Layer 2 HA Configuration.

To change an existing Cluster IP address, enter **2** and press **Enter** to re-configure the new address. The new IP address **must** be on the same subnet as the Nodes.

It is not recommended to disable the Cluster IP address. However, you can disable the Cluster IP address if you do not want to access the Cluster using this IP address. Enter **1 – Disable Cluster IP Address** and press **Enter** to disable the Cluster IP address. When you disable the Cluster IP address, the Virtual Captive Portal IP and Virtual Additional Web OV IP (if configured) are also disabled.

After disabling the Cluster IP address, you must access OmniVista using the physical IP address of the Active Node. After disabling the Cluster IP address, you can re-enable it and re-configure the Cluster IP address. The new IP address **must** be on the same subnet as the Nodes.

Configure Captive Portal Virtual IP

Enter **4** and press **Enter** to configure the Captive Portal Virtual IP address. Note that if you reconfigure the Captive Portal Virtual IP address you will have to make the applicable network updates. Captive Portal Virtual IP is only applicable for a Layer 2 HA Configuration.

If you are not using Captive Portal in your Cluster, you can enable and configure it. To create a new Captive Portal Virtual IP address, enter **1 – Enable Captive Portal Virtual IP** and press **Enter**. Enter the Virtual Captive Portal IP address. Note that the Captive Portal Virtual IP address must be on the same subnet as the current Cluster IP address.

If you are using Captive Portal in your Cluster, you can change the existing Captive Portal Virtual IP address, by entering **2 – Re-configure Captive Portal Virtual IP** and press **Enter** to configure the new address. You will be prompted to restart services for the change to take effect. The new Captive Portal Virtual IP address **must** be on the same subnet as the previous address.

To disable and existing Captive Portal IP address in a Cluster, enter 1 - **Disable Captive Portal Virtual IP** and press **Enter**. You will be prompted to restart services for the change to take effect. You can also re-enable and re-configure the Captive Portal Virtual IP address after disabling it.

Configure Captive Portal Virtual IPv6

Enter **5** and press **Enter** to configure the Captive Portal Virtual IPv6 address. You will be prompted to restart services for the change to take effect. Note that if you reconfigure the Captive Portal Virtual IPv6 address you will have to make the applicable network updates. Captive Portal Virtual IPv6 is only applicable for a Layer 2 HA Configuration.

```
**********************************************************************************************************
* Configure Captive Portal Virtual IPv6                                                                  *
**********************************************************************************************************
* [1] Enable Captive Portal Virtual IPv6                                                                 *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

To create a new Captive Portal Virtual IPv6 address, enter **1 – Enable Captive Portal Virtual IPv6** and press **Enter**. To change an existing Captive Portal Virtual IPv6 address, enter **2 – Re-configure Captive Portal Virtual IPv6** and press **Enter** to configure the new address. The new Captive Portal Virtual IPv6 address **must** be on the same subnet as the previous address.

To disable and existing Captive Portal IPv6 address, enter 1 - **Disable Captive Portal Virtual IP** and press **Enter**. You will be prompted to restart services for the change to take effect. You can also re-enable and re-configure the Captive Portal Virtual IPv6 address after disabling it.

Configure Additional OV Web Virtual IP

Enter **6** and press **Enter** to configure an Additional OV Web Virtual IP to access the OmniVista UI. You will be prompted to restart services for the change to take effect. The Additional OV Web Virtual IP is only applicable for a Layer 2 HA Configuration.

```
**********************************************************************************************************
* Configure Additional OV Web Virtual IP                                                                 *
**********************************************************************************************************
* [1] Enable Additional OV Web Virtual IP                                                                *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

To create a new Additional OV Web Virtual IP, enter **1 – Enable Additional OV Web Virtual IP** and press **Enter**. The Additional OV Web Virtual IP must be on the same subnet as the current static Additional OV Web IP. If no static Additional OV Web Virtual IP is configured, you will not be able to configure an Additional OV Web Virtual IP.

To change an existing Additional OV Web Virtual IP, enter **2 – Re-configure Additional OV Web Virtual IP** and press **Enter** to configure the new address. The new Additional OV Web Virtual IP address **must** be on the same subnet as the previous address.

To disable an Additional OV Web Virtual IP, enter **1 - Disable Additional OV Web Virtual IP**.

Remove Peer Node From Cluster

Enter **7**, press **Enter,** then enter **y** and press **Enter** at the Confirmation Prompt to remove the Peer Node from the Cluster. The process can take several minutes. When it is complete, a Confirmation Message will appear. Press **Enter** to return to the Configure Cluster Menu.

Note that this command can only be issued on the Active Node. This command is generally used if there is a problem with the Standby Node and you wish to permanently remove it. Once the Node is removed from the Cluster, it is essentially unusable. You cannot connect to it via a browser and it retains the HA Menu, so you cannot have it join another Cluster. However, you can have another Node join the Active Node in a new Cluster Configuration.

Configure OV Web Ports

Enter **8** and press **Enter** to configure the OmniVista Web HTTP/HTTPS ports. At the prompts, enter the IPv4 IP address and subnet mask; enter **y** and press **Enter** at the confirmation prompt, then press **Enter** to continue. At the prompts, enter the HTTP Port and the HTTPs Port (Defaults = HTTP - 80, HTTPS - 443). Enter **y** and press **Enter** at the confirmation prompt.

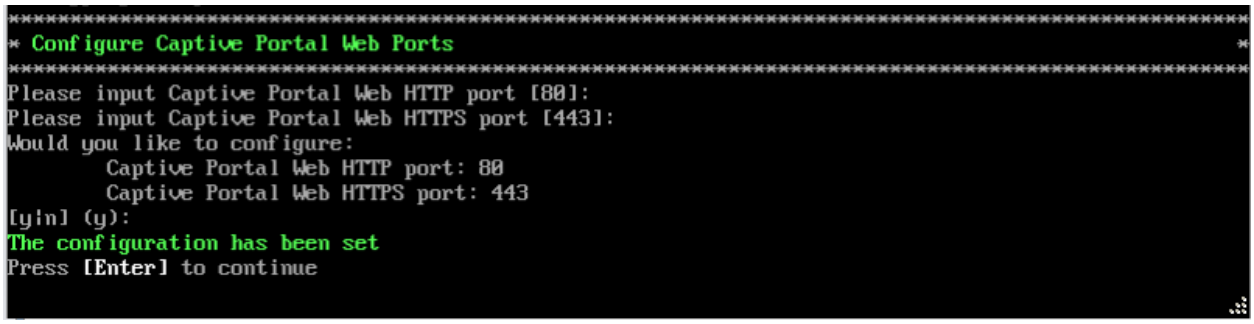
You will be prompted to restart the Watchdog Service for the change to take effect. Note that new port values must be unique (i.e., they must differ from any previously-configured ports).

Configure Captive Portal Web Ports

Enter **9** and press **Enter** to configure the Captive Portal Web Ports. Enter the Captive Portal HTTP and HTTPs port numbers. Press **Enter** to continue. You will be prompted to restart services for the change to take effect.

> **Note:** The default Captive Portal FQDN is "ov2500-upam-cportal.al-enterprise.com". If you want to replace it with your own FQDN you must:

1. Log into the OmniVista UI.
2. Go to the UPAM – Captive Portal Certificates page (U PAM – Settings – Captive Portal Certificates).
   - Create a Custom Certificate.
   - Activate the Certificate.



Configure OV SSL Certificate

To update the OmniVista Web Server SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VA. Make sure the destination directory is “keys”.

