Installation and Upgrade Guide

for

OmniVista 2500 NMS Enterprise
Version 4.3R1

June 2018

Revision B

Part Number 060547-10

READ THIS DOCUMENT

OmniVista 2500 NMS
for

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

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 4.3R1 Installation and Upgrade Guide

This document details the OmniVista 2500 NMS Enterprise 4.3R1 (OV 2500 NMS-E 4.3R1 installation/upgrade process. OV 2500 NMS-E 4.3R1 can be installed as a fresh installation from a download file available on the Customer Support website; or you can upgrade from OV 2500 NMS-E 4.2.2.R01 (MR2) using the OmniVista 2500 NMS Software Repository. Note that 4.2.2.R01 (MR2) includes the initial MR2 GA release (Build 115) as well as installations with any official patches installed.

If you are upgrading from an earlier release (3.5.7 – 4.2.2.R01 (MR1)), you must first upgrade to 4.2.2.R01 (MR2). The Upgrade Matrix below shows the upgrade paths that must be followed to get to 4.2.2.R01 (MR 2).

> **Note:** OV 2500 NMS-E 4.3R1 can be installed as a Standalone Installation or in a High-Availability configuration. However, you can only upgrade from OV 2500 NMS-E 4.2.2.R01 (MR 2) if you are upgrading to a standalone installation. Upgrade is not supported on a High-Availability installation.

Upgrade Matrix For OV 4.3R1

From	To OV 4.3R1
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
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
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
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
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
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

From	To OV 4.3R1
	Step 4: Automatic Upgrade to 4.3R1 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
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
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
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

* 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: If your network includes Stellar APs, you **must** upgrade these devices to AWOS 3.0.3.x 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 2500 NMS Screen).

Installing OV 2500 NMS-E 4.3R1

OV 2500 NMS-E 4.3R1 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 4.3R1 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, and 6.5
- VirtualBox: 5.2.x
- MS Hyper-V: 2012 R2 and 2016.

The sections below detail each of the steps required to deploy OV 2500 NMS-E 4.3R1 as Virtual Appliance on VMware, VirtualBox, and Hyper-V. If you are upgrading from OV 2500 NMS-E 4.2.2.R01 (MR 2), see Upgrading from OV 2500 NMS-E 4.2.2.R01 MR 2.

Note that If you are deploying OV 2500 NMS-E 4.3R1 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 OmniVista instability. For instance, if you allocate 16GB of memory for OV

VA but configure the network size to be Medium (500 – 2,000 devices) instead of Low (fewer than 500 devices), OmniVista may experience unexpected issues. Refer to Recommended System Configurations below for details.

Recommended System Configurations

The table below provides recommended Hypervisor configurations based on the number of devices being managed by OV 2500 NMS-E 4.3R1 (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 Cores	2.4 GHz 8 Cores	2.4 GHz 12 Cores	2.4 GHz 12 Cores
OV VA RAM	16GB	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:

- OmniVista VM RAM is configured from the Hypervisor
- Hypervisor Processors are configured from the Hypervisor.
- HDD Provisioning is configured from the VA Menu. By default, OV 2500 NMS-E 4.3R1 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 the increase the HDD2 provision. The data partition size is configured using the Configure Network Size menu option in the Configure the Virtual Appliance Menu.

Standalone and High-Availability Installations

OV 2500 NMS-E 4.3R1 can be installed in a Standalone or High-Availability configuration. A High-Availability 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). If Node 1 fails, OmniVista will automatically failover to Node 2. For a High-Availability

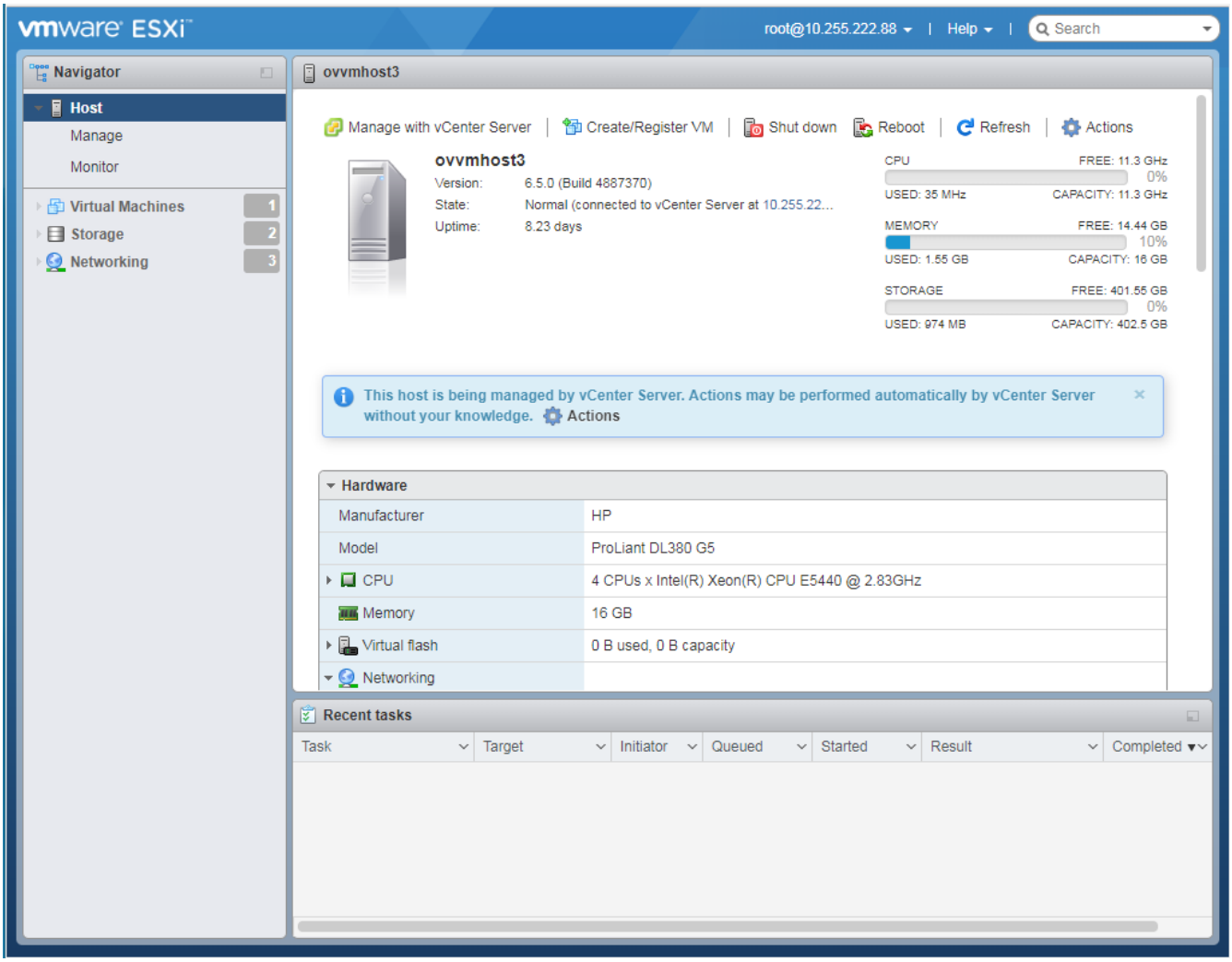
installation, you must deploy **two** (2) VMs – one for the Active OmniVista Server (Node 1) and one for the Standby OmniVista Server (Node 2).

> **Note:** At this time the High-Availability Feature is only supported on small networks ("Low" - up to 500 devices).

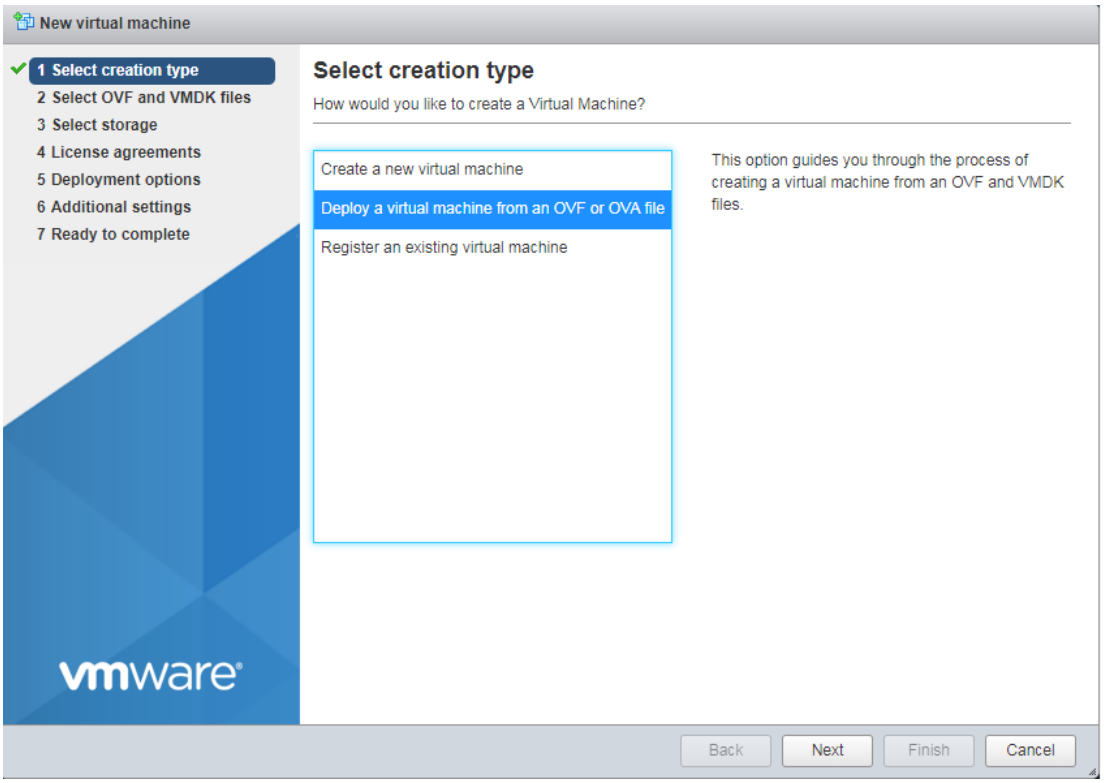
Deploying the Virtual Appliance in VMware ESXi

1. Download and unzip the OVF package.

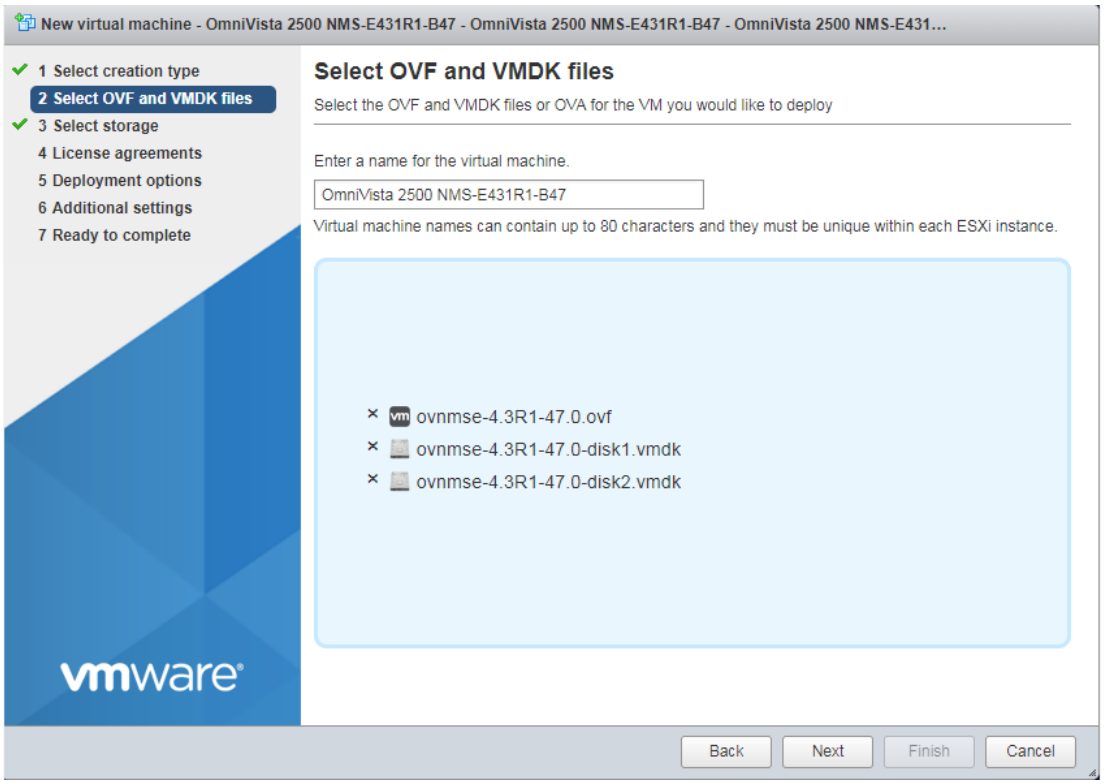
2. Log into VMware ESXi.



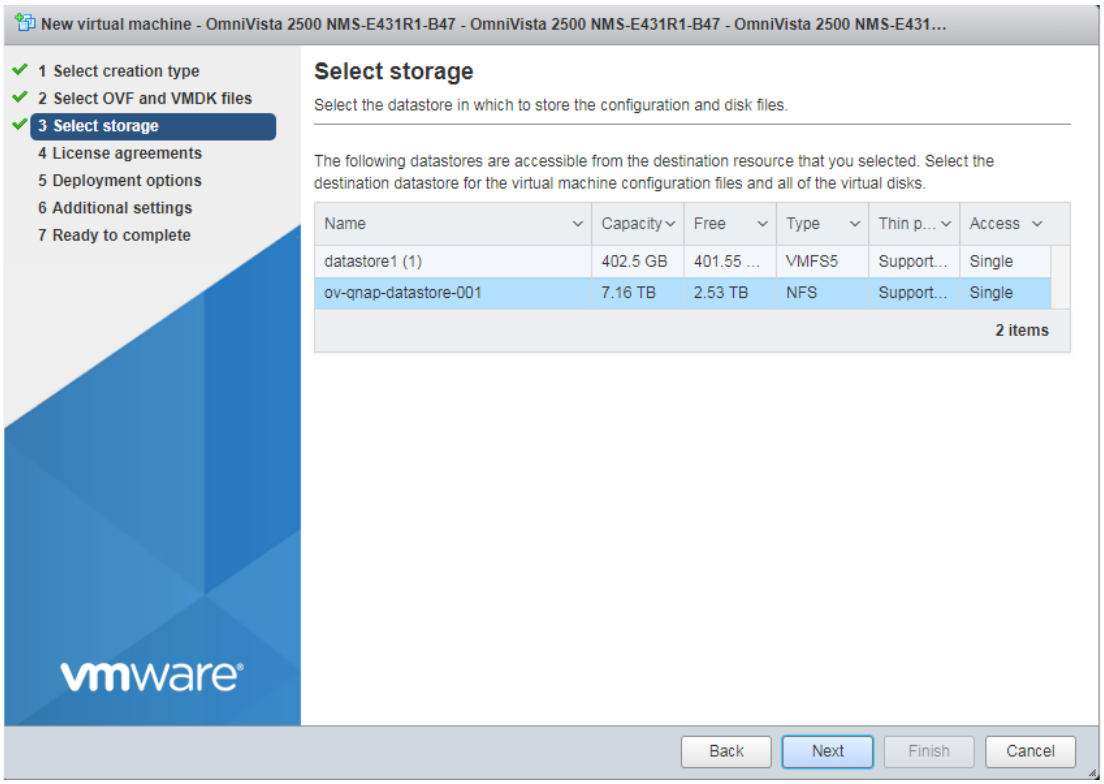
3. Select the Host on which you want to install OV 2500 NMS-E 4.3R1 and click on **Create/Register VM**. The first screen of the New Virtual Machine Wizard appears.



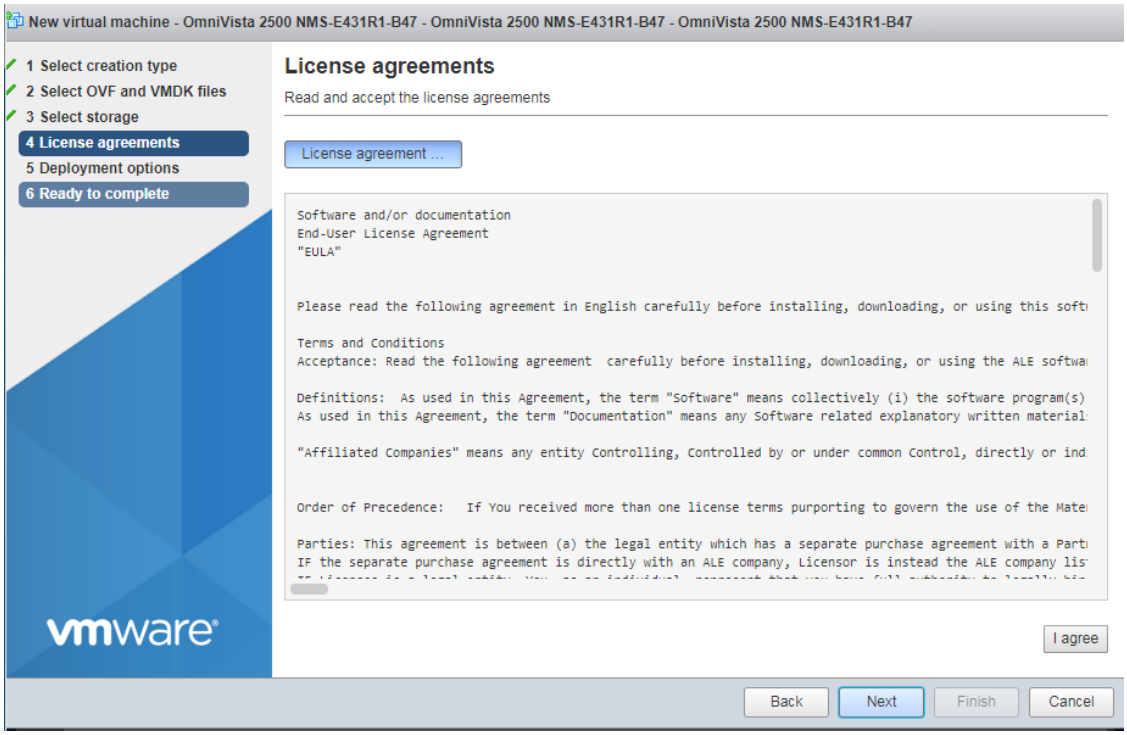
4. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



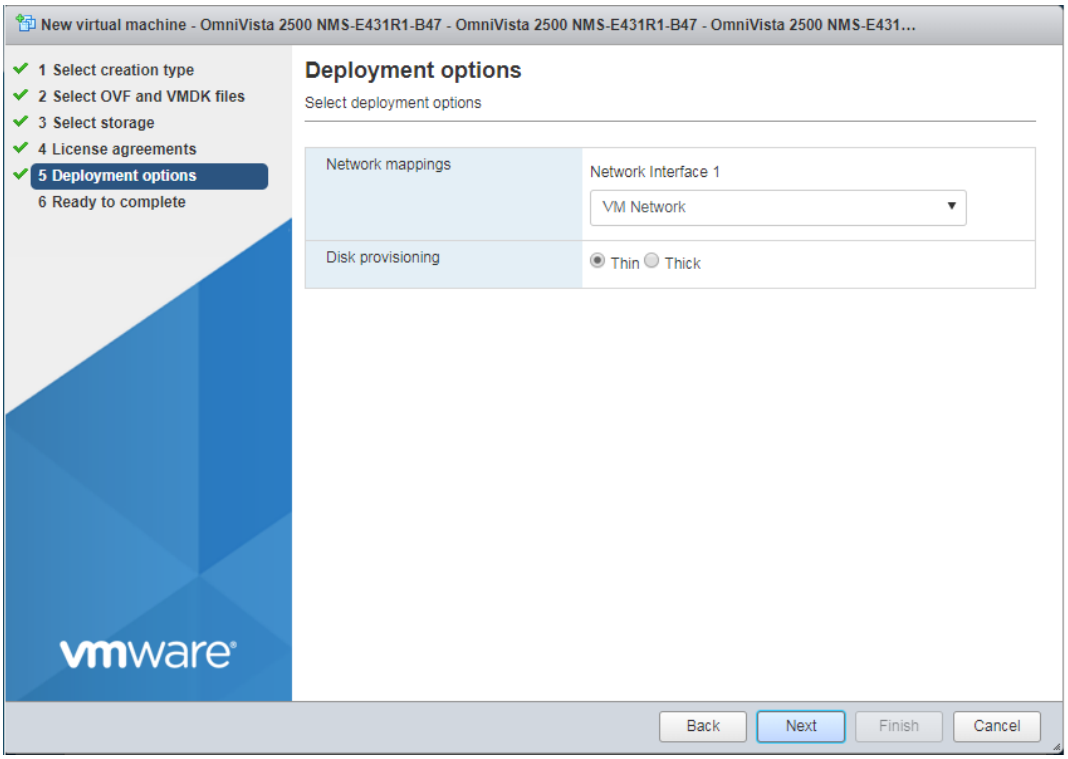
5. Enter a name for the VM, select the OVF File and both VMDK Files (disk 1 and disk 2) from the download archive), then click **Next**.