- **SFTP User:** cliadmin
- **SFTP Password:** <password when deploying VA>

- **SFTP Port:** 22

1. Enter **10** and press **Enter**.

2. Choose a certificate file (.crt) and enter **y** and press **Enter**. Choose a private key file (.key) and enter **y** and press **Enter**.

```
**********************************************************************************************************
* Update OmniVista Web Server SSL certificate
**********************************************************************************************************
**********************************************************************************************************
* Available certificate(s)
**********************************************************************************************************
* [1] ov_server.crt
* [0] Exit
**********************************************************************************************************
(*) Type your option: 1
Would you like to use this certificate?
        [1] ov_server.crt
[y|n] (n): y

**********************************************************************************************************
* Available private key(s)
**********************************************************************************************************
* [1] ov_server.key
* [0] Exit
**********************************************************************************************************
(*) Type your option: 1
Would you like to use this private key?
        [1] ov_server.key
[y|n] (n):
```

Enable/Disable AP SSL Authentication

Enables/Disables AP SSL Authentication. By default, AP SSL Authentication is enabled. However, you may want to disable it if there is a problem with the SSL Certificate. Enter **11** and press **Enter**. The current status will be displayed (Enabled/Disabled). Follow the prompts to enable or disable AP SSL Authentication. Once services have started/stopped, press **Enter** to return to the Configure the Virtual Appliance Menu.

Configure FTP Password

Enter **10** and press **Enter** to configure an FTP password for the Node. At the prompt, enter the old password, then enter and confirm the new password. You will be prompted to restart services for the change to take effect.

Configure Login Authentication Server

Enter **13** and press **Enter** to view/change the OmniVista Login Authentication Server.

```
**********************************************************************************************************
* Login Authentication Server                                                                            *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Current Login Authentication Server                                                                *
* [3] Change Login Authentication Server to local                                                        *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

Preferred Active Node

Enter **14** and press **Enter** to change the preferred Active Node. The Preferred Active Node is the Node that will be set following a system failure. When the system returns, the Preferred Active Node will be the Active Node when the system returns.

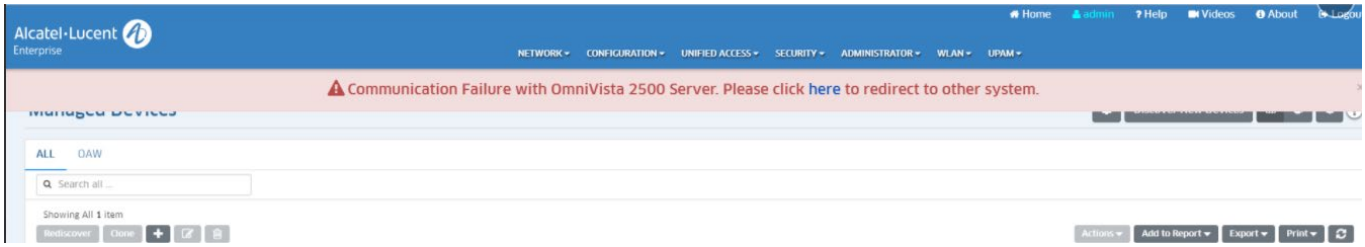
Select **1** to clear the current Active Node. This will remove the current Preferred Active Node setting, meaning there will be no Preferred Active Node in the case of a system failure. If no Preferred Active Node is set, the system will decide on the Active Node following a system failure. By default, no Preferred Active Node is set.

Select **2** or **3** to change the current Active Node. Enter **y** and press **Enter** at the Confirmation Prompt to clear the current Preferred Active Node and set the new one.

Manual Failover

Enter **15** and press **Enter** to manually initiate a failover to the Inactive Node. The current Inactive Node will become the Active Node. The process can take several minutes. After the failover is complete, the services on the Standby Node will be running. The previously Active Node will now be the Standby Node (with the upam, radius, and nginx services “Stopped”). A Banner will appear at the top of the UI warning that a “Communication Failure” has occurred.

- If you are using a Layer 2 Configuration, you can access OmniVista using the same Cluster IP address.
- If you are using a Layer 3 Configuration, the banner will contain a link to connect to the new Active Node, as shown below.



Cluster Error Check

Enter **16** and press **Enter** to display any Cluster Errors.

Configure Peer Node’s Information

Enter **17** and press **Enter** to change the IP address and Hostname (maximum of 15 characters) of the Peer Node. It is **not** recommended to re-configure the Peer Node once a cluster is initialized. If you change the configuration, you must take a backup of OmniVista and contact Customer Support to re-configure the Cluster.

Enable Maintenance Mode

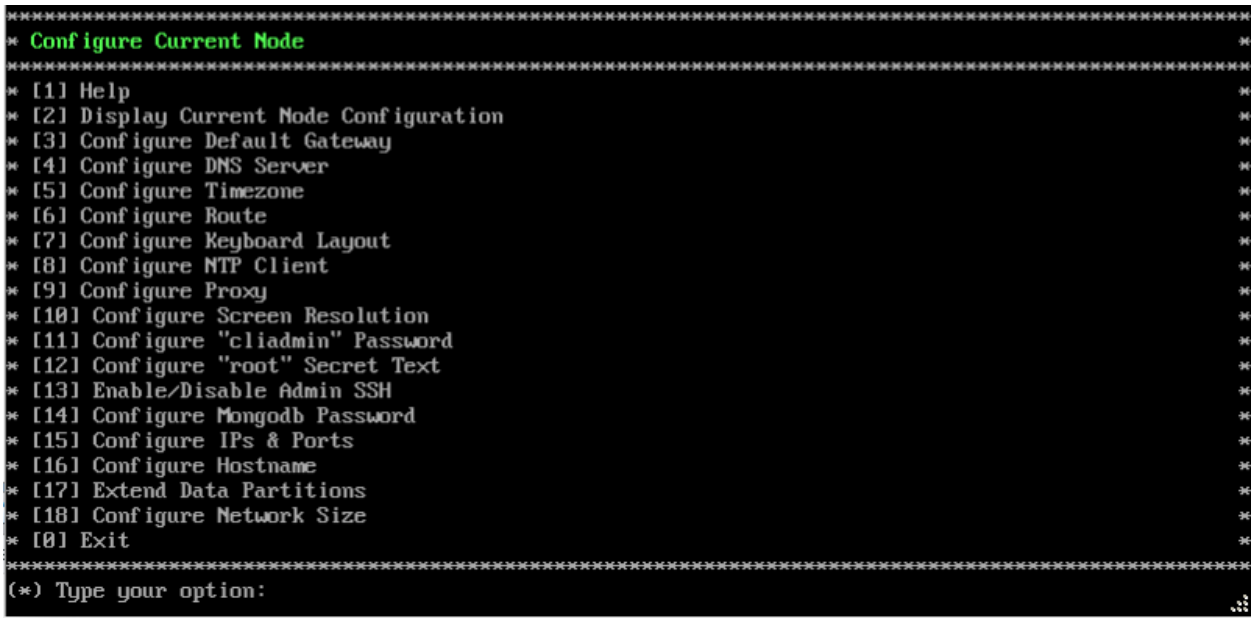