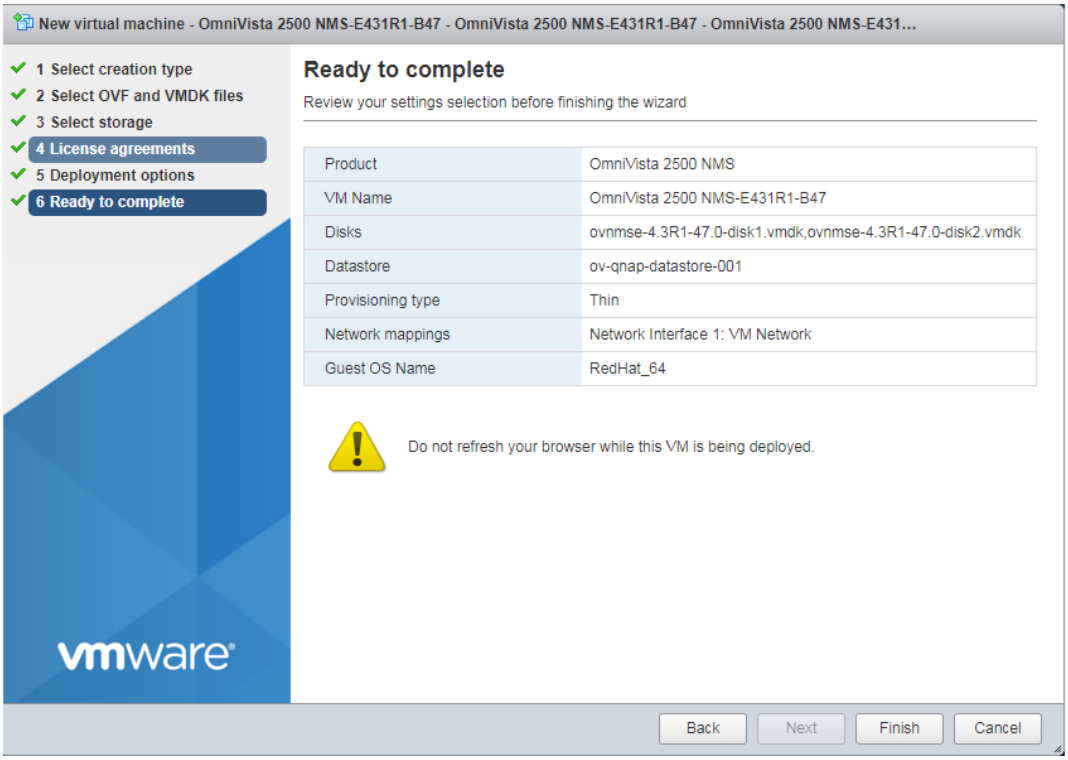
6. Select the destination storage where the template is to be deployed, then click **Next**.



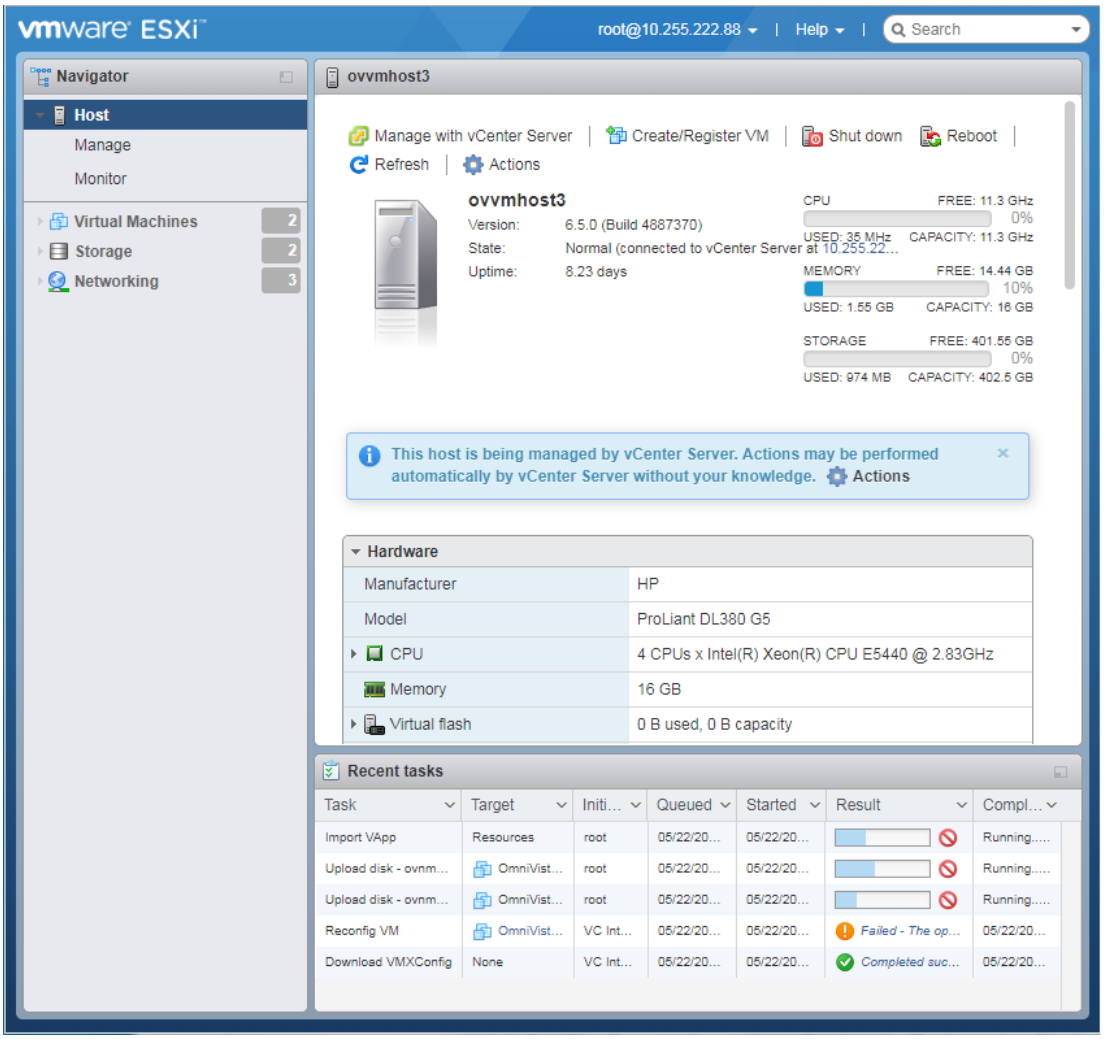
7. Review the License Agreement, click **I agree**, then click **Next**.



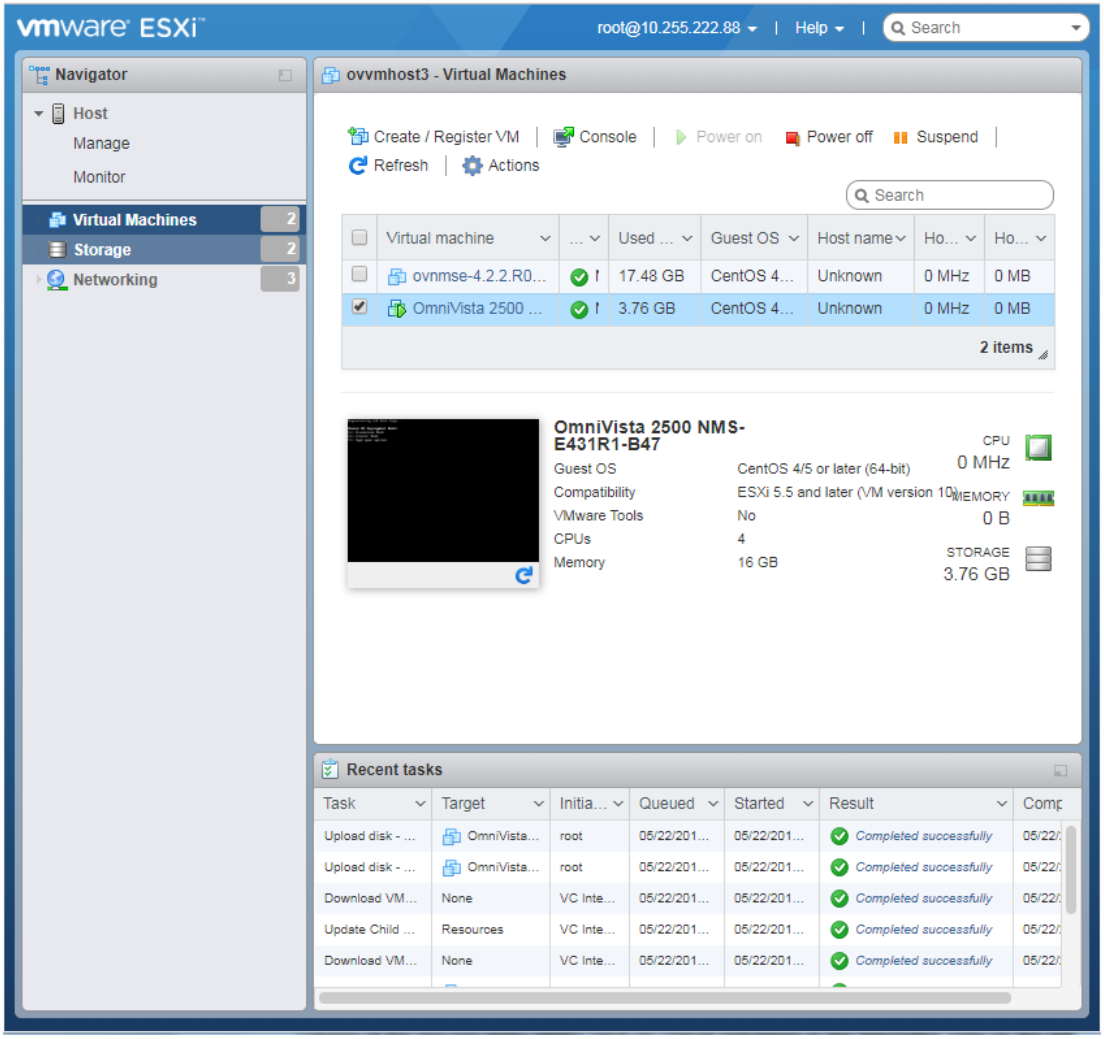
8. In the **Network mapping** field, select the Destination network that the deployed VM will use. In the **Disk provisioning** field, select **Thin**. Click **Next**.



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



10. When the installation is complete (indicated by “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.



11. Select the VM you just deployed. Basic details for the VM are displayed. Click on Console at the top of the screen to open a Console and go to Completing the OmniVista 2500 NMS-E 4.3R1 Installation to complete the installation.

Remember, if you are installing a High-Availability configuration, 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** completing the OmniVista 2500 NMS-E 4.3R1 Installation.

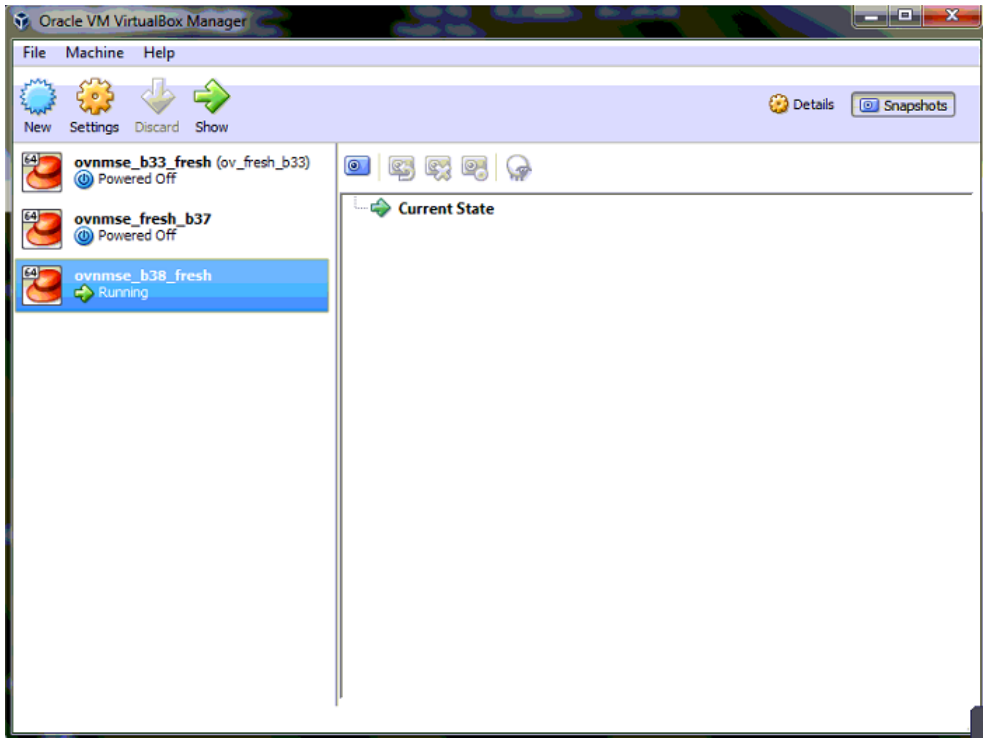
Deploying the Virtual Appliance in VirtualBox

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.

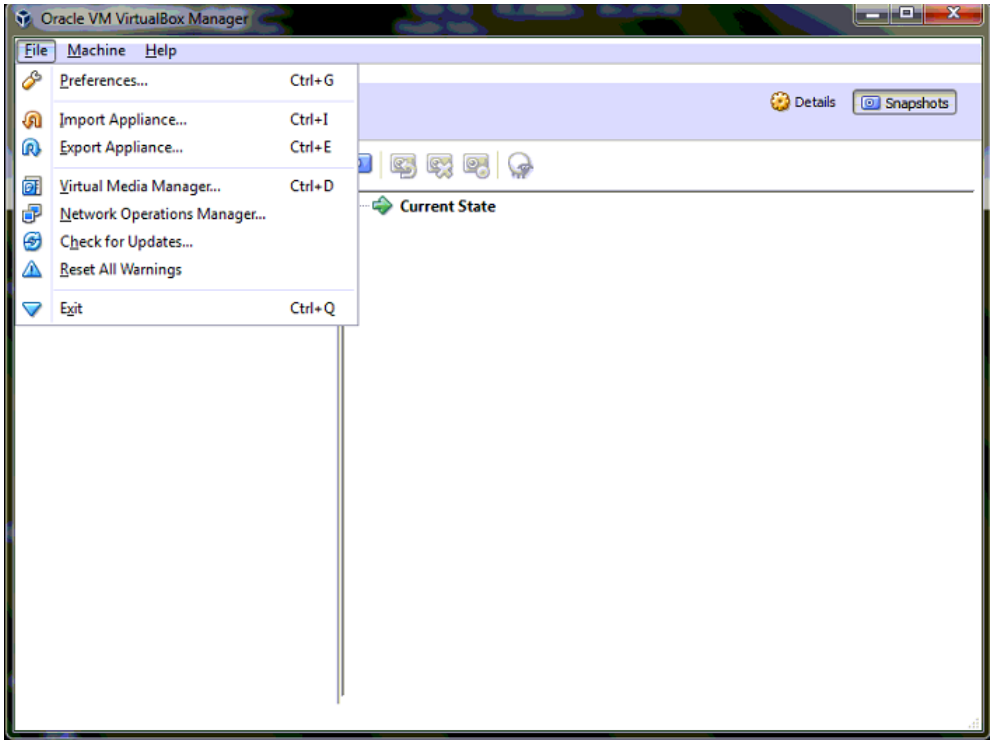
> **Note:** If you are deploying OV 2500 NMS-E 4.3R1 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See Appendix A for details.

1. Download and unzip the OVF package.

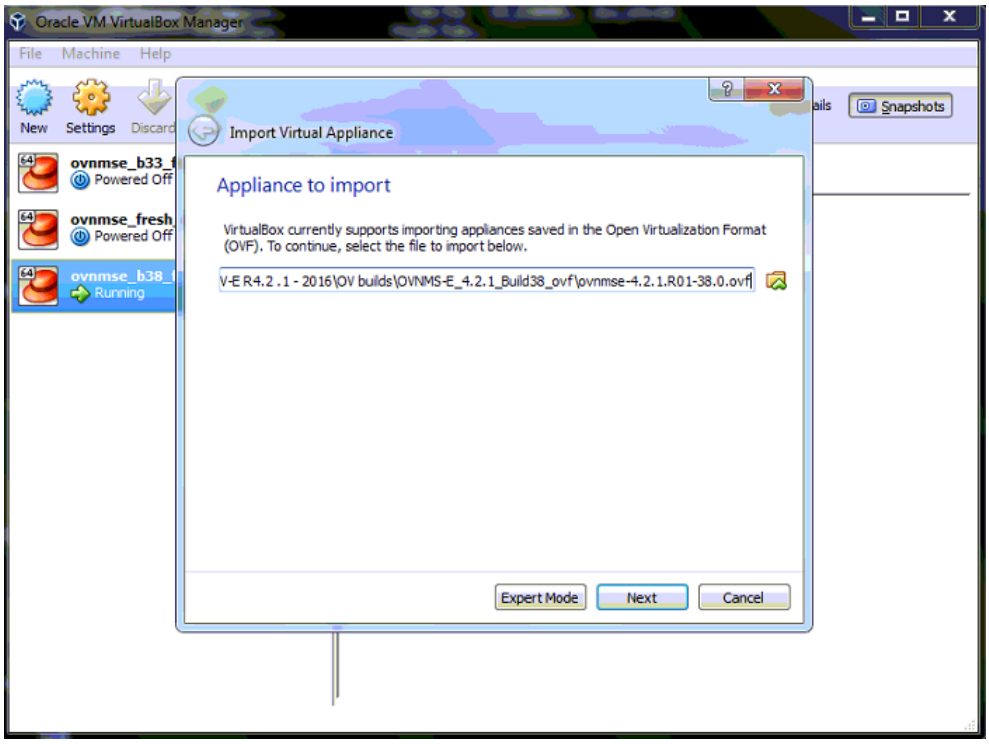
2. Log into Windows 7 and open the Oracle VM VirtualBox tool.