Enter **18** and press **Enter** to enable Maintenance Mode to perform an upgrade/disk extension on the VMs (Node 1 and Node 2). You only have to execute the command on one of the nodes. It will then be enabled on both Nodes.

Exit

Enter **0** and press **Enter** to exit to the Configure Cluster Menu and return to the HA Virtual Appliance Menu.

Configure Current Node

Enter **4** and press **Enter** to configure the Current Node (the Node that you are logged into).



The following options are available:

1 – Help

2 – Display Current Node Configuration

3 – Configure Default Gateway

4 – Configure DNS Server

5 – Configure Timezone

6 – Configure Route

7 – Configure Keyboard Layout

8 – Configure NTP Client

9 – Configure Proxy

10 – Configure Screen Resolution

11 – Configure “cliadmin” Password

12 – Configure “root” Secret Text

13 – Enable/Disable Admin SSH

14 – Configure Mongodb Password

15 – Configure IPs and Ports

16 – Configure Host Name

17 – Extend Data Partitions

18 – Configure Network Size

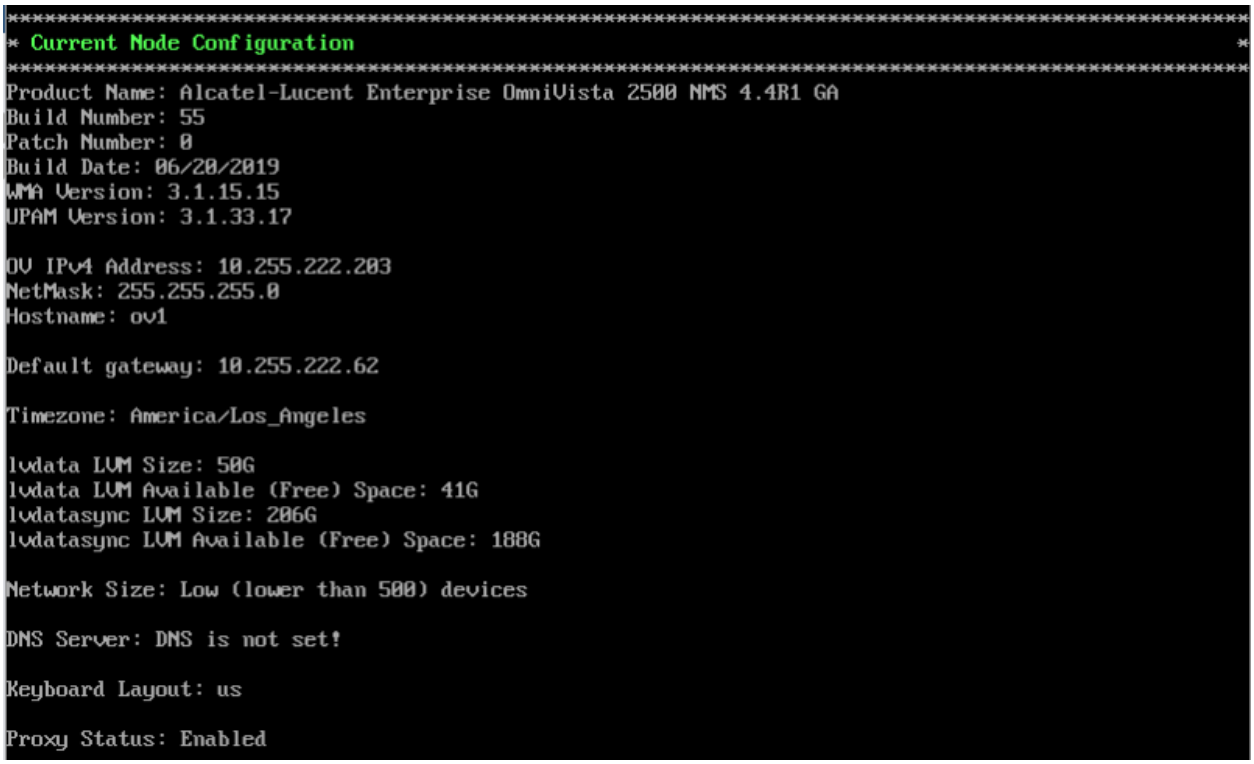
0 – Exit

Help

Enter **1** and press **Enter** to bring up help for the Configure Current Node Menu.

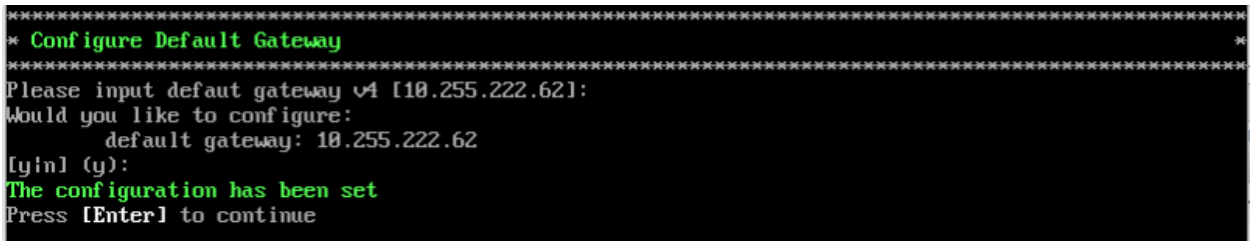
Display Current Node Configuration

Enter **2** and press **Enter** to display the configuration for the Node.



Configure Default Gateway

1. Enter **3** and press **Enter** to configure default gateway settings.



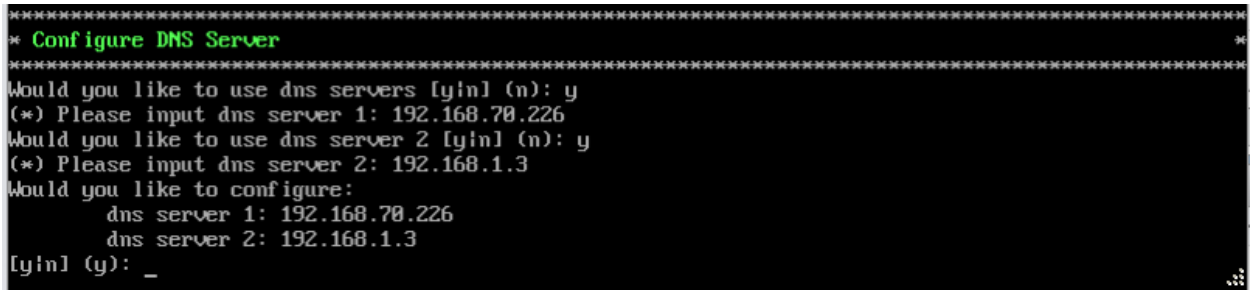
2. Enter an IPv4 default gateway.

3. Press **Enter** to confirm the settings. You will be prompted to restart services. Press **Enter**.

Configure DNS Server

1. Enter **4** to specify whether the VM will use a DNS Server.

2. If the VM will use a DNS server, enter **y**, then press **Enter**. Enter the IPv4 address for Server 1 and Server 2, if applicable.

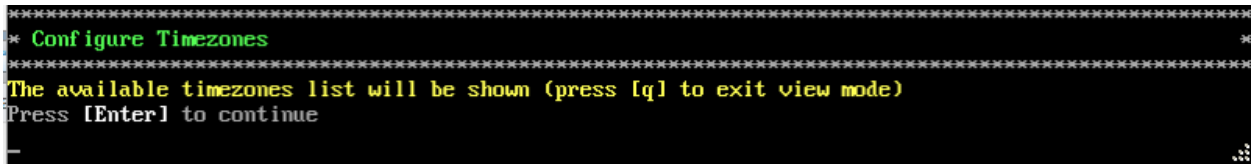


> **Note:** If **n** (No) is selected, all DNS Servers will be disabled. If **y** is selected, after DNS servers are set, you may be prompted to restart ovclient service if it was already running.

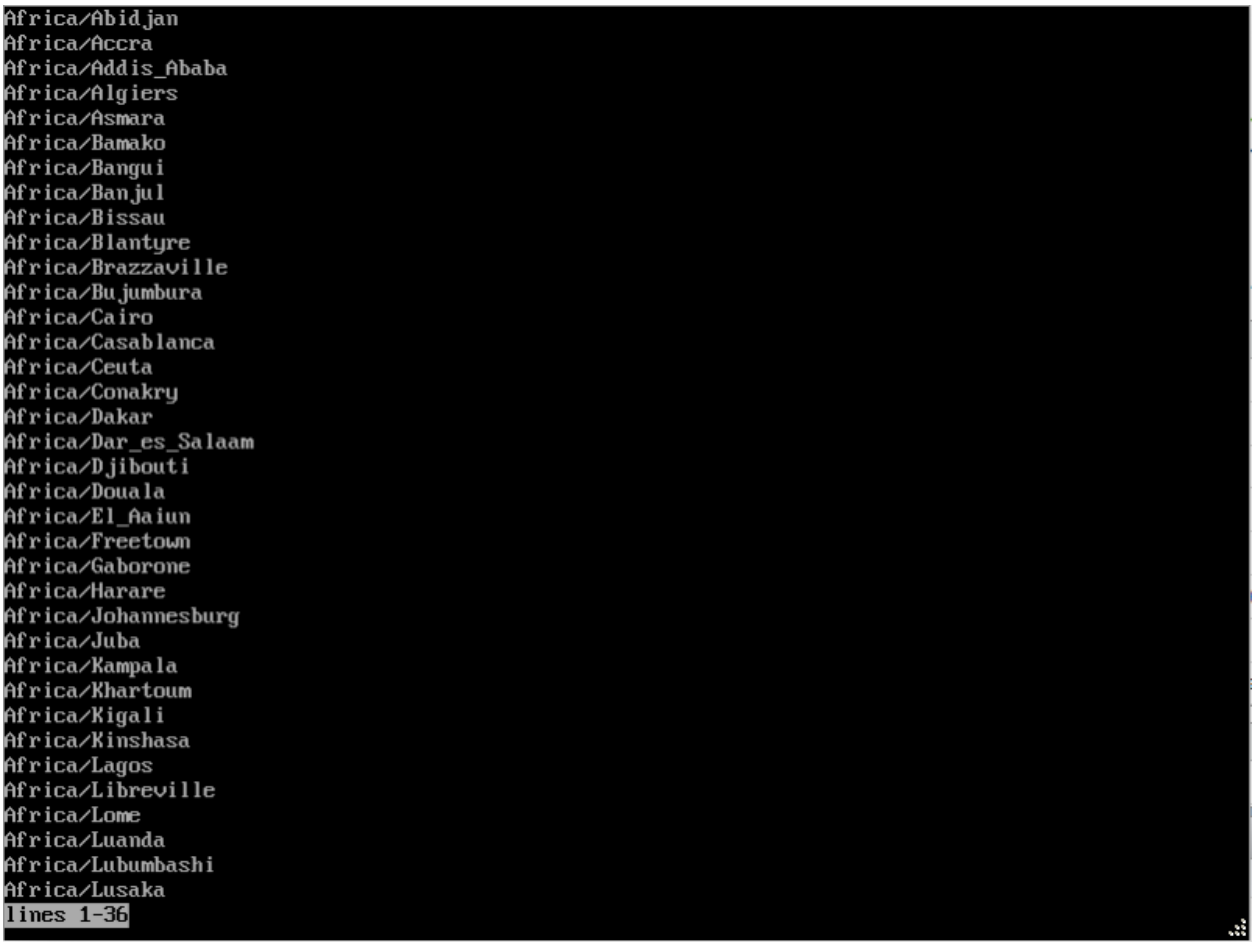
3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu. You will be prompted to restart the OV Client Service for the change to take effect.

Configure Timezone

1. Enter **5** and press **Enter** to begin setting up the timezone.



2. Press **Enter** to display timezones.



2. Press **Enter** to scroll through the list. After locating your timezone, press **q** and enter your timezone at the prompt (e.g., America/Los_Angeles). Then press **Enter** to set the timezone and return to the Configure Current Node Menu.

You can verify the change using the **(2) Display Current Node Configuration** command.

Configure Route

1. If you want to add a static route from the VM to another network enter **6** and press **Enter**.

2. Add an IPv4 route by entering **3** at the command prompt.