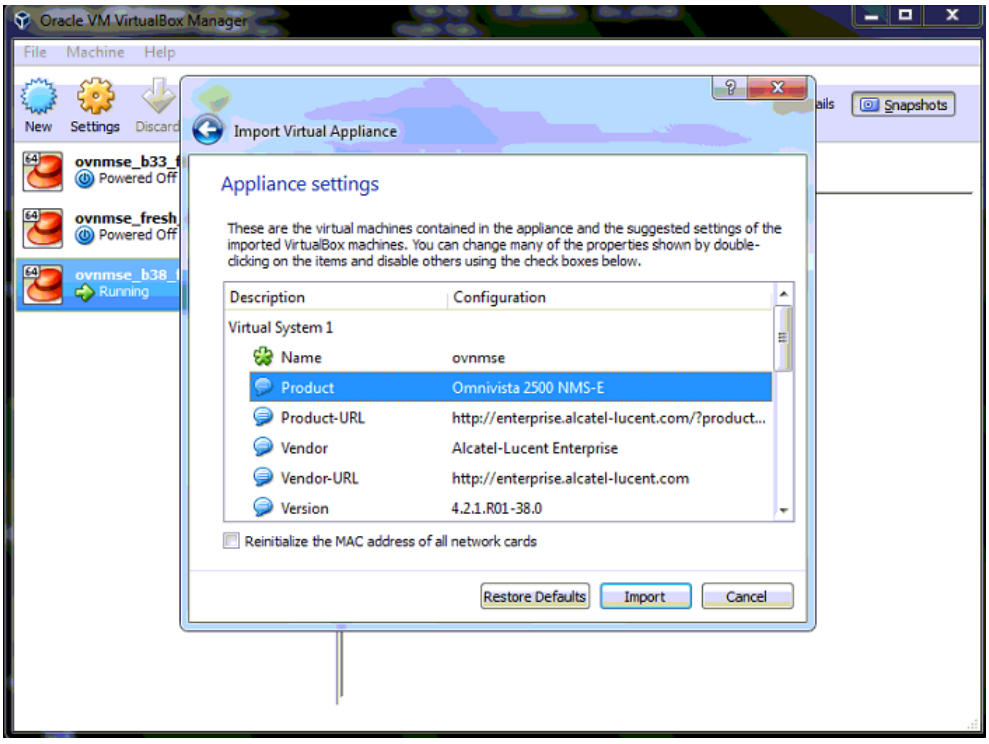
3. Click **File > Import Appliance**.



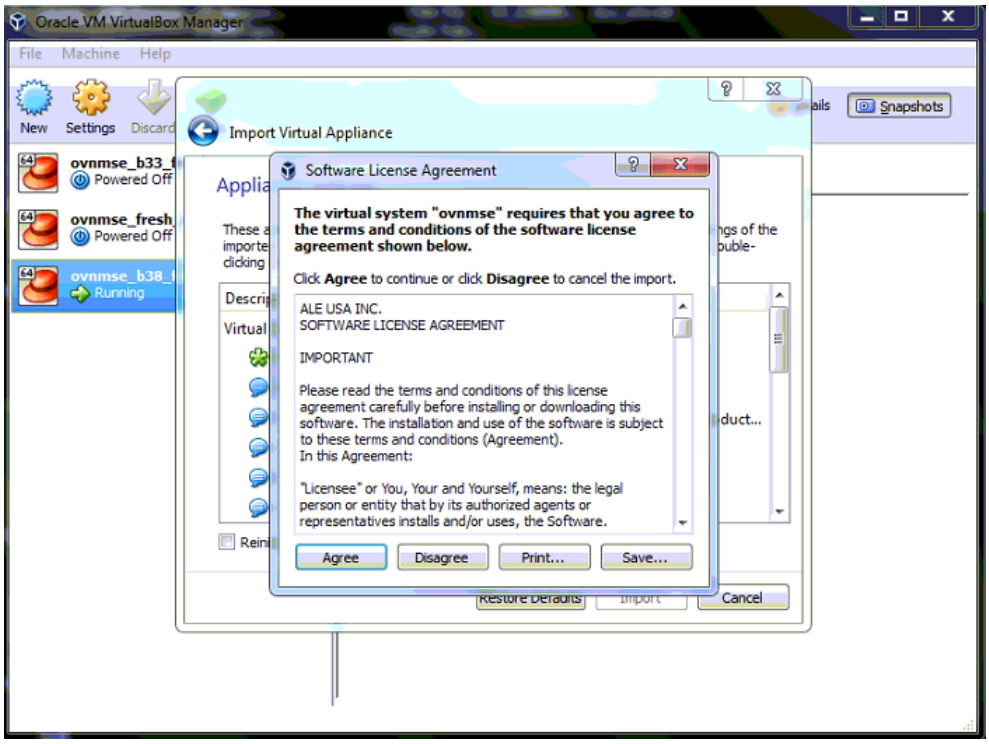
4. Click **browse** icon then select the **folder** which you extracted at step 1 above, then click **Next**.



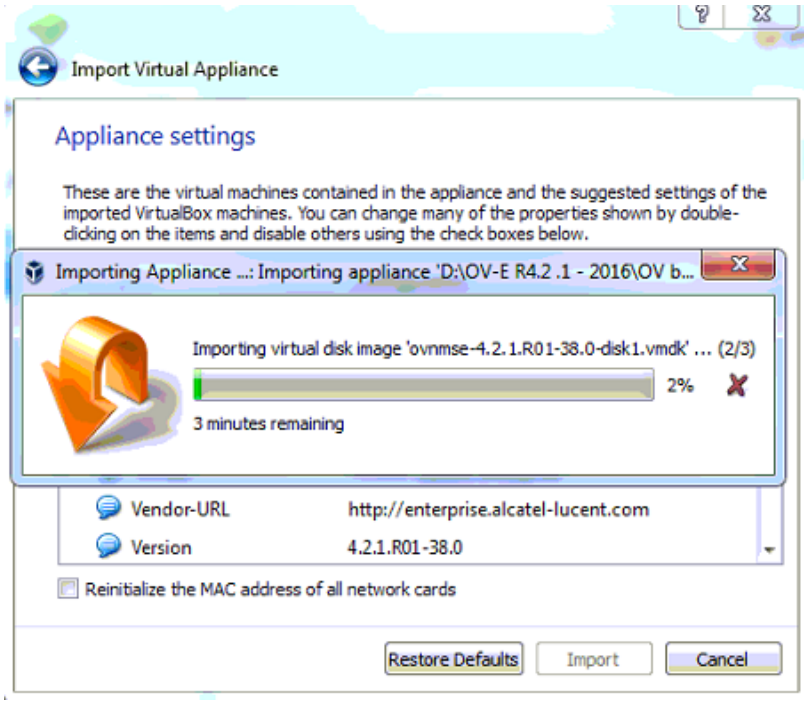
5. Review the configuration and click **Import**.



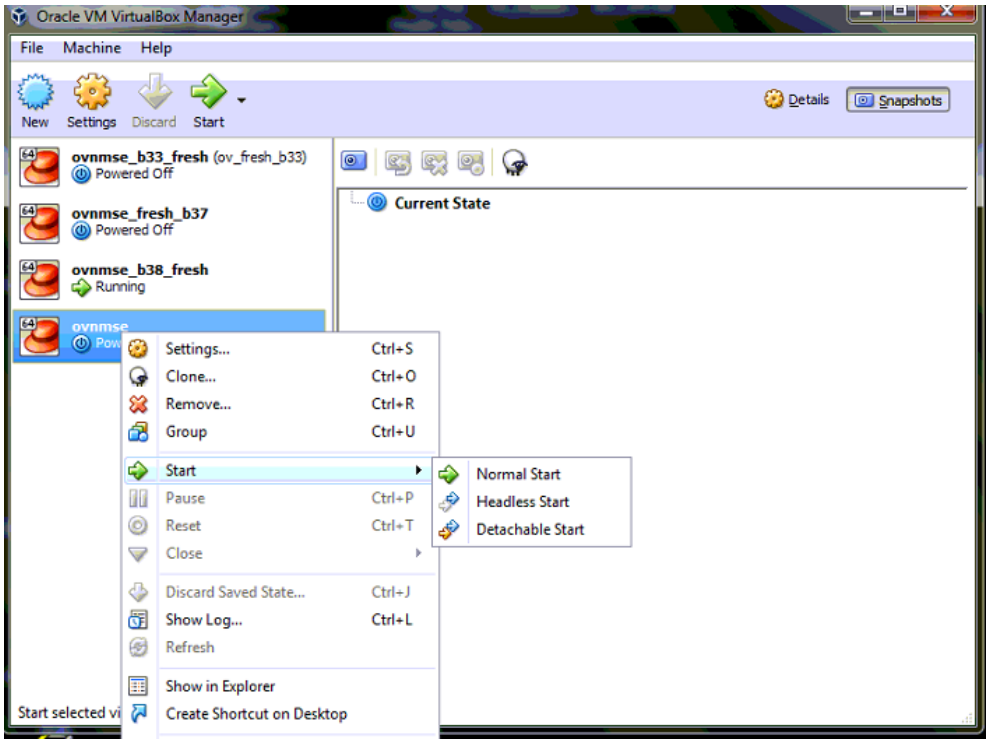
6. The **Software License Agreement** window displays, click on **Agree**.



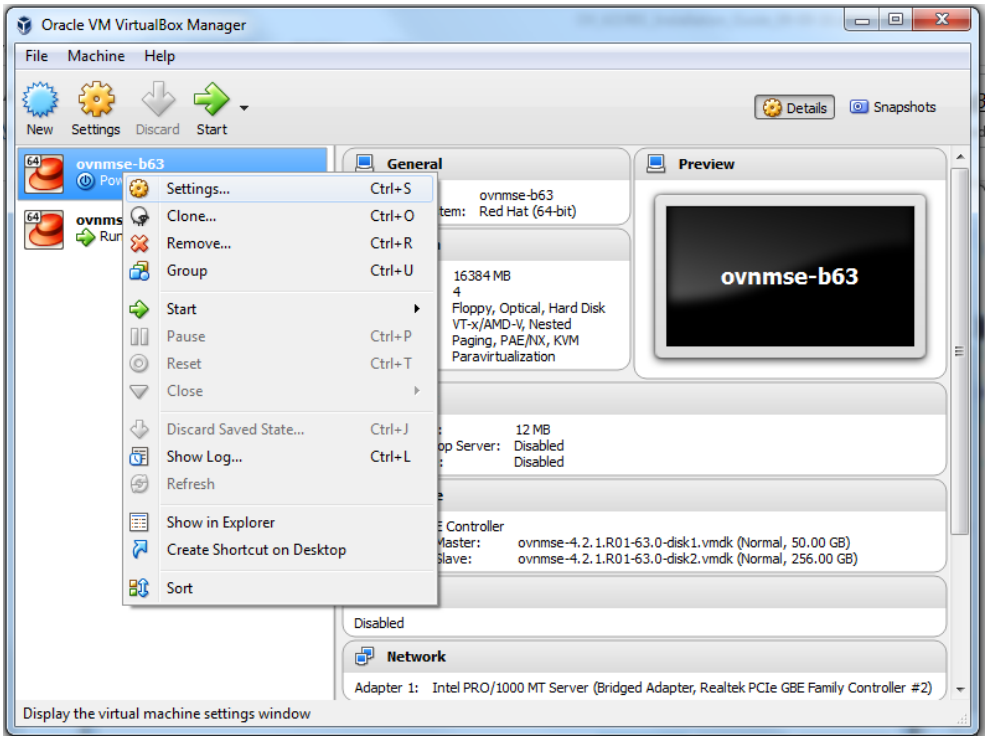
7. A status window appears and displays the progress of the deployment.



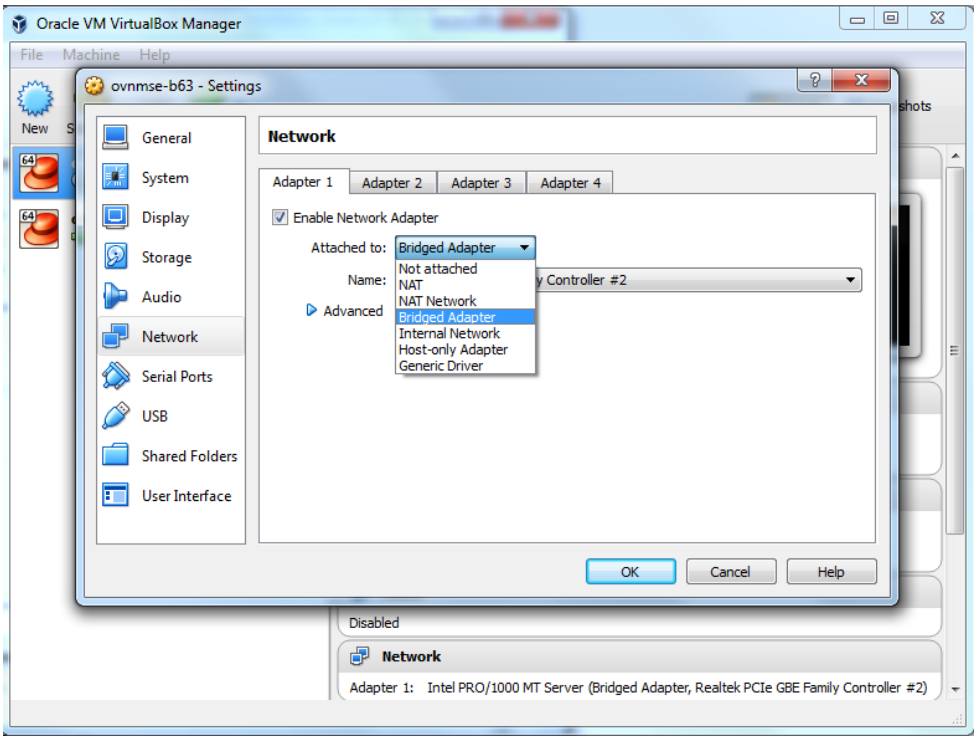
8. After the process is completed, right-click on the VM in the Navigation Panel and select **Start - Normal Start**.



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 2500 NMS-E 4.3R1 Installation to complete the installation.

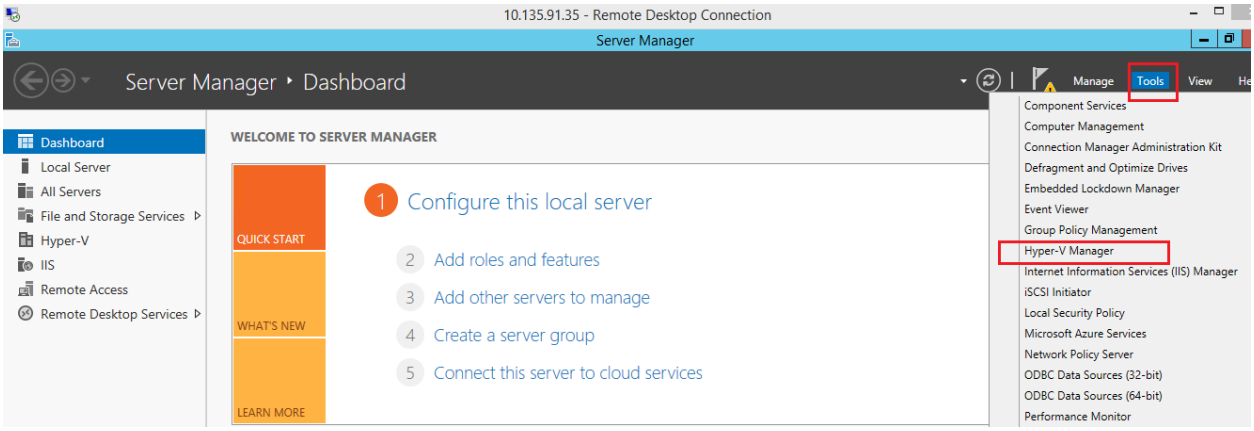
Remember, if you are installing a High-Availability configuration, you must deploy **two** (2) VMs – one for the Active OmniVista Server (Node 1) and one for the Standby OmniVista Server (Node 2). Make sure to deploy **both** VMs **before** completing the OmniVista 2500 NMS-E 4.3R1 Installation.

Deploying the Virtual Appliance in Hyper-V

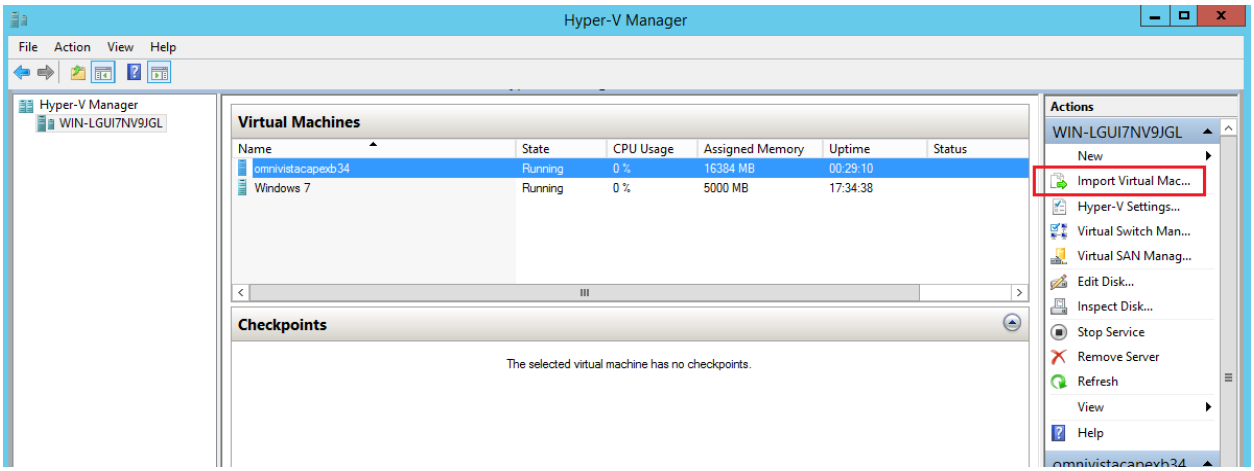
Note that in the instructions below, Hyper-V in Windows 2012 is used for demonstration purposes. Some of the screens shown may depict an older OmniVista Release.

1. Download and unzip the OVF Hyper-V package.

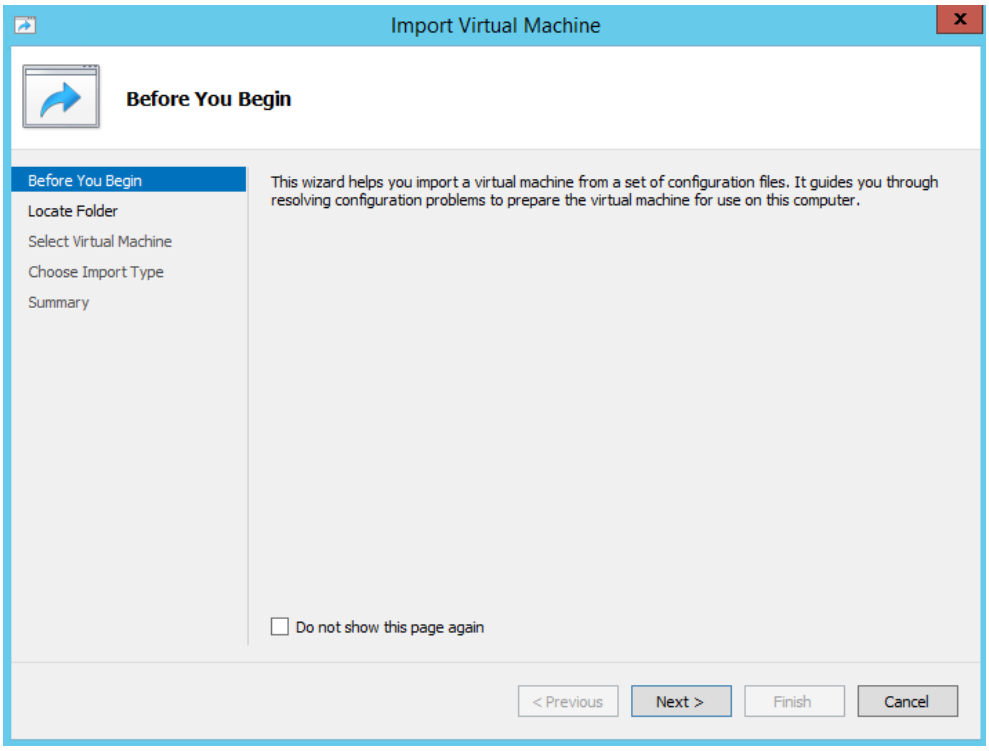
2. Log into Windows 2012 and open the Hyper-V tool.