```
**********************************************************************************************************
* Configure Route                                                                                        *
**********************************************************************************************************
* [1] Help                                                                                               *
* [2] Show Current Routes                                                                                *
* [3] Add Route v4                                                                                       *
* [4] Del Route v4                                                                                       *
* [0] Exit                                                                                               *
**********************************************************************************************************
```

3. Enter the subnet, netmask and gateway.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Keyboard Layout

1. Enter **7** and press **Enter** to specify a keyboard layout.

```
**********************************************************************************************************
* Configure Keyboard Layout                                                                              *
**********************************************************************************************************
The available keyboard layouts will be shown (press [q] to exit view mode)
Press [Enter] to continue
```

2. Press **Enter** to see the list of keyboard layouts.

3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Enter **y** at the confirmation prompt and press **Enter**.

```
Please input keyboard layout [us]:
Would you like to set:
       keyboard layout: us
[y|n] (y): _
```

The table below lists all supported keyboard layouts.

amiga-de	amiga-us	atari-uk-falcon	atari-se
atari-us	atari-de	pt-olpc	es-olpc
sg-latin1	hu	sg	fr_CH
de-latin1-nodeadkeys	fr_CH-latin1	de-latin1	de_CH-latin1
cz-us-qwertz	sg-latin1-lk450	croat	slovene
sk-prog-qwertz	sk-qwertz	de	cz
wangbe	wangbe2	fr-latin9	fr-old
azerty	fr	fr-pc	be-latin1
fr-latin0	fr-latin1	tr_f-latin5	trf-fgGIod
backspace	ctrl	applkey	keypad
euro2	euro	euro1	windowkeys
unicode	se-latin1	cz-cp1250	il-heb
ttwin_cplk-UTF-8	pt-latin1	ru4	ruwin_ct_sh-CP1251
ruwin_alt-KOI8-R	no-latin1	pl1	cz-lat2
nl2	mk	es-cp850	bg-cp855
by	uk	pl	ua-cp1251
pt-latin9	sk-qwerty	se-lat6	bg_bds-cp1251
ruwin_cplk-UTF-8	br-abnt	la-latin1	sr-cy
ruwin_ctrl-CP1251	ua	dk	ru-yawerty
mk-cp1251	ruwin_cplk-KOI8-R	kyrgyz	defkeymap_V1.0

se-fi-lat6	ruwin_ctrl-UTF-8	ro	fi
sk-prog-qwerty	trq	fi-latin9	gr
ru3	us	ruwin_ct_sh-KOI8-R	nl
ro_std	ttwin_alt-UTF-8	trf	ruwin_alt-UTF-8
it-ibm	il	by-cp1251	it
emacs	fi-latin1	pc110	bg_bds-utf8
tralt	defkeymap	bg_pho-utf8	ua-ws
cf	hu101	bg_pho-cp1251	se-ir209
ttwin_ctrl-UTF-8	cz-lat2-prog	br-latin1-us	mk-utf
cz-qwerty	ruwin_cplk-CP1251	ttwin_ct_sh-UTF-8	ru1
ruwin_ctrl-KOI8-R	ru-ms	no	us-acentos
pl2	sv-latin1	br-latin1-abnt2	et
ru-cp1251	ruwin_alt-CP1251	ru	it2
lt.l4	ua-utf	bywin-cp1251	bg-cp1251
ru_win	emacs2	dk-latin1	kazakh
br-abnt2	es	pl4	mk0
is-latin1	is-latin1-us	il-phonetic	fi-old
et-nodeadkeys	jp106	lt	ru2
ruwin_ct_sh-UTF-8	pt	se-fi-ir209	gr-pc
lt.baltic	tr_q-latin5	pl3	ua-utf-ws
bashkir	no-dvorak	dvorak-r	dvorak
ANSI-dvorak	dvorak-l	mac-euro	mac-euro2
mac-fr_CH-latin1	mac-us	mac-de-latin1	mac-be
mac-es	mac-pl	mac-se	mac-dvorak
mac-fi-latin1	mac-template	mac-dk-latin1	mac-de-latin1-nodeadkeys
mac-fr	mac-pt-latin1	mac-uk	mac-it
mac-de_CH	sunt4-no-latin1	sunt5-cz-us	sundvorak
sunt5-de-latin1	sunt5-us-cz	sunt5-es	sunt4-fi-latin1
sunkeymap	sunt4-es	sunt5-ru	sunt5-uk
sun-pl	sunt5-fr-latin1	sunt5-fi-latin1	sun-pl-altgraph

4. Press **Enter** to return to the Configure The Configure Current Node Menu.

Configure NTP Client

1. Enter **8** and press **Enter** to configure an NTP Server.

2. Enter **2** and press **Enter**.

3. Enter the IP address of the NTP Server and press **Enter**.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure Current Node Menu. You can enable the server when you create it, or enable it at a later time using option **5**.

Configure Proxy

OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management (PALM). If the OmniVista Server has a direct connection to the Internet, a Proxy is not required. Otherwise, a Proxy should be configured to enable OmniVista to connect to these external sites (Port 443):

- **ALE Central Repository -** ovrepo.fluentnetworking.com
- **AV Repository -** ep1.fluentnetworking.com
- **PALM -** palm.enterprise.alcatel-lucent.com
- **Call Home Backend -** us.fluentnetworking.com
- **Device Fingerprinting Service -** api.fingerbank.org.

1. Enter **9** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **2** and press **Enter** to configure a Proxy Server.

2. If a proxy has already been configured, the current configuration is displayed. Enter the Proxy Server IP address, along with the port (e.g., 8080).

Note: If **n** (No) is selected, all proxy servers will be disabled.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

4. Enter **3** and press **Enter** to enable the Proxy.

Change Screen Resolution

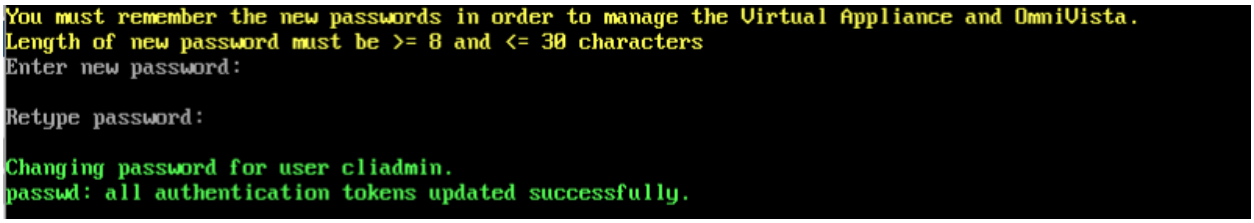
1. Enter **10** and press **Enter** to configure the VA screen resolution.

2. Select a screen resolution and press **Enter**. Enter **y** and press Enter **y** at the confirmation prompt. You will be prompted to restart the VA for the settings to take effect.

3. Enter **y** and press **Enter** at the confirmation prompt to restart the VA.

Configure "cliadmin" Password

Enter **11** and press **Enter** to change the "cliadmin" password for the Node VM. At the prompt, enter the new password and press **Enter**. Re-enter the password and press **Enter**.



Configure "root" Secret Text

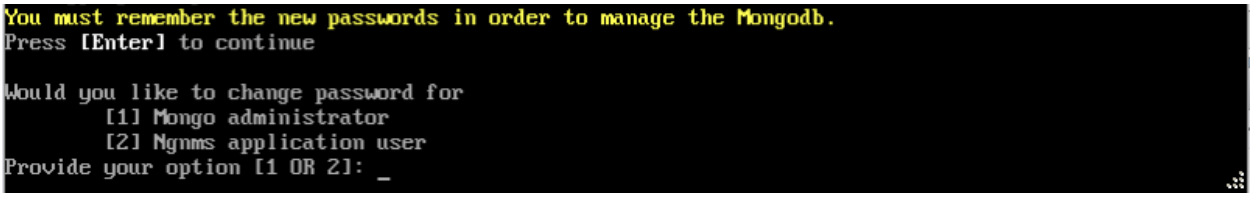
Enter **12** and press **Enter** to change the password of the "root" user of the VA. Enter the old password at the prompt and press **Enter**. Enter the new password and press **Enter**. Confirm the password and press **Enter**.

Enable/Disable Admin SSH

Enter **13** and press **Enter** to enable/disable OmniVista Admin SSH. If enabled, you can log into the OmniVista VM via SSH. If disabled, you can only log in using the Hypervisor Console. Admin SSH is enabled by default.

Configure Mongodb Password

Enter **14** and press **Enter** to change the Mongodb password. You have two options when changing the mongo database password.



Enter **1** to change the mongo administrator password. Enter **2** to change the application user password. At the prompts, enter the current password, then enter the new password.

Configure IPs and Ports

Enter **15** and press **Enter** to change the IP address and ports of the current Node. It is not recommended that you change the configuration of the Cluster once it has been initialized. If a Cluster has already been initialized, you must take a backup of OmniVista and contact Customer Support to re-configure the Cluster.

Configure Hostname

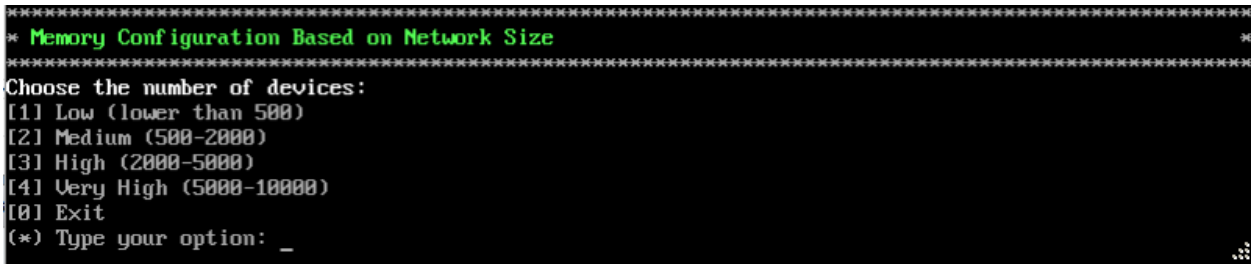
Enter **16** and press **Enter** to change the Hostname of the current Node (maximum of 15 characters).

Extend Data Partitions

Enter **17** and press **Enter** to add an additional hard disk and extend the current data partitions. By default, OV 2500 NMS-E 4.4R2 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you increase the provisioned hard disk.

Configure Network Size

Enter **18** and press **Enter** to configure the Node memory settings. Select an option (e.g., Low, Medium, High, Very High) based on the number of devices being managed and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the Watchdog Service for the change to take effect.



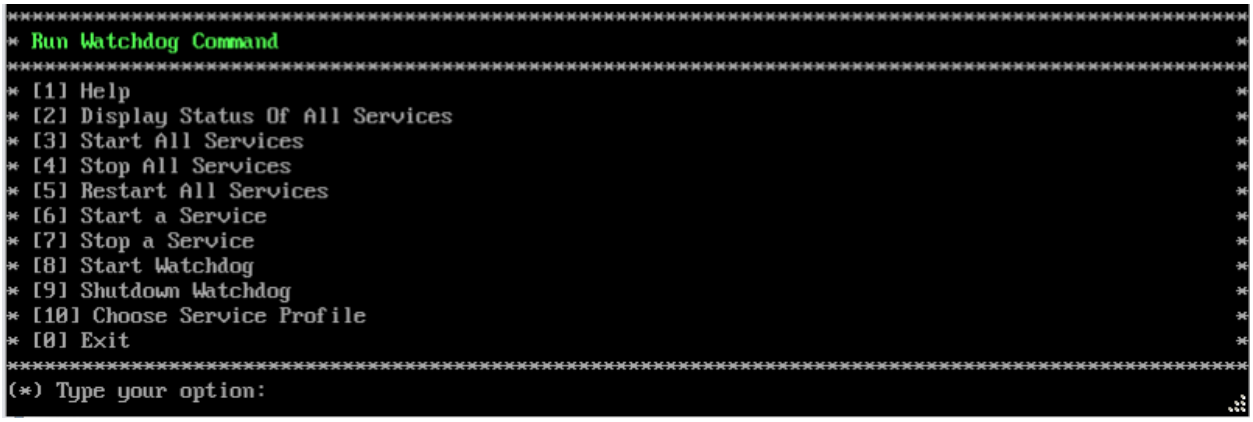
Exit

Enter **0** and press **Enter** to exit to the Configure Current Node Menu and return to the HA Virtual Appliance Menu.

Run Watchdog Command

The Watchdog command set is used to start and stop managed services used by OV 2500 NMS-E 4.4R2. If you stop certain framework services (e.g., ActiveMQ, Apache Tomcat) or a service that these services depend on, the web server will shut down, and you will have to restart the service manually. You will receive a warning prompt whenever you try to shut down one of these services.

To access the Watchdog CLI Command Menu, enter **5** at the command prompt.



The following options are available:

- **Choose Service Profile -** Used to save memory if certain services are not required for your network (e.g., you are not using Stellar APs in your network or you are not using the Application Visibility application). Note that when you change a service profile, all Watchdog Services will be restarted.
  - **All Features (Default) -** All services are started.
  - **No Stellar, No UPAM -** Services required for Stellar APs and UPAM will not be started.
  - **No Application Visibility -** Services required for the Application Visibility application will not be started.
  - **No Stellar, No UPAM, No Application Visibility -** Services required for Stellar APs, UPAM, and Application Visibility will not be started.
- **Display Status Of All Services -** Displays the status of all of the services used by OmniVista (Running/Stopped). To display the status for all services just once (Default), Enter **n** and press **Enter** at the "Continuous Status" Prompt (or just press **Enter**). The status will be displayed and you will be returned to the Run Watchdog Command Menu. To run and display continuous status checks for all services, enter **y** then press **Enter** at the "Continuous Status" Prompt. To stop the display and return to the Run Watchdog Command Menu, enter **Ctrl C**.
- **Start All Services -** Starts all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Stop All Services** - Stop all services. Enter y and press **Enter** at the confirmation prompt.
- **Restart All Services -** Stop and restart all services. Enter **y** and press **Enter** at the confirmation prompt.
- **Start a Service -** Starts a single service. Enter the service name at the prompt and press **Enter**. At the "Start Tree" option, enter **y** and press **Enter** to start all dependent services; enter **n** if you do not want to start dependent services. Press **Enter** at the confirmation prompt to start the service(s).
- **Stop a Service -** Stops a single service. Enter the service name at the prompt and press **Enter**. At the "Stop Tree" option, enter **y** and press **Enter** to stop all dependent services; enter **n** if you do not want to stop dependent services. Press **Enter** at the confirmation prompt to stop the service(s).
- **Start Watchdog -** Starts the Watchdog Service, which starts all services.

- **Shutdown Watchdog -** Stops the Watchdog Service, which stops all services.

Upgrade/Backup/Restore VA

The Upgrade VA command set is used to display information about the currently-installed OmniVista 2500 NMS software, upgrade OmniVista software, configure the OV Build Repository, and backup/restore OV software. OV software and updates are stored on an external repository (ALE Central Repository). By default, the OV Virtual Appliance points to the ALE Central Repository, which contains the latest builds and software updates. If a proxy has been configured, make sure to configure the proxy to connect to the external repository.

Note: If you have configured and enabled a Custom Repository, you must select option **4 – Enable Repository**, and enable the **ALE Custom Repository** to access the latest software.

To access the Upgrade VA Menu, enter 6 at the command prompt. The following options are available:

- **To 4.4R2 (Upgrade to Latest Patch of Current Release, if any) -** Displays information about the currently-installed OmniVista NMS software (e.g., Release Number, Build Number). It also checks for, and displays information about, any available updates. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. Select an option and press **Enter** to display information about the currently-installed OmniVista NMS software and download/upgrade an available update.
  - **Download and Upgrade -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available. (If you are using an Offline Repo, this is the only upgrade option supported. “Download Only” and “Upgrade from a Download Package” are not supported.)
  - **Download Only -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads the update, if available.