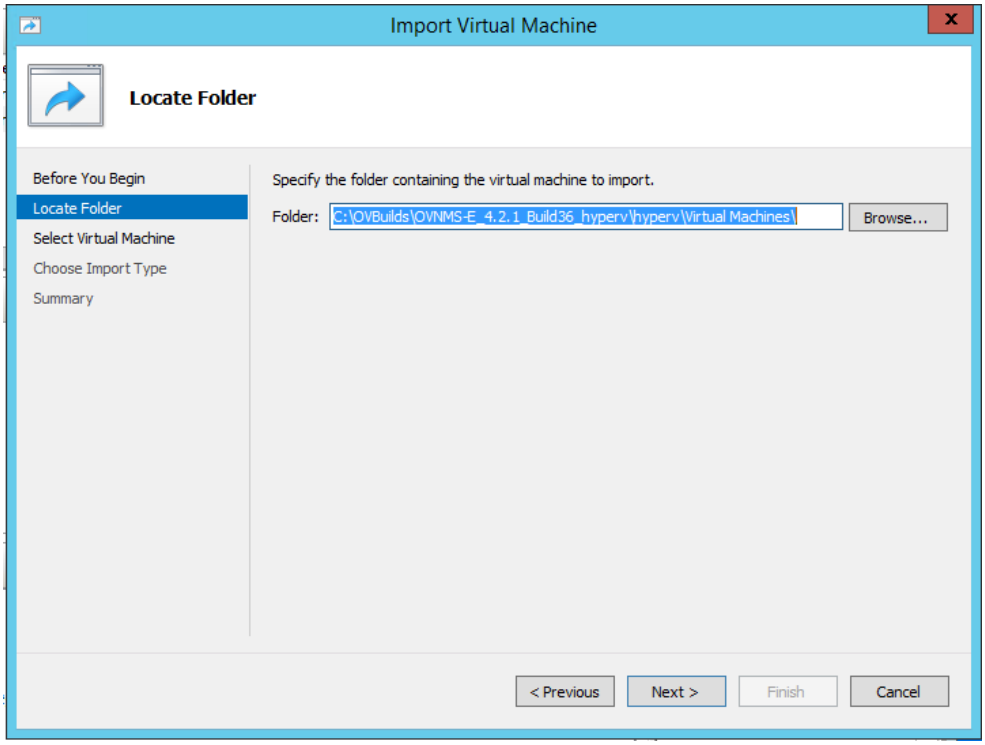
3. Select the Host on which you want to install OmniVista 2500 NMS, click on **Actions > Import Virtual Machine**.



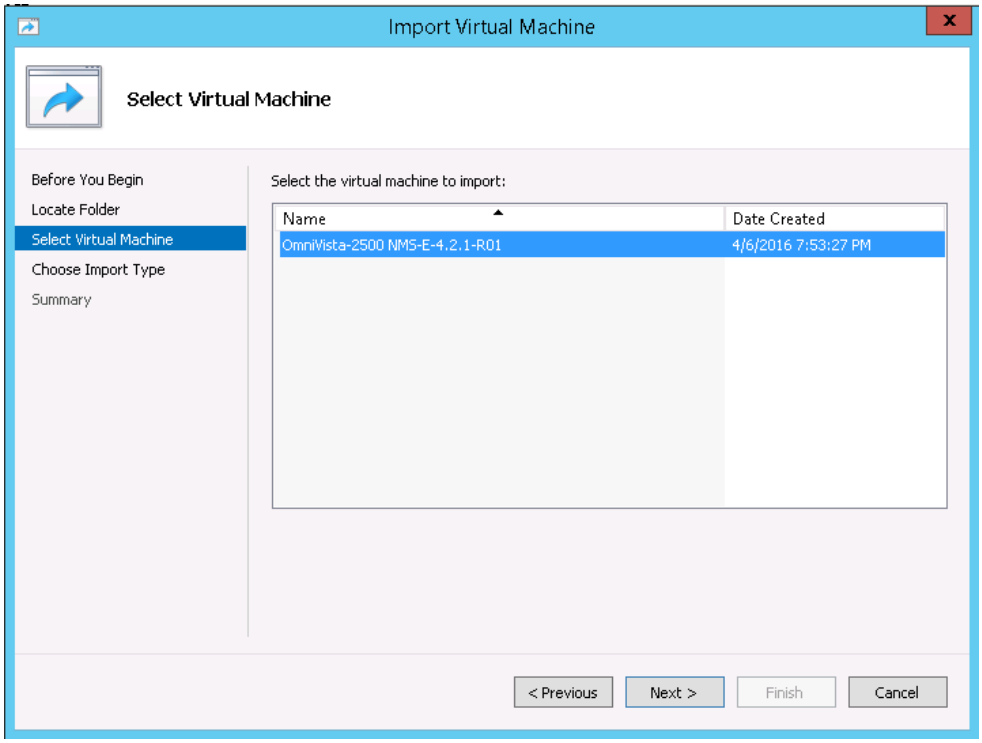
4. The Import Virtual Machine Wizard appears.



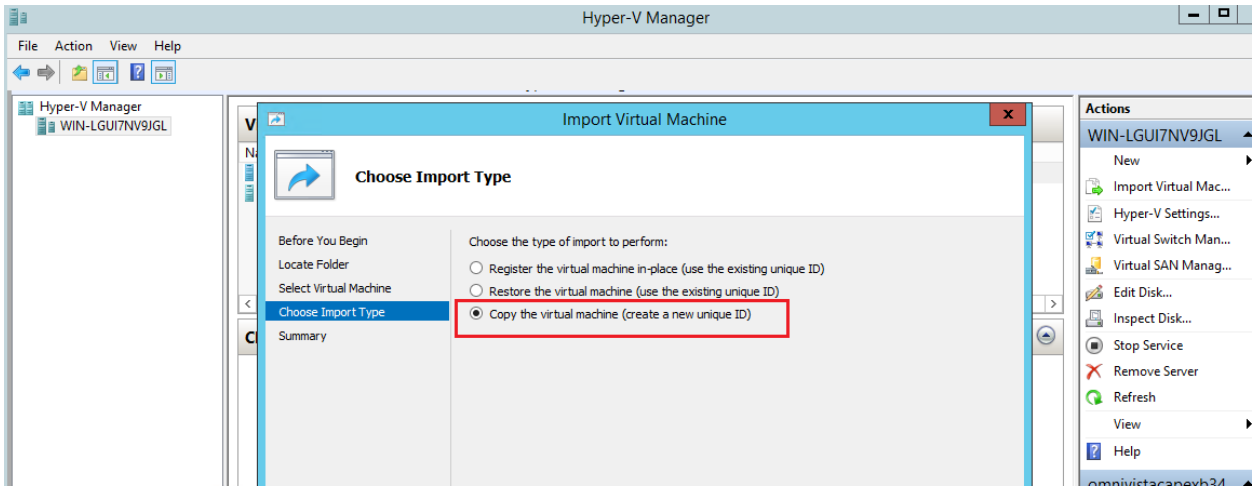
5. Click **Next** to go to the Locate Folder Screen, select the **Folder** that you extracted in Step 1, then click **Next**.



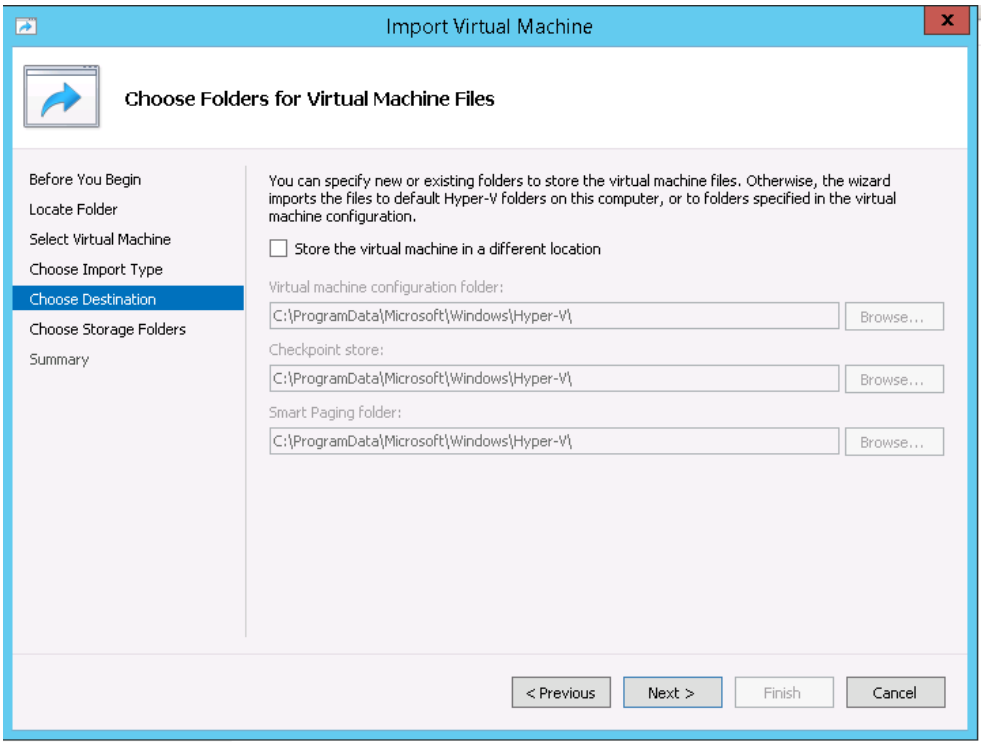
6. Select the Virtual Machine to import (Default = **OmniVista-2500 NMS-E-4.2.2.R01**), then click **Next**.



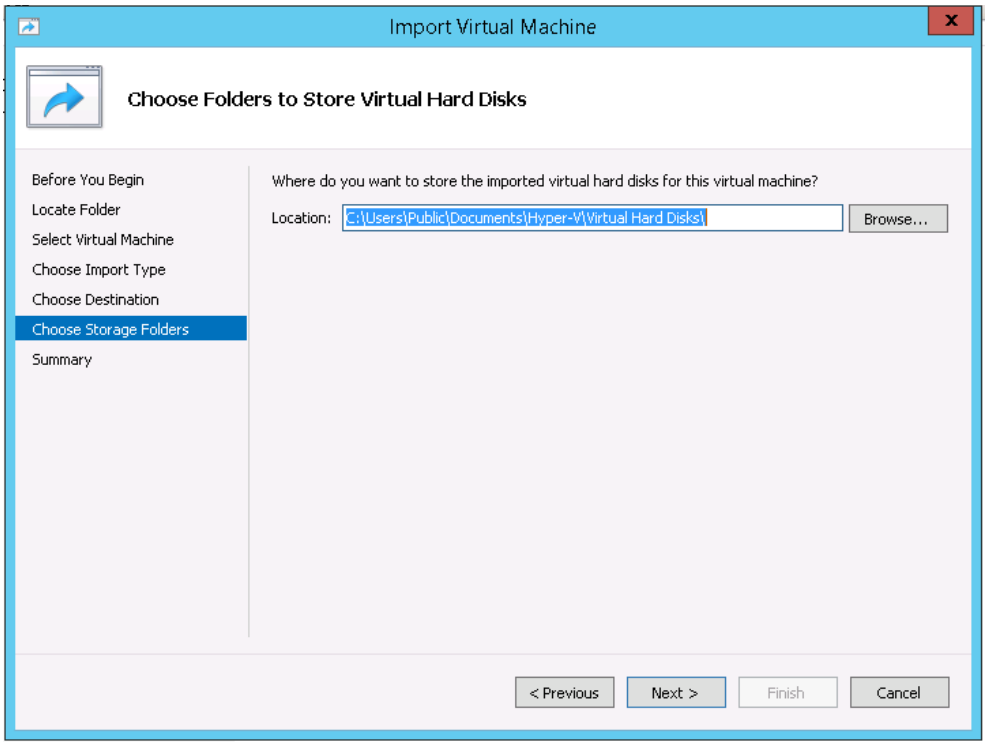
7. Select the default Import Type: **Copy the virtual machine (create a new unique ID)**, then click **Next**.



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

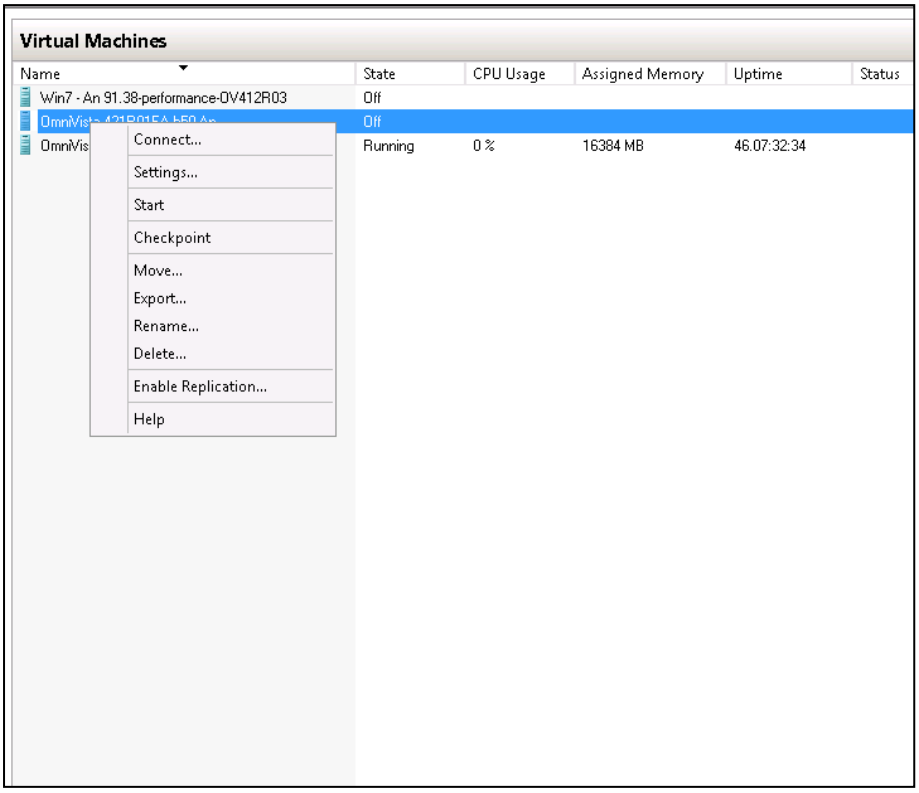


9. Choose folders to store the Virtual Hard Disks or accept the default location and click **Next**.

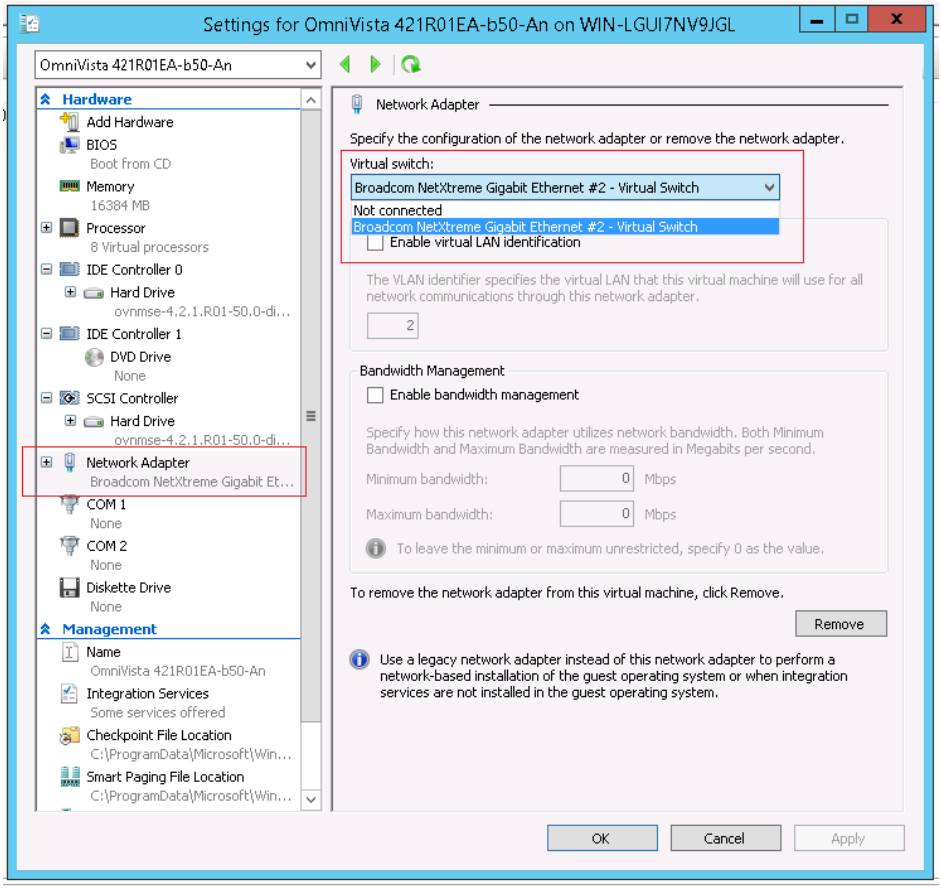


10. Review the import configuration and click **Finish**. (Click **Previous** to return to a screen and make changes.)

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 2500 NMS-E 4.3R1 Installation to complete the installation.

Remember, if you are installing a High-Availability configuration, 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** completing the OmniVista 2500 NMS-E 4.3R1 Installation.

Completing the OmniVista 2500 NMS-E 4.3R1 Installation

The sections below detail the final installation steps for a Standalone Installation and a High-Availability Installation.

Standalone Installation

Follow the steps in the following sections to complete the OV 2500 NMS-E 4.3R1 Standalone Installation.

1. Launch the Console for the new VM. The following screen will appear:

```
Regenerating ssh host keys...

Choose OV Deployment Model
[1] Standalone Mode
[2] Cluster Mode
(*) Type your option:
```

2. Enter **1** and press **Enter** to perform a Standalone installation.

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.

```
Configured Keyboard Layout: us
Would you like to configure new Keyboard Layout [y|n] (n): _
```

The password prompt appears.

```
*************************************************************************************************************
* Configure "cliadmin" password                                                                             *
*************************************************************************************************************
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 30 characters
Enter new password: _
```

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.

```
The OV IP address is not available, please configure it
Press [Enter] to continue
```

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

```
*************************************************************************************************************
* Configure OV IP                                                                                           *
*************************************************************************************************************
(*) Please input OV IPv4: 10.255.221.90
Please input subnet mask [255.255.255.0]:
Would you like to configure:
        IPv4: 10.255.221.90
        subnet mask: 255.255.255.0
[y|n] (y): y
The configuration has been set
Press [Enter] to continue
```

5. Enter an IPv4 address.

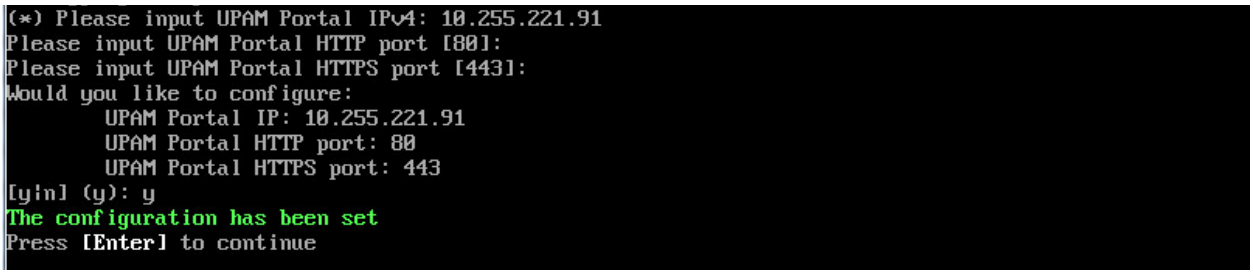
6. Enter the IPv4 network mask.

7. Press **Enter** at the confirmation prompt, then press **Enter** to continue. The UPAM Portal and IP Ports prompt appears.

```
Configure UPAM Portal IP & Ports
[1] Configure new IP & Ports
[2] Disable UPAM Portal
(*) Type your option:
```

8. Enter **1** and press **Enter** to configure the UPAM IP and Ports. If you are not managing a wireless network and will not be using UPAM, enter **2** and press **Enter**.