  - **Upgrade from a Download Package -** If you have previously downloaded an update but have not yet installed it, OV will install the downloaded update.

    Note: You can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available.
- **To New Release -** Upgrade to a new release. The options and processes are the same as above (“To 4.4R2 (Upgrade to Latest Patch of Current Release, if any”). Note that if a new version of the current release is available, you will be prompted to install the latest version of the current release before upgrading to the new release.

- **Enable Repository -** Enable an OV Build Repository. This is the repository that OmniVista 2500 NMS will use to retrieve OV upgrade software. Select a repository from the list, enter **y** and press **Enter** at the confirmation prompt to enable the repository. Only one (1) repository can be enabled at a time.
- **Configure Custom Repositories -** Configure a custom repository. By default, the OV Virtual Appliance points to the external ALE Central Repository, which contains the latest OV software. However, you can configure up to three (3) custom repositories. Select a repository (e.g., [2] "Custom Repo 1" Repository) and press **Enter**. Complete the fields as described below, then enter **y** and press **Enter** at the confirmation prompt:
  - **Repository Name -** User-configured repository name.
  - **Repository URL -** The URL of the custom repository (e.g., 192.168.70.10/repo/centos). Enter the URL only. There is no need to enter the "https://" prefix.

  Only one (1) repository can be enabled at a time. The user is responsible for ensuring that the custom repository contains the latest OV software.
- **Configure Update Check Interval -** Configure how often the OmniVista 2500 NMS Server will check the OV Build Repository for updates. You can perform a check immediately or schedule the check to be performed at regular intervals. The results of the scheduled checks are displayed on the Welcome Screen.
  - **Check Now -** Run the Update Check Task immediately and displays the results. Enter **2** and press **Enter**. If an update is available, the update information is displayed and the user is prompted select whether or not to upgrade to the latest OV software. If an upgrade is available, enter **y** and press **Enter** to install the upgrade. Note that you can only upgrade to the latest OV software - only the latest software will be presented for upgrade, if available. Also note that if a new release is available (e.g., R01 to R02), and do not have the latest R01 software patches installed, you will first be prompted to install the latest R01 patches, and will then be prompted to install R02.
  - **Check Daily/Weekly/Monthly -** Run the Update Check Task at the configured intervals and displays the results on the Welcome Screen. Select an interval and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
  - **Disable (Default) -** Disable the Update Check Task. Enter **6** and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt.
- **Backup/Restore OV2500 NMS Data -** Backup/Restore OmniVista 2500 NMS data. The following options are available. Note that Backup/Restore is only supported on Standalone Installations, not HA Installations.
  - **Configure Backup Retention Policy -** Configure the maximum number of days that you want to retain backups (Range = 1 – 30, Default = 7), and the maximum number of backups that you want to retain (Range = 1 – 30, Default = 5). Backup files are automatically deleted based on the Backup Retention Policy.
  - **Backup Now -** Perform an immediate backup. Enter an optional name for the backup (default = ov2500nms) and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. When the backup is complete, it will be stored in the "backups" Directory with the backup name and the date and time of the backup (<base name>_<yyyy-MM-dd--HH-mm>.bk). If you do not enter a name, the backup will be stored as ov2500nms- yyyy-MM-dd--HH-mm>.bk. (e.g., ov2500nms-2018-11-16--16-21.bk).

- **Schedule Backup -** You can schedule an automatic backup to begin at a specific time and repeat at a specific daily interval. Enter a time for the backup to begin (HH:mm format) and press **Enter**. Enter the time between backups (Range = 1 – 30 Days, Default = 1) and press **Enter**. You can change the backup schedule at any time.

  Note: Scheduled backups utilize the Task Scheduler (Windows) and Cron Job (Linux) utilities. If necessary, these utilities can be used to modify a scheduled backup.

  Note: Backup files are automatically deleted based on the Backup Retention Policy. Monitor and maintain the Backup Directory to optimize disk space.

- **Restore -** Select a backup and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt and press **Enter**.

  Note: You can only perform a restore using a backup from the same release (e.g., you can only restore a 4.4R2 configuration using a 4.4R2 Backup File). OmniVista will not allow you to perform a restore using a backup from a previous release.

  Note: If you want to perform a restore using a 4.4R2 Backup File residing on a different system, you must change the OV IP address/ports and UPAM IP address/ports of the system on which you are performing the restore to match the OV IP address/ports and UPAM IP address/ports of the system from which the backup file was taken before performing the restore. After the restore is complete, you can use the Configure Cluster Menu to return the restored system to its original OV IP address/ports and UPAM IP address/ports.

  For example, if you want to use a backup file on System A to perform a restore on the System B, you must change the OV IP address/ports and UPAM IP address/ports of System B to the OV IP address/ports and UPAM IP address/ports of System A before performing the restore. After the restore is complete, you can use the Configure Cluster Menu to change the OV IP address/ports and UPAM IP address/ports on System B back to their original configuration.

- View Backup Configurations - View the backup retention policies. The policies are configured using Option 2 – Configure Backup Retention Policy. Note that if you have not configured a Backup Retention Policy, the “Maximum Backup Retention Days” and Maximum Backup Retention Files” fields will show “-1”.

Logging

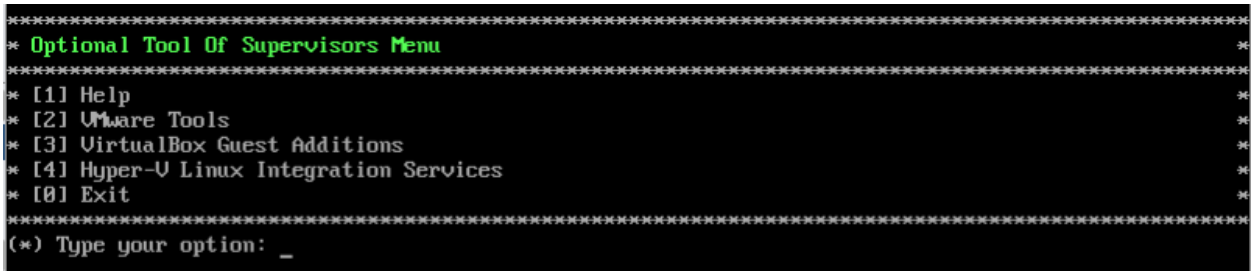
You can view OV 2500 NMS-E 4.4R2 Logs using the “Logging” option. Enter **7**, then press **Enter**.

The following options are available:

- **Change Log Level -** Changes the logging level for OV services. Enter the number corresponding to the OV service for which you want to change the logging level (e.g. 13 - ovsip) and press **Enter**. Enter the number corresponding to the package for which you want to change the logging level (e.g. 1 - com.alu.ov.ngms.sip.service) and press **Enter**. Enter the number corresponding to the log level you want to set (e.g., 2 - DEBUG) and press **Enter**.
- **Collect Log Files -** Collects all log files from a specific date to the current date. Enter the date from which you want to collect log files in dd-MM-yyyy format (e.g., 10-15-2018) and press **Enter**. When finished, a "Collecting completed" message is displayed. The log files are stored in a zip file in the "logs" Directory with the date and time the logs were collected appended to the file name (e.g., ovlogs-15-10-2018_12-04-18.zip). SFTP to the VA using the "cliadmin" username and password to view the log files (Port 22).
- **Collect JVM Information -** Collects and archives Java Virtual Machine (JVM) information. Enter **y** and press **Enter** at the confirmation prompt to collect JVM information. When finished, a "Collecting completed" message is displayed along with the JVM information file name. The file is stored in the "jvm-info" directory with date and time the file was created collected appended to the file name (e.g., jvm -info-02018-10-15-12-18-43.jar). SFTP to the VA using the "cliadmin" username and password to view the log file (Port 22).

Set Up Optional Tools

Enter **8**, then press **Enter** to bring up the Setup Optional Tools command set. The Setup Optional Tools command set is used to install/upgrade Hypervisor Optional Tools Packages.



Enter the number corresponding to the Hypervisor you are using (**2 - VMWare**, **3 - Virtual Box**, **4 - Hyper-V**) and press **Enter**. Information about available packages is displayed. If a new package is available, enter **y** and press **Enter** at the "Would you like to install the package" prompt. The package will automatically be downloaded from the OV Repository and installed (this may take several minutes). When the "Installation Complete" messaged is displayed, press **Enter** to continue. Press **Enter** again to restart the Virtual Appliance.

Advanced Mode

Advanced Mode enables you to use read-only UNIX commands for troubleshooting. Enter **9**, then press **Enter** to bring up the CLI prompt. Enter **exit** and press **Enter** to return to the Virtual Appliance Menu. The following commands are supported:

- /usr/bin/touch
- /usr/bin/mktemp
- /usr/bin/dig

- /usr/bin/cat
- /usr/bin/nslookup
- /usr/bin/which
- /usr/bin/less
- /usr/bin/tail
- /usr/bin/vi
- /usr/bin/tracepath
- /usr/bin/tty
- /usr/bin/systemctl
- /usr/bin/grep
- /usr/bin/egrep
- /usr/bin/fgrep
- /usr/bin/dirname
- /usr/bin/readlink
- /usr/bin/locale
- /usr/bin/ping
- /usr/bin/traceroute
- /usr/bin/netstat
- /usr/bin/id
- /usr/bin/ls
- /usr/bin/mkdir
- /usr/sbin/ifconfig
- /usr/sbin/route
- /usr/sbin/blkid
- /usr/sbin/sshd-keygen
- /usr/sbin/consoletype
- /usr/sbin/ntpdate
- /usr/sbin/ntpq
- /usr/bin/ntpstat
- /usr/bin/abrt-cli
- /usr/sbin/init
- /usr/sbin/tcpdump
- /bin/mountpoint

Power Off

Before powering off the VM, you must stop all services using the **Stop All Services** option in the **Run Watchdog Command**. After all the services are stopped, enter **10** at the command line to power off the VM. Confirm the power is off by entering **y**. The power off may take several minutes to complete.

Note: OV 2500 NMS-E 4.4R2 functions stop running following power off. The VM must be powered back on via the VMware client software and you must log back into the VM via the console.

Reboot

Before rebooting the VM, you must stop all services using the **Stop All Services** option in the **Run Watchdog Command**. After all services are stopped, enter **11** at the command line to reboot the VM. Confirm reboot by entering **y**. The reboot may take several minutes to complete. When rebooted, you will be prompted to log in through the cliadmin user and password prompts. Note that OV 2500 NMS-E 4.4R2 functions continue following reboot.

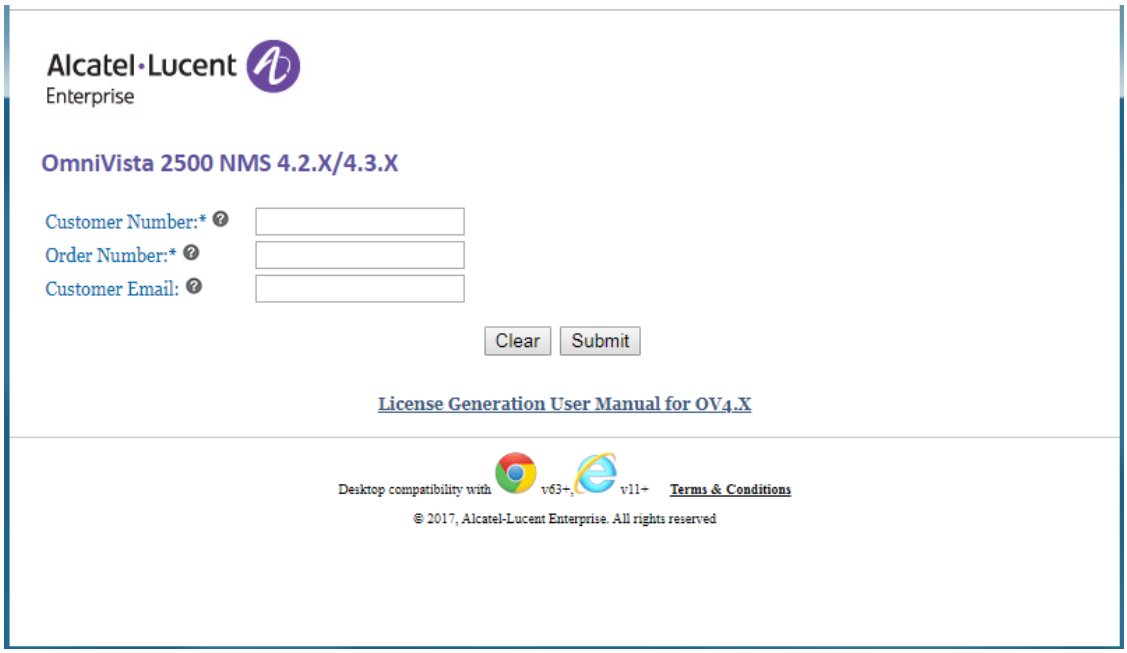
Log Out

To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OV 2500 NMS-E 4.4R2 functions continue following logout.

Appendix D – Generating an Evaluation License

An Evaluation License provides full OV 2500 NMS-E 4.4R2 feature functionality, but is valid only for 90 Days (starting from the date the license is generated). There is one file that contains all of the Device (AOS, Third-Party, Stellar APs) and Service Licenses (VM, Guest, BYOD). Follow the steps below to generate an Evaluation License Key.

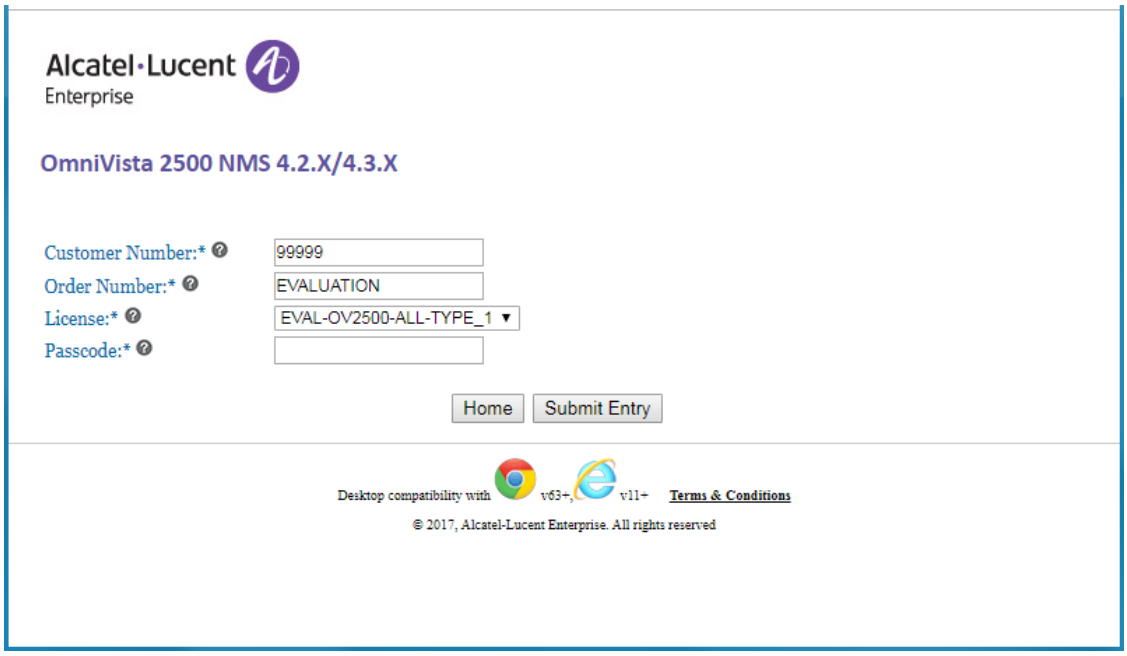
1. Go to https://lds.al-enterprise.com/ARB/loadOmniVistaLicGeneration.action.



2. Complete the fields as described below, the click **Submit**.

- **Customer ID –** 99999
- **Order Number –** evaluation
- **Customer Email –** Enter your contact email.

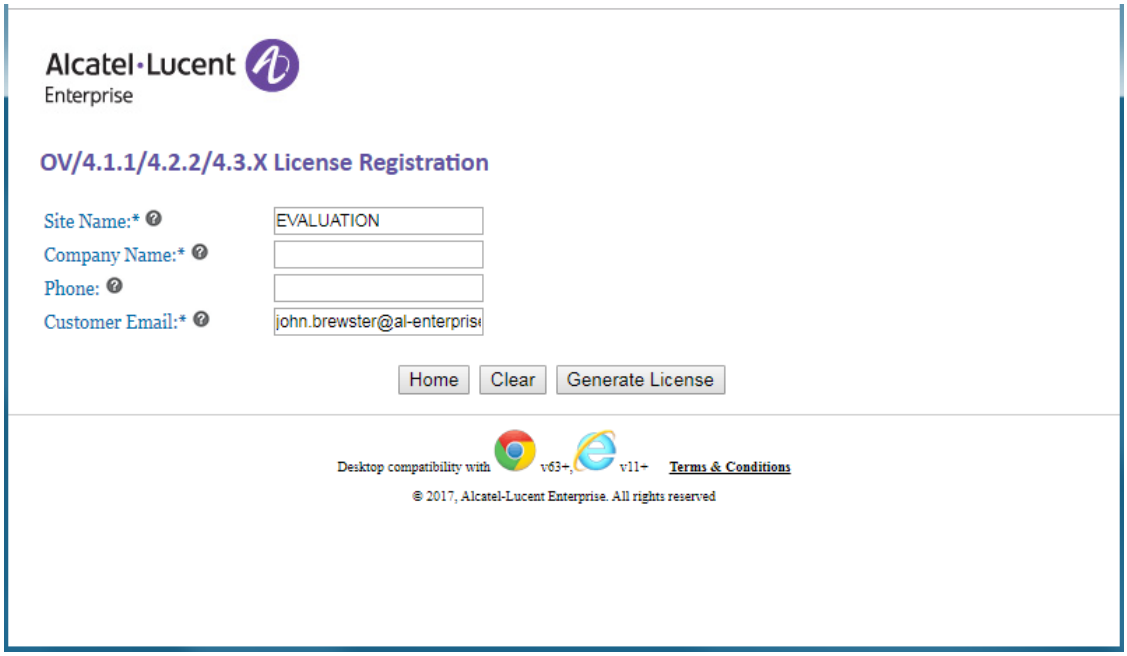
The following screen will appear.



3. Complete the fields as described below, the click **Submit Entry**.

- **Customer ID –** 99999 (pre-filled)
- **Order Number –** EVALUATION (pre-filled)
- **License –** EVAL-OV2500-ALL-TYPE_1 (pre-selected)
- **Passcode –** omnivista

The following screen will appear.



4. Complete the fields as described below, the click **Generate License**.

- **Customer ID –** 99999 (pre-filled)
- **Site Name –** EVALUATION
- **Company Name –** Company name to be used for the license
- **Phone –** Contact phone number
- **Customer Email –** E-mail address to which the license will be sent.

The license will be downloaded to your computer. (The license file will also be e-mailed to the address you entered in the screen above.)

5. Go to the **License – Add/Import License Screen** in OmniVista to import the license file you just downloaded.