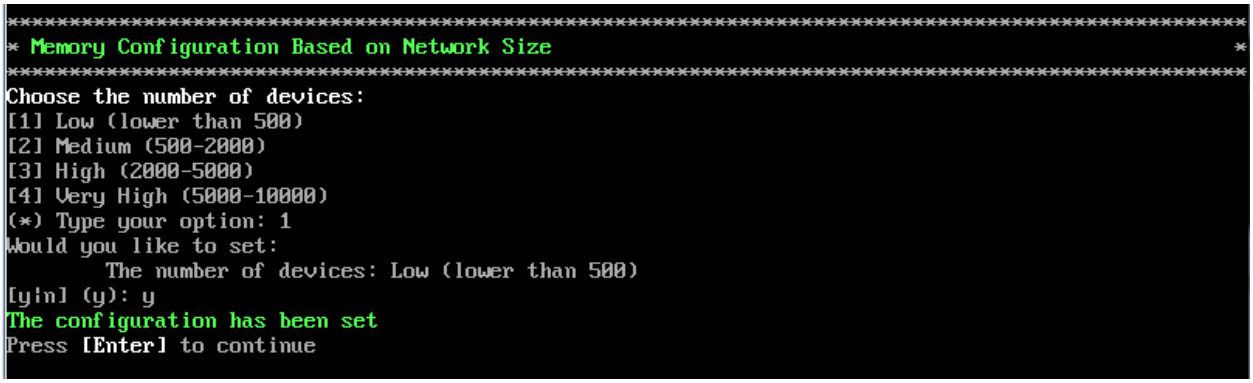
If you select **1** in this step, UPAM IP and Ports configuration must be completed (Steps 9 – 10). If you select **2**, go to Step 11.



9. Enter a UPAM IP address and UPAM HTTP and HTTPS ports. The UPAM IP address can be the same as the OV IP address or different. However, if you use a different IP address for UPAM it is recommended that you use the default ports. If you do not use the default ports, the ports should be >1024.

10. Press **Enter** at the confirmation prompt, then press **Enter** to continue.

11. The **Memory Configuration Based on Network Size** screen is displayed.



Select the number of devices OV 2500 NMS-E 4.3R1 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, 15,000 wireless clients)
- Medium (500 to 2,000 devices, 30,000 wireless clients)
- High (2,000 to 5,000 devices, 1,000,000 wireless clients)
- Very High (5,000 to 10,000 devices, 1,000,000 wireless clients).

Press **Enter**; then enter **y** and press **Enter** at the confirmation prompt. Press **Enter** to display the Configure the Virtual Appliance Menu.

Important Note: Make sure that your VA configuration (e.g., Hypervisor Processor, OV VA RAM, Data Partitioning) 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. For instance, if you allocate 16GB of memory for OV VA but configure the network size to be Medium (500 – 2,000 devices) instead of Low (fewer than 500 devices), OV may experience unexpected issues. Refer to Recommended System Configurations for details.

```
*************************************************************************************************
* Configure The Virtual Appliance                                                               *
*************************************************************************************************
* [1] Help                                                                                      *
* [2] Display Current Configuration                                                             *
* [3] Configure OV IP & OV Ports                                                                *
* [4] Configure UPAM Portal IP & Ports                                                          *
* [5] Configure Default Gateway                                                                 *
* [6] Configure Hostname                                                                        *
* [7] Configure DNS Server                                                                      *
* [8] Configure Timezone                                                                        *
* [9] Configure Route                                                                           *
* [10] Configure Network Size                                                                   *
* [11] Configure Keyboard Layout                                                                *
* [12] Configure NTP Client                                                                     *
* [13] Configure Proxy                                                                          *
* [14] Change screen resolution                                                                 *
* [15] Configure the other Network Cards                                                        *
* [0] Exit Configuration Menu And Continue                                                      *
*************************************************************************************************
(*) Type your option: _
```

12. Type **5** then press **Enter** to configure the Default Gateway.

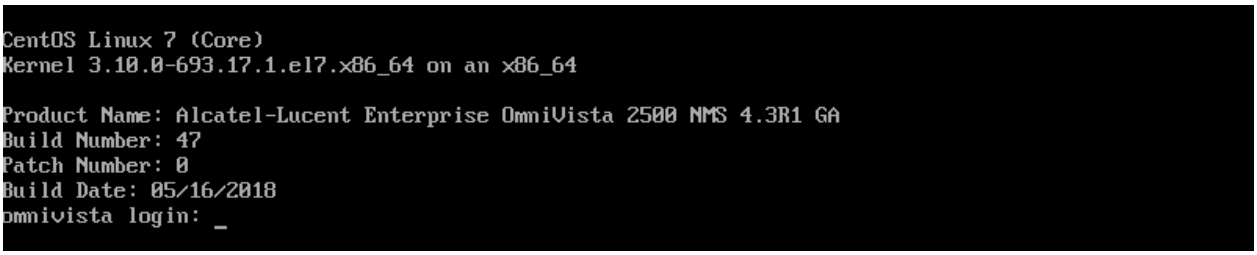
```
*************************************************************************************************
* Configure Default Gateway                                                                     *
*************************************************************************************************
(*) Please input defaut gateway v4: 10.255.221.254
Would you like to configure:
       default gateway: 10.255.221.254
[y|n] (y):
The configuration has been set
Press [Enter] to continue
```

13. Enter an IPv4 default gateway IP address.

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

```
*************************************************************************************************
* Configure The Virtual Appliance                                                               *
*************************************************************************************************
* [1] Help                                                                                      *
* [2] Display Current Configuration                                                             *
* [3] Configure OV IP & OV Ports                                                                *
* [4] Configure UPAM Portal IP & Ports                                                          *
* [5] Configure Default Gateway                                                                 *
* [6] Configure Hostname                                                                        *
* [7] Configure DNS Server                                                                      *
* [8] Configure Timezone                                                                        *
* [9] Configure Route                                                                           *
* [10] Configure Network Size                                                                   *
* [11] Configure Keyboard Layout                                                                *
* [12] Configure NTP Client                                                                     *
* [13] Configure Proxy                                                                          *
* [14] Change screen resolution                                                                 *
* [15] Configure the other Network Cards                                                        *
* [0] Exit Configuration Menu And Continue                                                      *
*************************************************************************************************
(*) Type your option: _
```

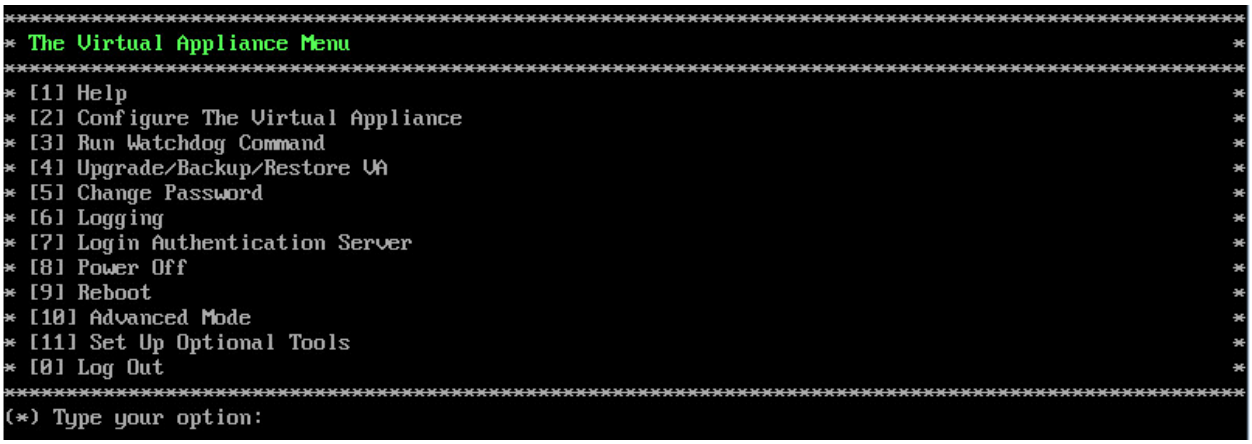
15. Type **0** and press **Enter** to exit the menu and complete the installation. OmniVista will reboot and display the current configuration. When the reboot is complete the OmniVista Login Screen will appear.



16. 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.



If necessary, you can configure additional settings (e.g., Proxy, DNS) that may be required to access OV 2500 NMS-E 4.3R1. For more information on configuring the VM, see Appendix B – Using the Virtual Appliance Menu.

> **Note:** OV 2500 NMS-E 4.3R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. 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 4.3R1 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

17. 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 **2** and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details.

18. Once all services are running, enter *https://<OVServerIPaddress>* in a supported browser to launch OV 2500 NMS-E 4.3R1.

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

19. 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**.

High-Availability Installation

A High-Availability 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.

Notes:

- The VMs (Node 1 and Node 2) must be on the same subnet.
- 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.
- As mentioned earlier, the High-Availability Feature is only supported on small networks ("Low" - up to 500 devices). There is no step in the installation process to configure the network size (as in the standalone installation). The network size is automatically configured for a "Low" sized network.

To configure the Cluster, you will need three (3) IP addresses:

- **Cluster IP Address –** This is a virtual IP address that is used to communicate with the network (and with the Active and Standby Nodes). It is the IP address you will enter in the browser to bring up OmniVista. Basically, it is the OmniVista Server IP address. You will use the same Cluster IP address when configuring each Node – the Active Node and The Standby Node.

- **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).

  Important Note: Make sure to plan the Cluster IP address, Node IP addresses and Host Names carefully and have them available for reference throughout the installation process for both VMs (Node 1 and Node 2).

Configuring a High-Availability Cluster consists of the following steps:

1. Configuring Node 1
2. Configuring Node 2
3. Initializing the Cluster

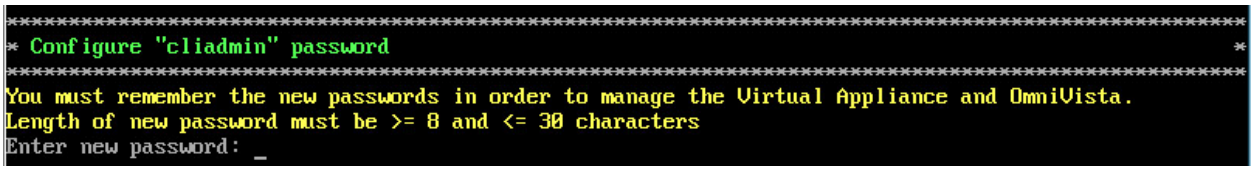
Configuring Node 1

1. Launch the Console for the Node 1 VM. The following screen will appear:

2. Enter **2** (Cluster Mode) and press **Enter** to perform a High-Availability installation.

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 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.

4. Enter the IP address, subnet and hostname (e.g., ov1) for Node 1. Press **Enter** at the Confirmation Prompt, then press **Enter** to continue.

Important Note: The hostname **must** be in lower case letters (e.g., “ov1” **not** “OV1”).

```
**********************************************************************************************************
* Configure OV IP and Hostname                                                                           *
**********************************************************************************************************
(*) Please input IPv4 address for eth0 interface: 10.255.221.92
Please input subnet mask [255.0.0.0]: 255.255.255.0
Please input hostname [omnivista]: ov1
Would you like to configure eth0 interface:
        IPv4 address: 10.255.221.92
        Subnet mask: 255.255.255.0
        Host name: ov1
[y|n] (y): _
```

The Peer Node IP address prompt appears.

```
**********************************************************************************************************
* Configure Peer Node's Information                                                                      *
**********************************************************************************************************
(*) Please input IP of Peer Node: _
```

5. Enter the IP address and hostname for the Peer Node (this is the hostname and IP address of Node 2), then press **Enter** at the Confirmation Prompt. 1

```
**********************************************************************************************************
* Configure Peer Node's Information                                                                      *
**********************************************************************************************************
(*) Please input IP of Peer Node: 10.255.221.93
(*) Please input Hostname of Peer Node: ov2
Would you like to to configure
        IP of Peer Node: 10.255.221.93
        Hostname of Peer Node: ov2
[y|n] (y):
```

The Cluster Name prompt appears.

```
**********************************************************************************************************
* Configure Cluster Name                                                                                 *
**********************************************************************************************************
(*) Please input Cluster Name: _
```

6. Enter a Cluster Name, then press **Enter** at the Confirmation Prompt.

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

The Cluster IP address prompt appears.

```
**********************************************************************************************************
* Configure OV Cluster IP                                                                                *
**********************************************************************************************************
(*) Please input OV Cluster IPv4 address: _
```

7. Enter a Cluster IP address and subnet, then press **Enter** at the Confirmation Prompt. Remember, you will configure the same Cluster IP address for both Nodes in the Cluster.

```
**********************************************************************************************************************
* Configure OV Cluster IP                                                                                            *
**********************************************************************************************************************
(*) Please input OV Cluster IPv4 address: 10.255.221.90
Please input subnet mask [255.0.0.0]: 255.255.255.0
Would you like to configure OV Cluster IP:
        IPv4 address: 10.255.221.90
        Subnet mask: 255.255.255.0
[y|n] (y):
```

The configuration will complete.

```
**********************************************************************************************************************
* Setting Up On This Node                                                                                            *
**********************************************************************************************************************
Initializing network to support Cluster...
Initializing OS to support Cluster...
Setting up OV services...
Preparing Sync-Data...
This could take some minutes to finish, please wait!
Cluster setting up is now completed.
Press [Enter] to continue
```

8. Press **Enter** to continue. The login prompt 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 4.3R1 GA
Build Number: 47
Patch Number: 0
Build Date: 05/16/2018
omnivista login:
```

9. Log into the VM.

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

After successful login, the HA Virtual Appliance Menu appears.

```
**********************************************************************************************************************
* The HA Virtual Appliance Menu                                                                                      *
**********************************************************************************************************************
* [1] Help                                                                                                           *
* [2] Initialize OV Cluster                                                                                          *
* [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: _
```

The Node is configured, but you must still configure the Default Gateway.

10. Enter **4** (Configure the Current Node) and press **Enter**. The Configure Current Node Menu appears.

```
**********************************************************************************************************
* Configure Current Node                                                                                 *
**********************************************************************************************************
* [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] Configure Mongodb Password                                                                        *
* [14] Configure IP & Hostname                                                                           *
* [15] Extend Data Partitions                                                                            *
* [0] Exit                                                                                               *
**********************************************************************************************************
(*) Type your option: _
```

11. Type **3** (Configure Default Gateway) and press **Enter**. The Configure Default Gateway prompt appears.

```
**********************************************************************************************************
* Configure Default Gateway                                                                              *
**********************************************************************************************************
(*) Please input defaut gateway v4:
```

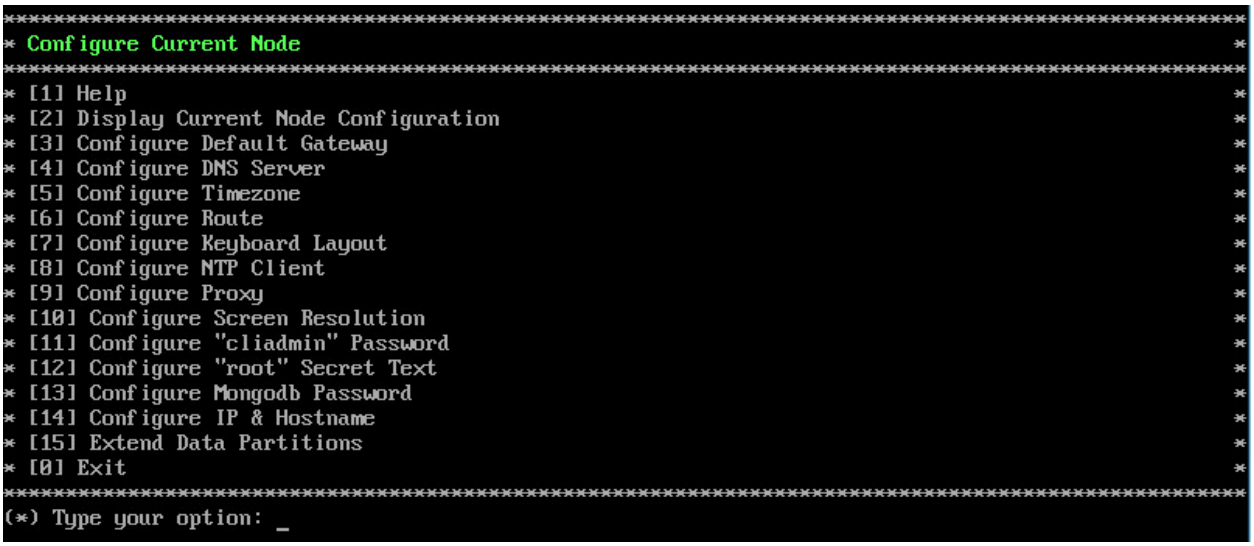
12. Enter an IPv4 Default Gateway. Press **Enter** at the Confirmation Prompt, then press **Enter** again to continue.

```
**********************************************************************************************************
* Configure Default Gateway                                                                              *
**********************************************************************************************************
(*) Please input defaut gateway v4: 10.255.221.254
Would you like to configure:
       default gateway: 10.255.221.254
[y|n] (y): _
```

The following warning prompt will appear.

```
Some services must be restarted for the change to take effect
Would you like to restart services now [y|n] (y):
```

13. Press **Enter** to restart services and complete the Default Gateway configuration. The services will restart and the Configure Current Node Menu will appear.



14. The configuration of Node 1 is complete. Configure Node 2 as described below.

Important Note: After configuring **both** nodes you must initialize the Cluster as detailed below.

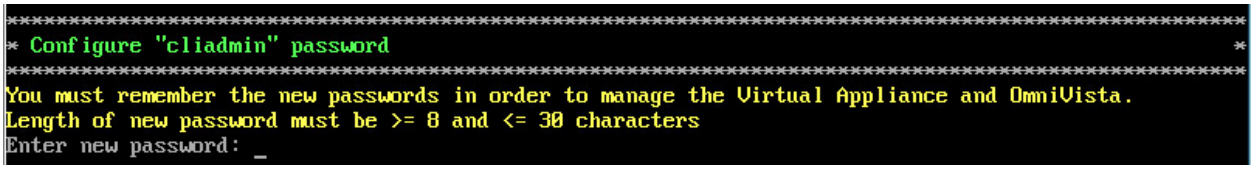
Configuring Node 2

1. Launch the Console for the Node 2 VM. The following screen will appear:

2. Enter **2** (Cluster Mode) and press **Enter** to perform a High-Availability installation.

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 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.

```
******************************************************************************************************************
* Configure OV IP and Hostname                                                                                   *
******************************************************************************************************************
(*) Please input IPv4 address for eth0 interface: _
```

4. Enter the IP address, subnet and hostname (e.g., ov2) for Node 2. Press **Enter** at the Confirmation Prompt, then press **Enter** to continue.

Important Note: The hostname **must** be in lower case letters (e.g., “ov2” **not** “OV2”).

```
******************************************************************************************************************
* Configure OV IP and Hostname                                                                                   *
******************************************************************************************************************
(*) Please input IPv4 address for eth0 interface: 10.255.221.93
Please input subnet mask [255.0.0.0]: 255.255.255.0
Please input hostname [omnivista]: ov2
Would you like to configure eth0 interface:
        IPv4 address: 10.255.221.93
        Subnet mask: 255.255.255.0
        Host name: ov2
[y|n] (y): _
```

The Peer Node IP address prompt appears.

```
******************************************************************************************************************
* Configure Peer Node's Information                                                                              *
******************************************************************************************************************
(*) Please input IP of Peer Node: _
```

5. Enter the IP address and hostname for the Peer Node (this is the Host Name and IP address of Node 1), then press **Enter** at the Confirmation Prompt.

```
******************************************************************************************************************
* Configure Peer Node's Information                                                                              *
******************************************************************************************************************
(*) Please input IP of Peer Node: 10.255.221.92
(*) Please input Hostname of Peer Node: ov1
Would you like to to configure
        IP of Peer Node: 10.255.221.92
        Hostname of Peer Node: ov1
[y|n] (y): _
```

The Cluster Name prompt appears.

```
******************************************************************************************************************
* Configure Cluster Name                                                                                         *
******************************************************************************************************************
(*) Please input Cluster Name: _
```

6. Enter the Cluster Name you entered when configuring Node 1 (e.g., ovcluster), then press **Enter** at the Confirmation Prompt.

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

The Cluster IP address prompt appears.

```
********************************************************************************
* Configure OV Cluster IP                                                      *
********************************************************************************
(*) Please input OV Cluster IPv4 address: _
```

7. Enter the **same Cluster IP address and subnet that you entered for Node 1**, then press **Enter** at the Confirmation Prompt.

```
********************************************************************************
* Configure OV Cluster IP                                                      *
********************************************************************************
(*) Please input OV Cluster IPv4 address: 10.255.221.90
Please input subnet mask [255.0.0.0]: 255.255.255.0
Would you like to configure OV Cluster IP:
        IPv4 address: 10.255.221.90
        Subnet mask: 255.255.255.0
[y|n] (y):
```

The configuration will complete.

```
********************************************************************************
* Setting Up On This Mode                                                      *
********************************************************************************
Initializing network to support Cluster...
Initializing OS to support Cluster...
Setting up OV services...
Preparing Sync-Data...
This could take some minutes to finish, please wait!
Cluster setting up is now completed.
Press [Enter] to continue
```

8. Press **Enter** to continue. The login prompt 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 4.3R1 GA
Build Number: 47
Patch Number: 0
Build Date: 05/16/2018
omnivista login:
```

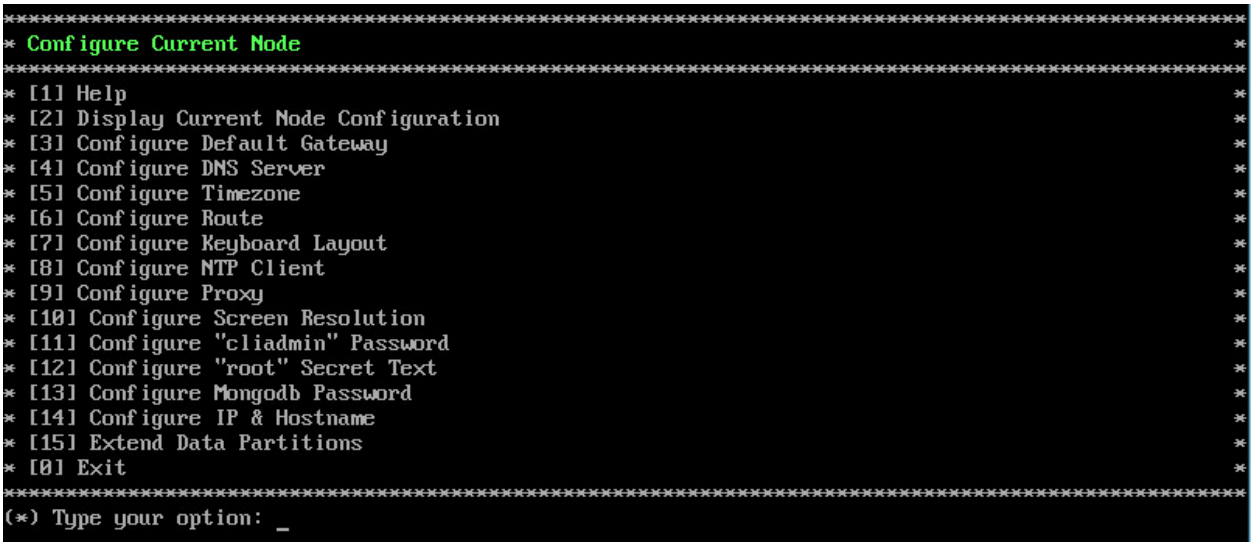
9. Log into the VM.

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

After successful login, the HA Virtual Appliance Menu appears.

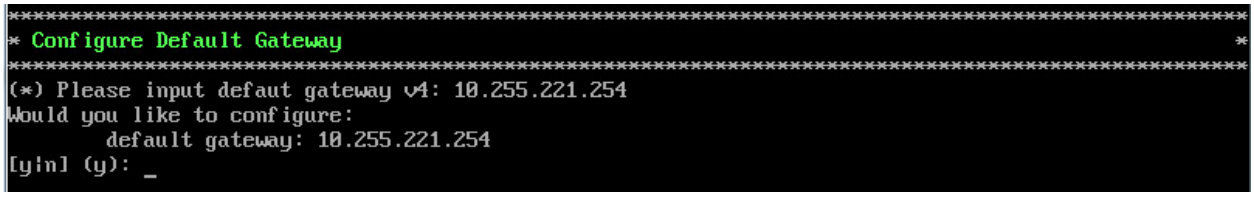
The Node is configured, but you must still configure the Default Gateway.

10. Enter **4** (Configure the Current Node) and press **Enter**. The Configure Current Node Menu appears.



11. Enter **3** (Configure Default Gateway) and press **Enter**. The Configure Default Gateway prompt appears.

12. Enter an IPv4 Default Gateway. Press **Enter** at the Confirmation Prompt, then press **Enter** again to continue.



The following warning prompt will appear.

```
Some services must be restarted for the change to take effect
Would you like to restart services now [y|n] (y):
```

13. Press **Enter** to restart services and complete the Default Gateway configuration. The services will restart and the Configure Current Node Menu will appear.

```
*****************************************************************************************************
* Configure Current Node                                                                            *
*****************************************************************************************************
* [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] Configure Mongodb Password                                                                   *
* [14] Configure IP & Hostname                                                                      *
* [15] Extend Data Partitions                                                                       *
* [0] Exit                                                                                          *
*****************************************************************************************************
(*) Type your option: _
```

14. The configuration of Node 2 is complete. To complete the installation, Initialize the Cluster as detailed below.

Initializing the Cluster

After configuring both nodes, follow the steps below to initialize the Cluster. This will complete the installation process and sync Nodes 1 and 2. It may take up to an hour to complete. **This must be done on Node 1 only**, not both Nodes.

1. Log into **Node 1**. The HA Virtual Appliance Menu will appear.

```
*****************************************************************************************************
* The HA Virtual Appliance Menu                                                                     *
*****************************************************************************************************
* [1] Help                                                                                          *
* [2] Initialize OV Cluster                                                                         *
* [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. Enter **2** (Initialize OV Cluster) and press **Enter**. The following prompt will appear.

```
Please ensure following before continuing:
        Both VAs are up
        Both VAs can access/ping each other via OV IPs
        Both VAs can access/ping each other via hostnames
Would you like to initialize OV Cluster now [y|n] (n):
```

3. Enter **y** and press **Enter.** Press **Enter** at the next two prompts (n) to initialize the Cluster.

```
Would you like to re-configure Cluster IP [y|n] (n):

Would you like to re-configure Peer Node's Information [y|n] (n): _
```

The initialization will begin and start synchronizing data between the two nodes.

```
*************************************************************************************************************
* Initialize OV Cluster (HA)                                                                                *
*************************************************************************************************************
Doing some beginning steps...
Creating Cluster IP...
Syncing Sync-Data...
This could take a long time (between 30 mins and 1 hour) to finish, please wait!
_
```

```
Initializing PostgreSQL service...
Initializing InfluxDB service...
Initializing Grafana service...
Initializing Telegraf service...
Doing some final steps...
Cluster initialization is now completed. Please wait until all OV processes are started, before atte
mpting to launch OV from web browser.
Press [Enter] to continue
```

Once initialization is complete ("Cluster initialization is now completed."), press **Enter** to continue. 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:
```

4. Perform the following verification steps:

- Verify that all services are running on Node 1:
  - Go to the Virtual Appliance Menu of Node 1.
    - Enter **5** (Run Watchdog Command) then press **Enter**. Enter and press **Enter** to display the status of OmniVista Services. See Run Watchdog Command for more details.
- Check the Cluster status on Node 1.
  - Go to the Virtual Appliance Menu of Node 1.
    - Enter **2** (Show OV Cluster Status) the press **Enter**. See Show OV Cluster Status for more information.

Note: You can also use the Run Watchdog Command on Node 2 to check the services status. Note that on Node 2, all services should be Running except ovnginx. It is the expected behavior on Standby Node that ovnginx service will be "Stopped".

5. Once all services are running, enter *https://<ClusterIPaddress>* in a supported browser to launch OV 2500 NMS-E 4.3R1.

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

6. The first time you launch OmniVista you will be prompted to activate the OmniVista License and the High-Availability License. Import the license file (.dat) or enter the license key to activate the licenses. 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 OV 2500 NMS-E 4.2.2.R01 (MR2)

Follow the steps below to use the Upgrade option in the Virtual Appliance Menu to upgrade from OV 2500 NMS-E 4.2.2.R01 MR2 to OV 2500 NMS-E 4.3R1. Remember, if you are upgrading from an older version (3.5.7 or 4.2.2.R01 (MR1)), you must first upgrade to 4.2.2.R01 (MR2) before upgrading to 4.3R1.

Remember, you can only upgrade to a standalone installation. The High-Availability Feature requires a fresh installation of OV 2500 NMS-E 4.3R1.

Important Notes: Before beginning the upgrade:

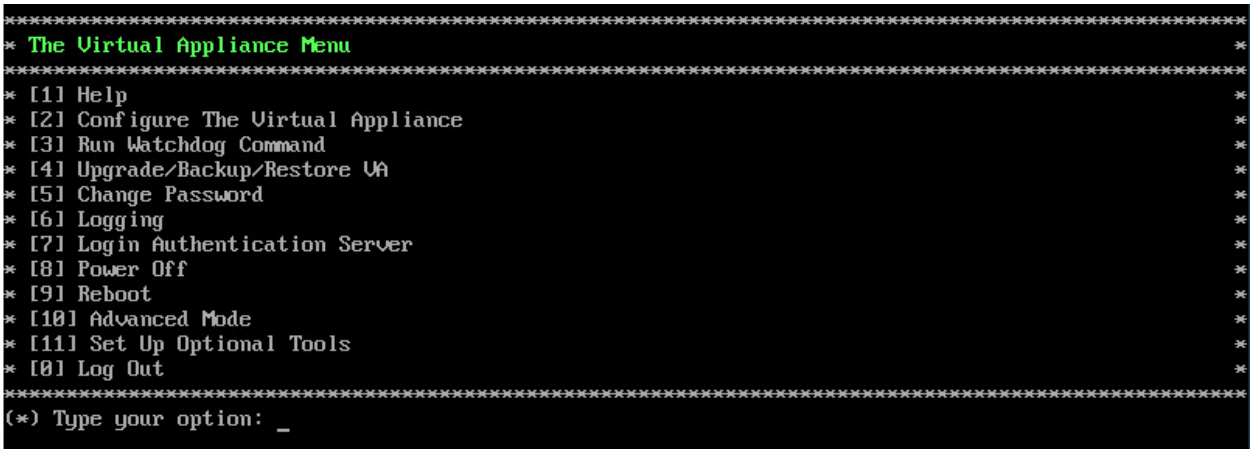
- Take a VM Snapshot of the OmniVista VA.
- Move old OmniVista and switch backup files to external storage. (SFTP to OmniVista using port 22 and "cliadmin" login to access the files.)
- Purge very old backup files by configuring the Backup Retention Policy (Configuration - Resource Manager Settings).
- Ensure that there is enough free disk space for OmniVista. If necessary, move VM Snapshots to free up space.
- 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 4.3R1 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 **14 - Configure Proxy**.

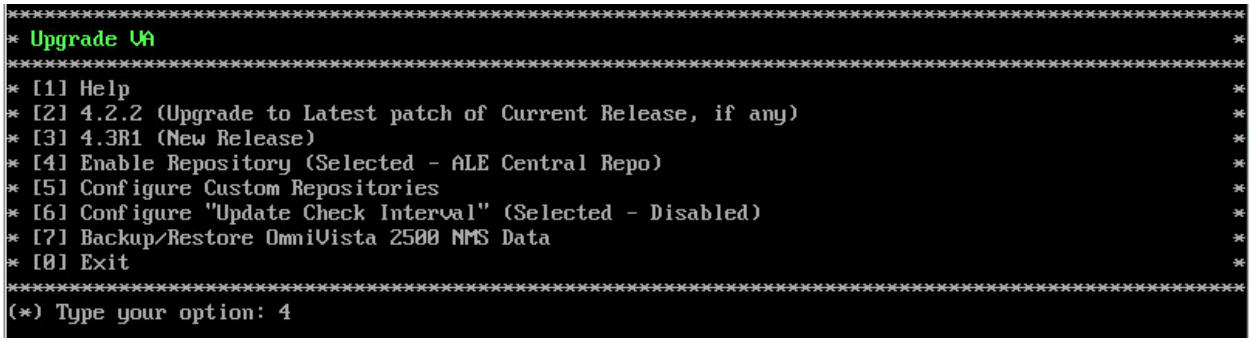
It is recommended that you perform the upgrade directly from the VM Console. The upgrade can take anywhere from 30 minutes to 4 hours depending on network speed, network size, and

database size. 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.

1. Open a Console on your existing Virtual Appliance (OV 2500 NMS-E 4.2.2.R01 MR2).



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



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

Note: You may skip creating Custom Repository and use the default “ALE Central Repo” if you are **sure** that your OV 422 MR 2 installation was installed as a **fresh installation** and not upgraded from a previous OmniVista release. If so, go to Step 10. If in doubt, you should create a new Custom Repository.

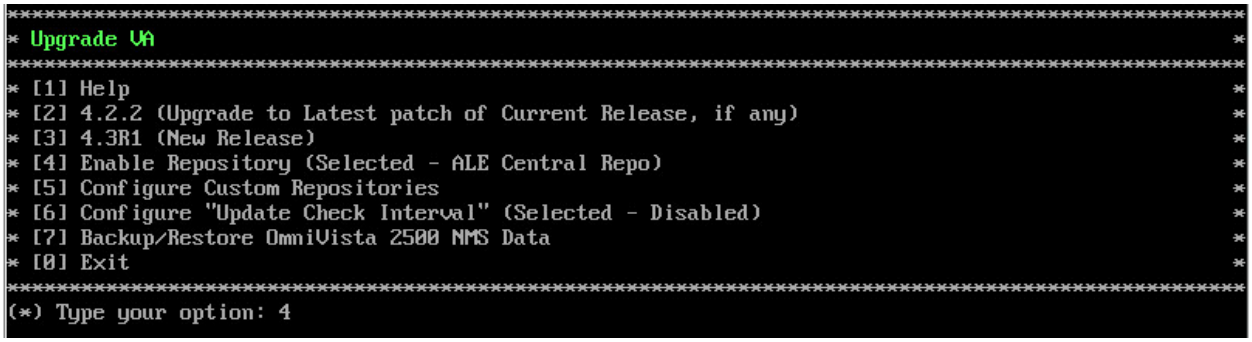
4. Select a Custom Repository (e.g., **2** – “Custom Repo 1” Repository) and press **Enter**.

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”).

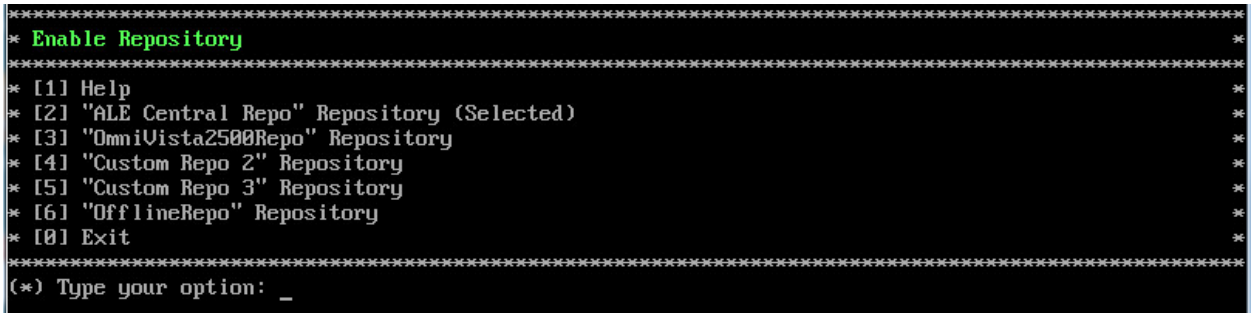
5. Configure the repository as described below, then Enter **y** and press **Enter** to confirm the configuration.

- Repository Name – OmniVista2500Repo
- Repository URL Host – ovrepo.fluentnetworking.com
- Repository URL Location – ov

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



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



8. Select the Custom Repository you just created (e.g., **3** – "OmniVista2500Repo" 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.

```
*************************************************************************************************************
* Enable Repository                                                                                         *
*************************************************************************************************************
* [1] Help                                                                                                  *
* [2] "ALE Central Repo" Repository                                                                         *
* [3] "OmniVista2500Repo" Repository (Selected)                                                             *
* [4] "Custom Repo 2" Repository                                                                            *
* [5] "Custom Repo 3" Repository                                                                            *
* [6] "OfflineRepo" Repository                                                                              *
* [0] Exit                                                                                                  *
*************************************************************************************************************
(*) Type your option: _
```

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

```
*************************************************************************************************************
* 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 - OmniVista2500Repo)                                                      *
* [5] Configure Custom Repositories                                                                         *
* [6] Configure "Update Check Interval" (Selected - Disabled)                                               *
* [7] Backup/Restore OmniVista 2500 NMS Data                                                                *
* [0] Exit                                                                                                  *
*************************************************************************************************************
(*) Type your option:
```

10. Enter **3 - 4.3R1 (New Release)** and press **Enter** to bring up the Upgrade Systems 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** 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 to upgrade to OV 4.3R1.

```
Getting upgrade information for 4.3R1...
Upgrade information for 4.3R1
Available Packages
Name        : ovnmse
Arch        : x86_64
Version     : 4.3R1
Release     : 51.0.el7
Size        : 1.0 G
Repo        : CustomRepo1_4.3R1
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 4.3R1 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):
```

Note: If a new version (patch) of OV 4.2.2 (MR2) is available, you will be prompted to install the latest version before upgrading to OV 4.3R1. Enter **y** and press **Enter** at the Confirmation Prompt to install the latest version. When that installation is complete, enter **y** and press **Enter** at the Confirmation Prompt to upgrade to 4.3R1.

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 **2 – Display Status of All Services**. See Run Watchdog Command for more details.

14. Once all services are running, enter *https://<OVServerIPaddress>* in a supported browser to launch OV 2500 NMS-E 4.3R1. 2

Important Notes for Stellar APs:

- If your network includes Stellar APs, you must upgrade these devices to AWOS 3.0.3.x **after** completing 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.
- Also note that 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 VA Main Menu. Select **2 - Configure the Virtual Appliance.**

  2. Select **2 - Display Current Configuration** to verify your currently-configured network size (e.g., Low, Medium, High).

  3. Select **10 - Configure Network Size**, then select **2 - Configure OV2500 Memory**.

  4. Select your current memory configuration (e.g., 1 - Low). Press **y** at the confirmation prompt, then press **Enter** to continue.

  5. At the Watchdog Service prompt, press **y**, then press **Enter** to restart Watchdog Services.

Appendix A – Installing Virtual Box

If you are deploying OV 2500 NMS-E 4.3R1 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
```

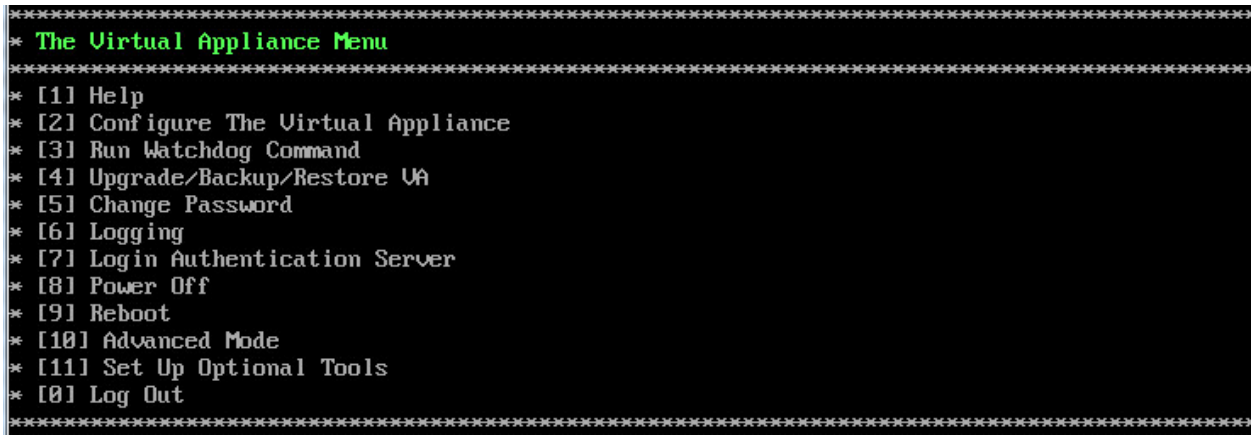
Appendix B – Using the Virtual Appliance Menu

To access the Main Virtual Appliance Menu for a VM, launch the Console. (In vCenter, this can be done by right-clicking on the VM in the Navigation Tree and selecting **Open 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

- 0 - Log Out

For information on these menu options, refer to the sections below.

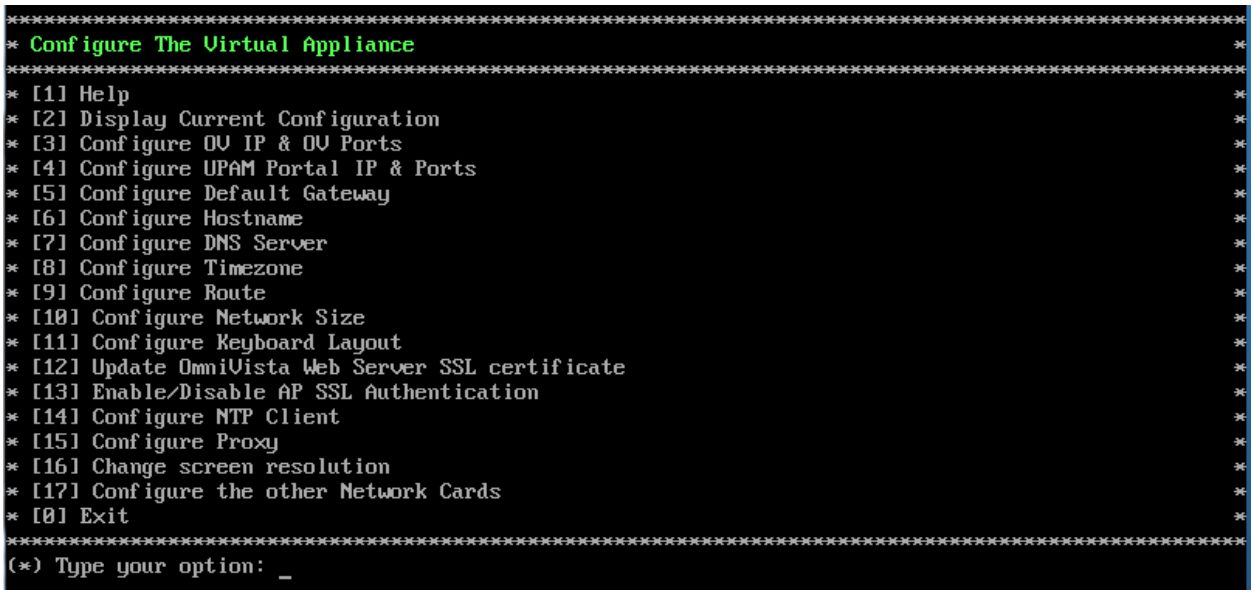
Help

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 OV IP & OV Ports
- 4 - Configure UPAM Portal IP & Ports
- 5 - Configure Default Gateway
- 6 - Configure Hostname
- 7 - Configure DNS Server
- 8 - Configure Timezone
- 9 - Configure Route
- 10 - Configure Network Size
- 11 - Configure Keyboard Layout
- 12 – Update OmniVista Web Server SSL Certificate
- 13 - Enable/Disable AP SSL Authentication
- 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.

```
**********************************************************************************************************
* Current configuration                                                                                  *
**********************************************************************************************************
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.3R1 GA
Build Number: 49
Patch Number: 0
Build Date: 05/25/2018
WMA Version: 3.0.12.28
UPAM Version: 3.0.30.43

OV IPv4 Address: 10.255.221.70
NetMask: 255.255.255.0
OV Web HTTP Port: 80
OV Web HTTPS Port: 443

UPAM Portal IPv4 Address: 10.255.221.71
UPAM Portal Web HTTP Port: 80
UPAM Portal Web HTTPS Port: 443

Default Gateway v4: 10.255.221.254

Hostname: omnivista

DNS Server 1: 10.255.120.121

Timezone: America/Los_Angeles

lvdata LVM Size: 255G
lvdata LVM Available (Free) Space: 255G

Network Size: Low (lower than 500) devices
```

Configure OV IP & OV Ports

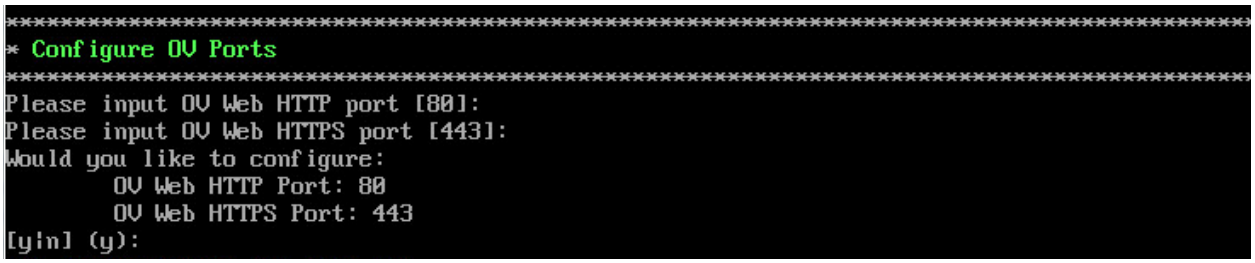
1. If you want to re-configure the OV IP address and Ports, enter **3** and press **Enter**.

```
**********************************************************************************************************
* Configure OV IP
**********************************************************************************************************
Please input OV IPv4 [10.255.221.19]:
Please input subnet mask [255.255.255.0]:
Would you like to configure:
        IPv4: 10.255.221.19
        subnet mask: 255.255.255.0
[y|n] (y):
```

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. Press **Enter** to return to the Configure The Virtual Appliance Menu.

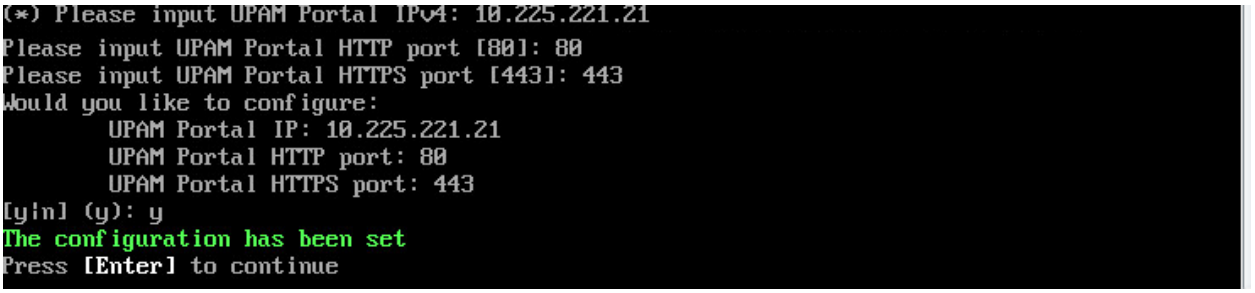
After entering values and confirming, you must restart all services for the changes to take effect. Use the **Restart All Services** option in the **Run Watchdog** command in the Virtual Appliance Menu.

> **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.

Configure UPAM Portal IP & Ports

1. Enter **4** and press **Enter** to bring up the Configure UPAM Portal IP & Ports Menu.

2. Enter **1** and press **Enter** to configure the IP address and Ports.



3. Enter a UPAM IP address and UPAM HTTP and HTTPS ports. The UPAM IP address can be the same as the OV IP address or different. However, if you use a different IP address for

UPAM it is recommended that you use the default ports. If you do not use the default ports, the ports should be >1024.

4. Enter **y** at the confirmation prompt and press **Enter** to confirm the settings.

5. At the prompt, enter an HTTP value and press **Enter**. Enter an HTTPS value and press **Enter**.

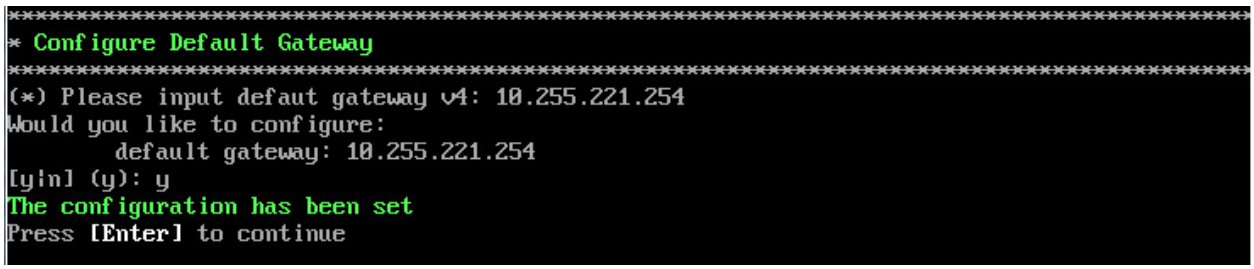
- HTTP Port (Valid range: 1024 to 65535, Default = 80)
- HTTPS Port (Valid range: 1024 to 65535, Default = 443)

6. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the Watchdog Service for the change to take effect.

7. Once Watchdog has restarted, enter **0** and press Enter to return to the Configure the Virtual Appliance Menu.

Configure Default Gateway

1. Enter **5** 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 **6** and press **Enter**.

2. Enter a hostname.

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 **7** 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.

```
******************************************************************************
* Configure DNS Server
******************************************************************************
Would you like to use dns servers [y|n] (n): y
(*) Please input dns server 1: 192.168.70.226
Would you like to use dns server 2 [y|n] (n): y
(*) Please input dns server 2: 192.168.1.3
Would you like to configure:
        dns server 1: 192.168.70.226
        dns server 2: 192.168.1.3
[y|n] (y): y
The configuration has been set
Press [Enter] to continue
```

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 **8** and press **Enter** to begin setting up the time zone; then confirm by typing **y** at the prompt.

2. Select the region for the VM by entering its corresponding numeric value (e.g., **10**).

```
******************************************************************************
* Configure Timezone
******************************************************************************
Would you like to configure Timezone of system [y|n] (n): y
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa           4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas         5) Asia             8) Europe
3) Antarctica       6) Atlantic Ocean   9) Indian Ocean
#?
```

3. Select a country within the region by entering its corresponding numeric value (e.g., **25**).

```
Please select a country.
 1) Chile                       15) Northern Mariana Islands
 2) Cook Islands                16) Palau
 3) Ecuador                     17) Papua New Guinea
 4) Fiji                        18) Pitcairn
 5) French Polynesia            19) Samoa (American)
 6) Guam                        20) Samoa (western)
 7) Kiribati                    21) Solomon Islands
 8) Marshall Islands            22) Tokelau
 9) Micronesia                  23) Tonga
10) Nauru                       24) Tuvalu
11) New Caledonia               25) United States
12) New Zealand                 26) US minor outlying islands
13) Niue                        27) Vanuatu
14) Norfolk Island              28) Wallis & Futuna
#?
```

4. If prompted, enter the numeric value for the specific time zone within the country (e.g., **21**).

```
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#?
```

5. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Route

1. If you want to add a static route from the VM to another network enter **9** 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 **10** and press **Enter** to begin configuring a Network Size.

2. You can re-configure OV 2500 NMS-E 4.3R1 memory settings by selecting option **2**. Select an option (e.g., Low, Medium, 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.

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 4.3R1 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, Data Partitioning) 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 OmniVista instability. For instance, if you allocate 16GB of memory for OV VA but configure the network size to be Medium (500 – 2,000 devices) instead of Low (fewer than 500 devices), OmniVista may experience unexpected issues. Refer to Recommended System Configurations for details.

Configure Keyboard Layout

1. Enter **11** 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**.

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 **12** 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 **13** 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 NTP Client

1. Enter **14** 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

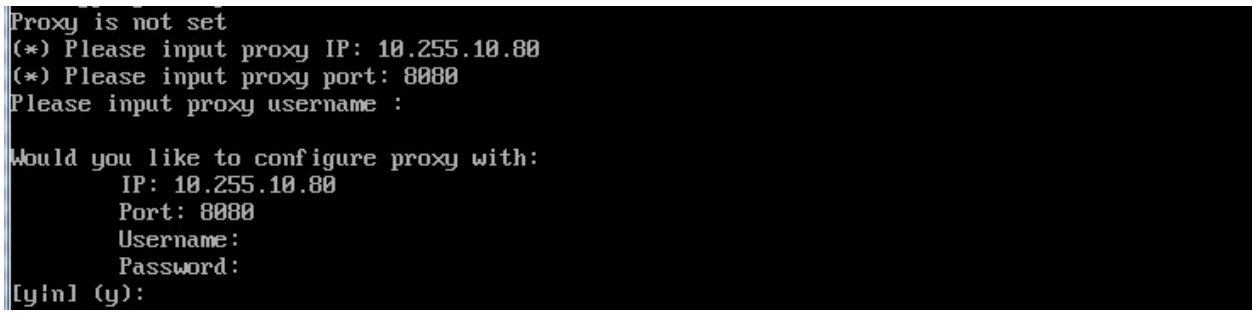
OV 2500 NMS-E 4.3R1 makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. If the OV 2500 NMS-E 4.3R1 Server has a direct connection to the Internet, a

Proxy is not required. Otherwise, a Proxy should be configured to enable OV 2500 NMS-E 4.3R1 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

1. Enter **15** 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 **16** 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 **17** and press **Enter** to configure additional Network Cards on the Virtual Appliance.

```
**********************************************************************************************
* Configure the other Network Cards
**********************************************************************************************
Choose the number of network card to configure:
[1] eth1
[0] Exit
(*) Type your option: 1
(*) Please input IPv4 for eth1: 10.1.10.214
Please input subnet mask [255.0.0.0]: 255.255.255.0
Would you like to configure:
        IPv4: 10.1.10.214
        subnet mask: 255.255.255.0
[y|n] (y): y
The configuration has been set
Press [Enter] to continue
```

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 4.3R1. 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 **3** at the command prompt. The following displays:

```
**********************************************************************************************
* Run Watchdog Command
**********************************************************************************************
* [1] Help
* [2] Display Status Of All Services
* [3] Start All Services
* [4] Stop All Services
* [5] Restart All Services
* [6] Start a Service
* [7] Stop a Service
* [8] Start Watchdog
* [9] Shutdown Watchdog
* [0] Exit
**********************************************************************************************
```

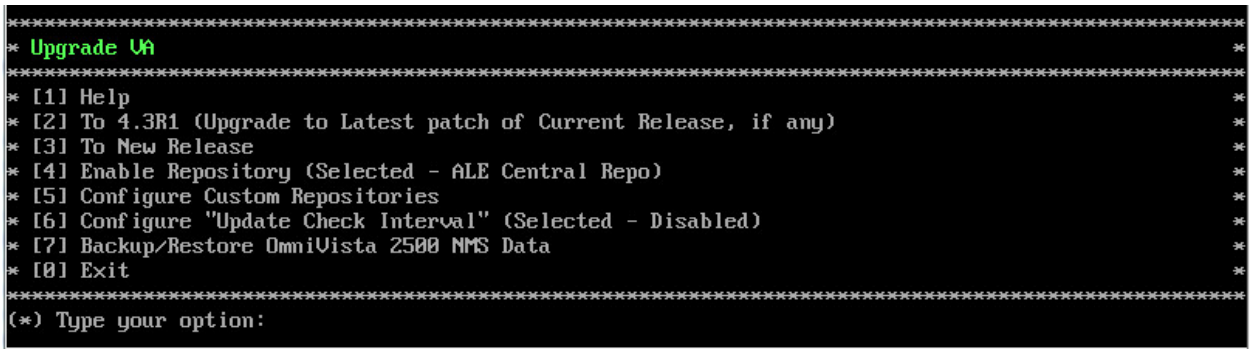
The following options are available:

- **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.

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.



The following options are available:

- **To 4.3R1 (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 Update -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available.
- **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 4.3R1 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 Host -** The IP address of the custom repository (e.g., 192.168.70.10).
  - **Repository URL Location -** The directory location of the upgrade software (e.g., repo/centos)
  - **Repository Full URL -** Is automatically completed by OV after confirming the configuration.

  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 (/opt/OmniVista_2500_NMS/data/file_server/cliadmin/backups) 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.
  - **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 4.3R1 configuration using a 4.3R1 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 4.3R1 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.

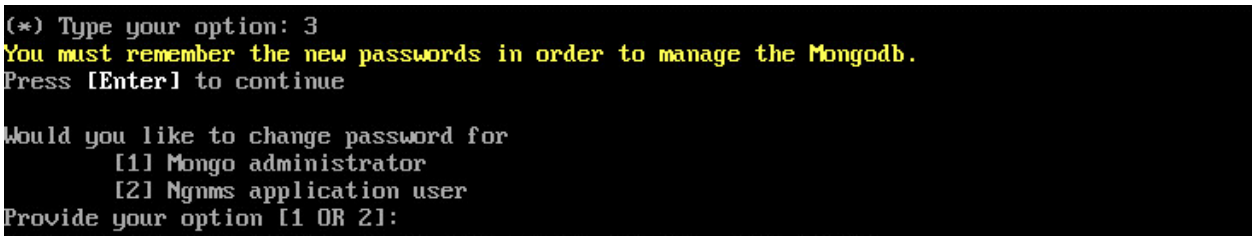
- **View Backup Configurations -** View the backup retention policies. The policies are configured using Option 2 – Configure Backup Retention Policy. Note that if you have not configured a Backup Retention Policy, the "Maximum Backup Retention Days" and Maximum Backup Retention Files" fields will show "-1".

Change Password

You can change the Virtual Appliance cliadmin password and/or mongo database password.

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.



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 password of the "root" user of the VA 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

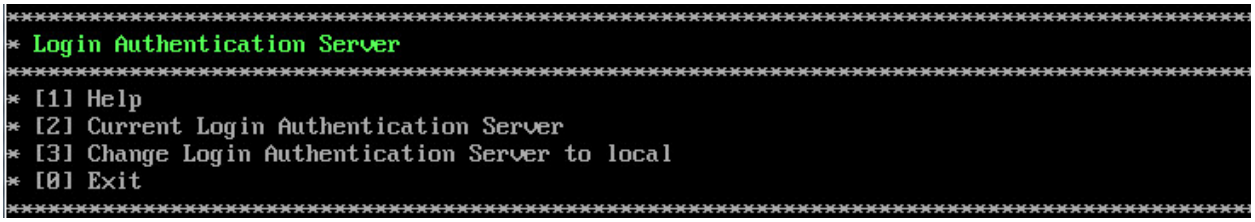
You can view OV 2500 NMS-E 4.3R1 Logs using the "Logging" option. Enter **6**, then press **Enter**.

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-02018-10-15-12-08-43.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 4.3R1 Login Authentication Server.



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 OV 2500 NMS-E 4.2.2.R01services 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 4.3R1 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 OV 2500 NMS-E 4.3R1 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 4.3R1 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 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.

Log Out

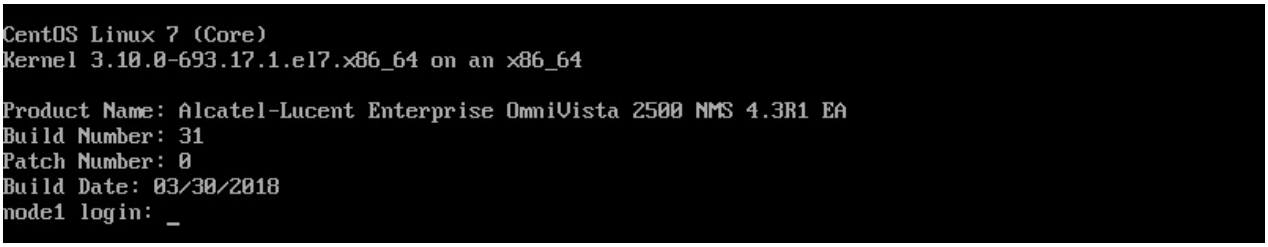
To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OV 2500 NMS-E 4.3R1 functions continue following logout.

Appendix C – Using the HA Virtual Appliance Menu

To access the High-Availability (HA) Virtual Appliance Menu for a VM, launch the Console. The login prompt is displayed.

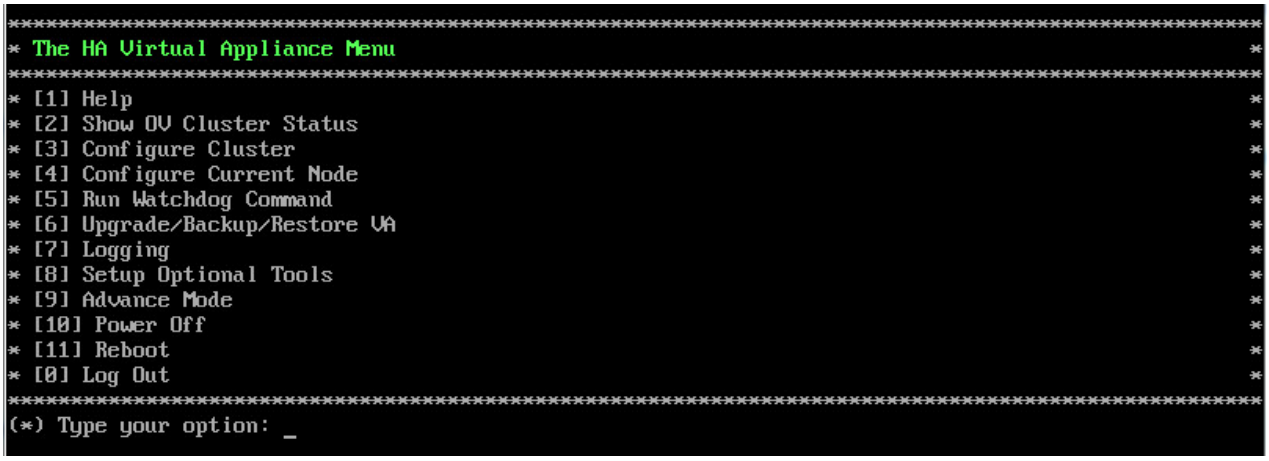
> **Note:** You can also access the Virtual Appliance Menu by connecting via SSH using port 2222, user **cliadmin,** and password set when deploying VA (e.g., ssh cliadmin@192.160.70.230 –p 2222).

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.



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 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       10.255.221.92  Active  Online
Peer     ov2       10.255.221.93          Online
Data sync: Up to Date
```

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 OV Ports                                                                        *
* [5] Configure UPAM Portal Ports                                                               *
* [6] Configure OV SSL Certificate                                                              *
* [7] Enable/Disable AP SSL Authentication                                                      *
* [8] Configure FTP Password                                                                    *
* [9] Configure Login Authentication Server                                                     *
* [10] Preferred Active Node                                                                    *
* [11] Manual Failover                                                                          *
* [12] Cluster Error Check                                                                      *
* [13] Configure Peer Node's Information                                                        *
* [14] Enable Maintenance Mode                                                                  *
* [0] Exit                                                                                      *
*************************************************************************************************
(*) Type your option: _
```

The following options are available:

1 - Help

2 - Display Cluster Configuration

3 – Configure Cluster IP

4 - Configure OV Ports

Help

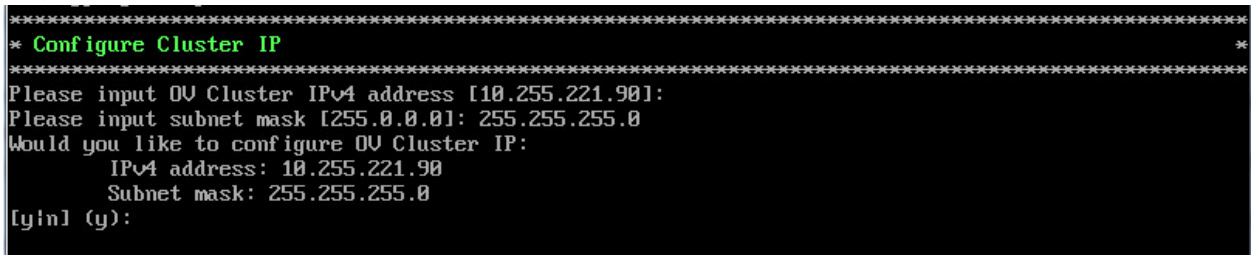
Enter **1** and press **Enter** to bring up help for the Configure Cluster Menu.

Display Cluster Configuration

Enter **2** and press **Enter** to view information about the Cluster, including Node information, HTTP/HTTPS port information and proxy information.

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.

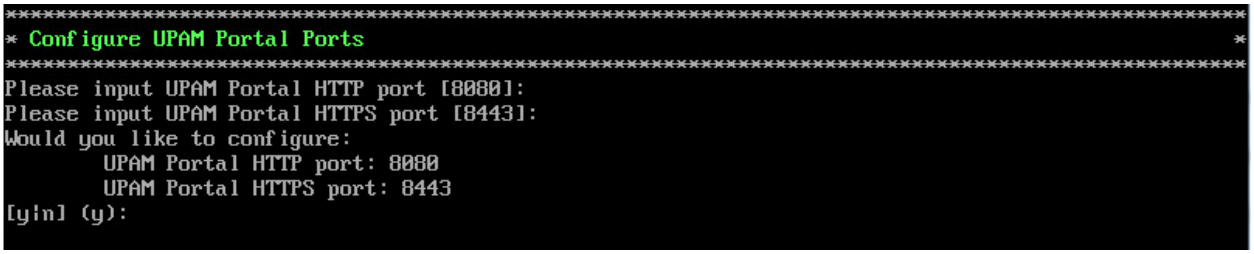


Configure OV Ports

Enter **4** and press **Enter** to configure the OmniVista Web HTTP/HTTPS ports.

Configure UPAM Portal Ports

Enter **5** and press **Enter** to configure the UPAM Portal Ports. You will be prompted to restart services for the change to take effect.



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 **6** 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 **7** 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 **8** 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 **9** and press **Enter** to view/change the OmniVista Login Authentication Server.

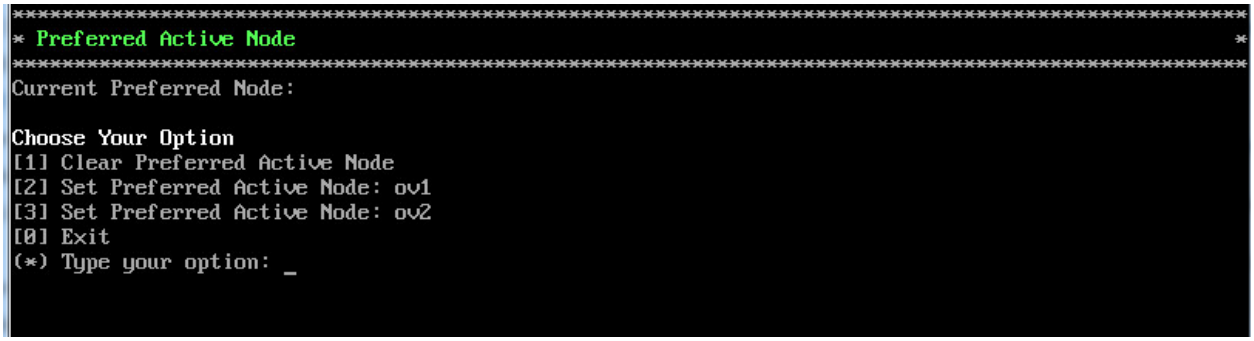
```
*******************************************************************************************************
* Login Authentication Server                                                                         *
*******************************************************************************************************
* [1] Help                                                                                            *
* [2] Current Login Authentication Server                                                             *
* [3] Change Login Authentication Server to local                                                     *
* [0] Exit                                                                                            *
*******************************************************************************************************
(*) Type your option: _
```

Preferred Active Node

Enter **10** 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 **11** 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.

Cluster Error Check

Enter **12** and press **Enter** to display any Cluster Errors.

Configure Peer Node's Information

Enter **13** and press **Enter** to change the IP address and Hostname 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 **14** and press **Enter** to enable Maintenance Mode to perform an upgrade 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. To upgrade the Nodes:

1. Enable Maintenance Mode.
2. Perform the upgrade on Node 1 (do not restart Node 1)
3. Perform the upgrade on Node 2.
4. Restart both Nodes.
5. Disable Maintenance Mode (you only have to execute the command on one Node).

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 – Configure Mongodb Password

14 – Configure IP and Hostname

15 – Extend Data Partitions

0 – Exit

Help

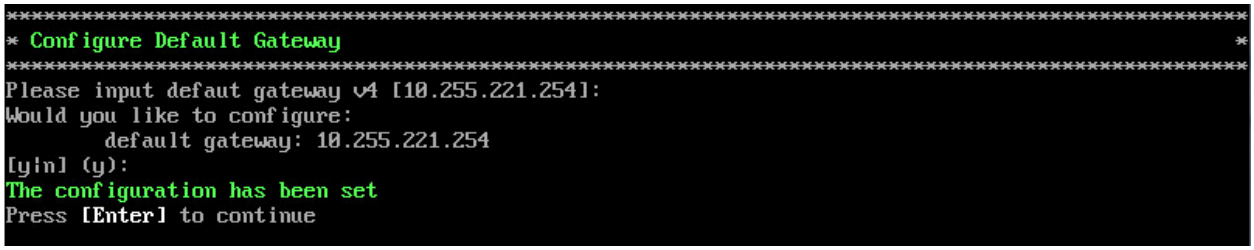
Enter **1** and press **Enter** to bring up help for the Configure Current Node Menu.

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.



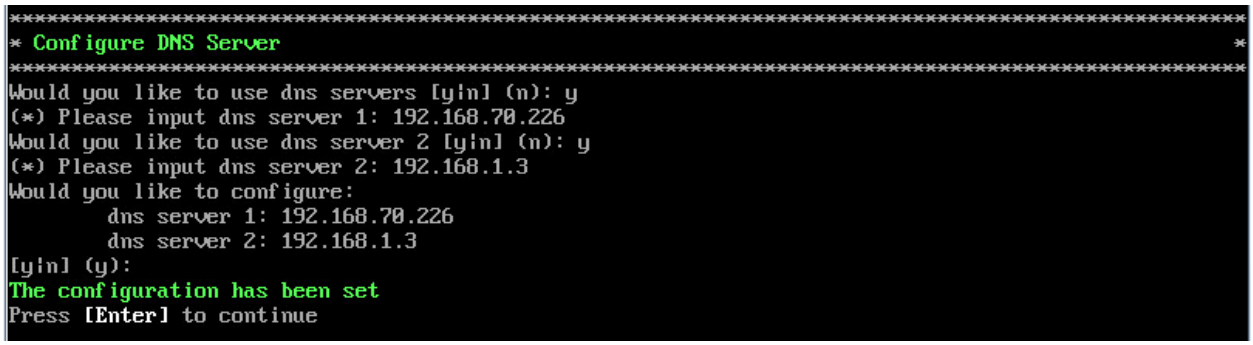
2. Enter an IPv4 default gateway.

3. Press **Enter** to confirm the settings. Press **Enter** to return to the Configure Current Node Menu.

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 time zone; then confirm by typing **y** at the prompt.

2. Select the region for the VM by entering its corresponding numeric value (e.g., **10**).

3. Select a country within the region by entering its corresponding numeric value (e.g., **25**).

4. If prompted, enter the numeric value for the specific time zone within the country (e.g., **21**).

```
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#?
```

5. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure Current Node Menu.

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                                                                                       *
**************************************************************************************************
(*) Type your option: _
```

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.

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**.

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**.

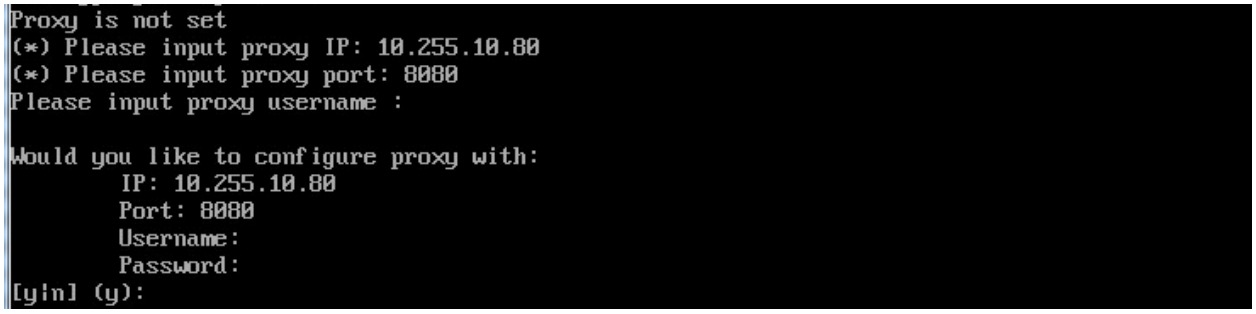
Configure Proxy

OmniVista makes an HTTPS connection to the OmniVista 2500 NMS External Repository for upgrade software, Application Visibility Signature Files, and ProActive Lifecycle Management. 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

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 the VM will use a proxy server, 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**.

```
(*) Type your option: 11
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 30 characters
Enter new password:

Retype password:

Changing password for user cliadmin.
passwd: all authentication tokens updated successfully.
```

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**.

Configure Mongodb Password

Enter **13** and press **Enter** to change the Mongodb password. 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.

Configure IP and Hostname

Enter **14** and press **Enter** to change the IP address and Hostname 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.

Extend Data Partitions

Enter **15** and press **Enter** to add an additional hard disk and extend the current data partitions. By default, OV 2500 NMS-E 4.3R1 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.

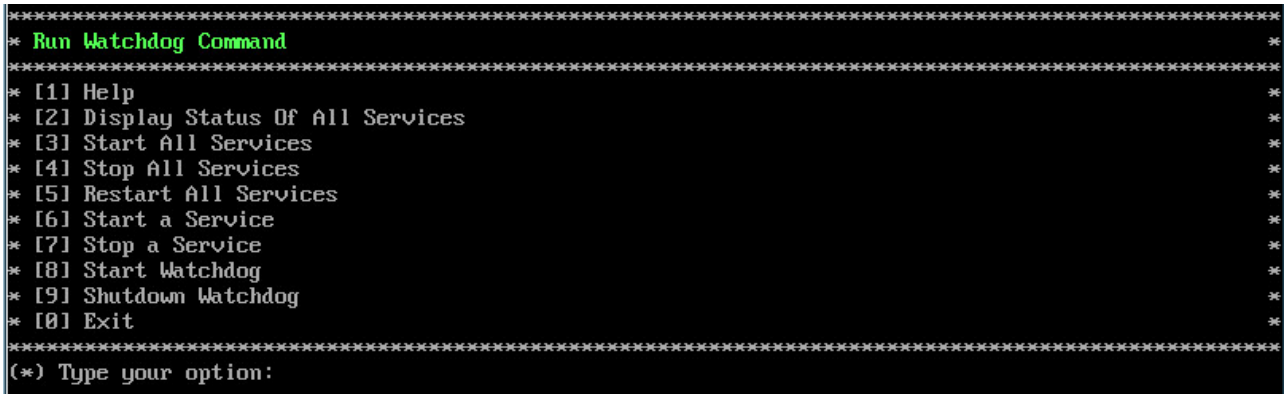
Exit

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 4.3R1. 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.



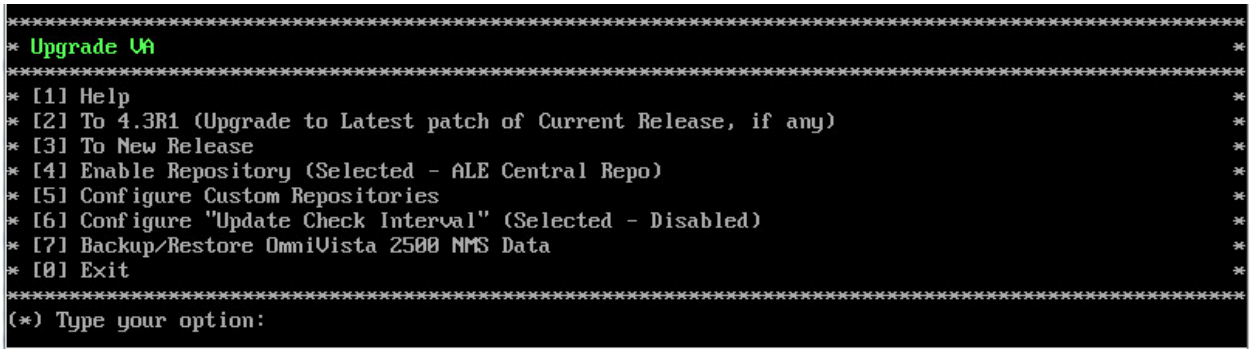
The following options are available:

- **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 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.



The following options are available:

- **To 4.3R1 (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 Update -** OV displays information about the currently-installed OmniVista NMS software, checks for available updates and downloads and installs the update, if available.
  - **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 4.3R1 (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 Host -** The IP address of the custom repository (e.g., 192.168.70.10).
- **Repository URL Location -** The directory location of the upgrade software (e.g., repo/centos)
- **Repository Full URL -** Is automatically completed by OV after confirming the configuration.

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 (/opt/OmniVista_2500_NMS/data/file_server/cliadmin/backups) 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.
  - **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 4.3R1 configuration using a 4.3R1 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 4.3R1 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

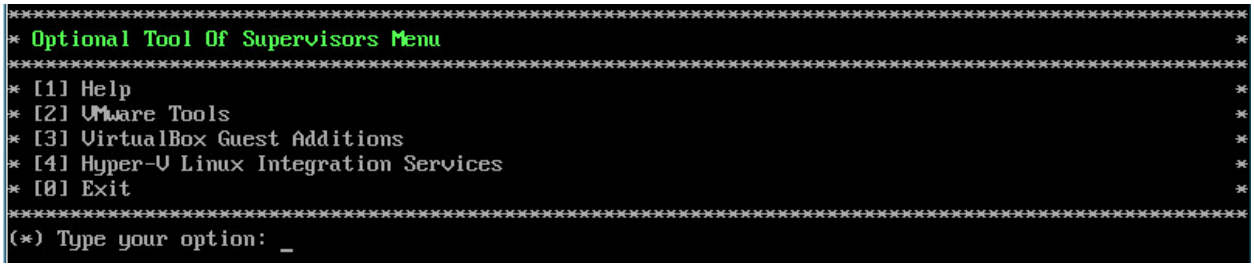
You can view OV 2500 NMS-E 4.3R1 Logs using the “Logging” option. Enter **6**, then press **Enter**.

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 **7**, 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 **8**, 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

Enter **8** and press **Enter** to

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 **9** 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 4.3R1 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 **10** 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 4.3R1 functions continue following reboot.

Log Out

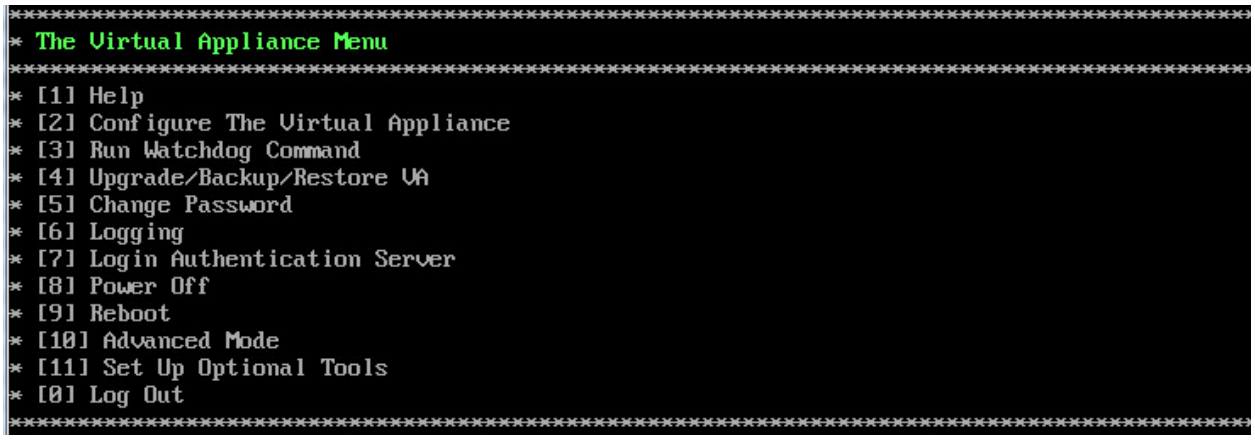
To log out of the VM and return to the cliadmin login prompt, enter **0** at the command line. Confirm logout by entering **y**. Note that OV 2500 NMS-E 4.3R1 functions continue following logout.

Appendix D – Extending the VA Partition Size

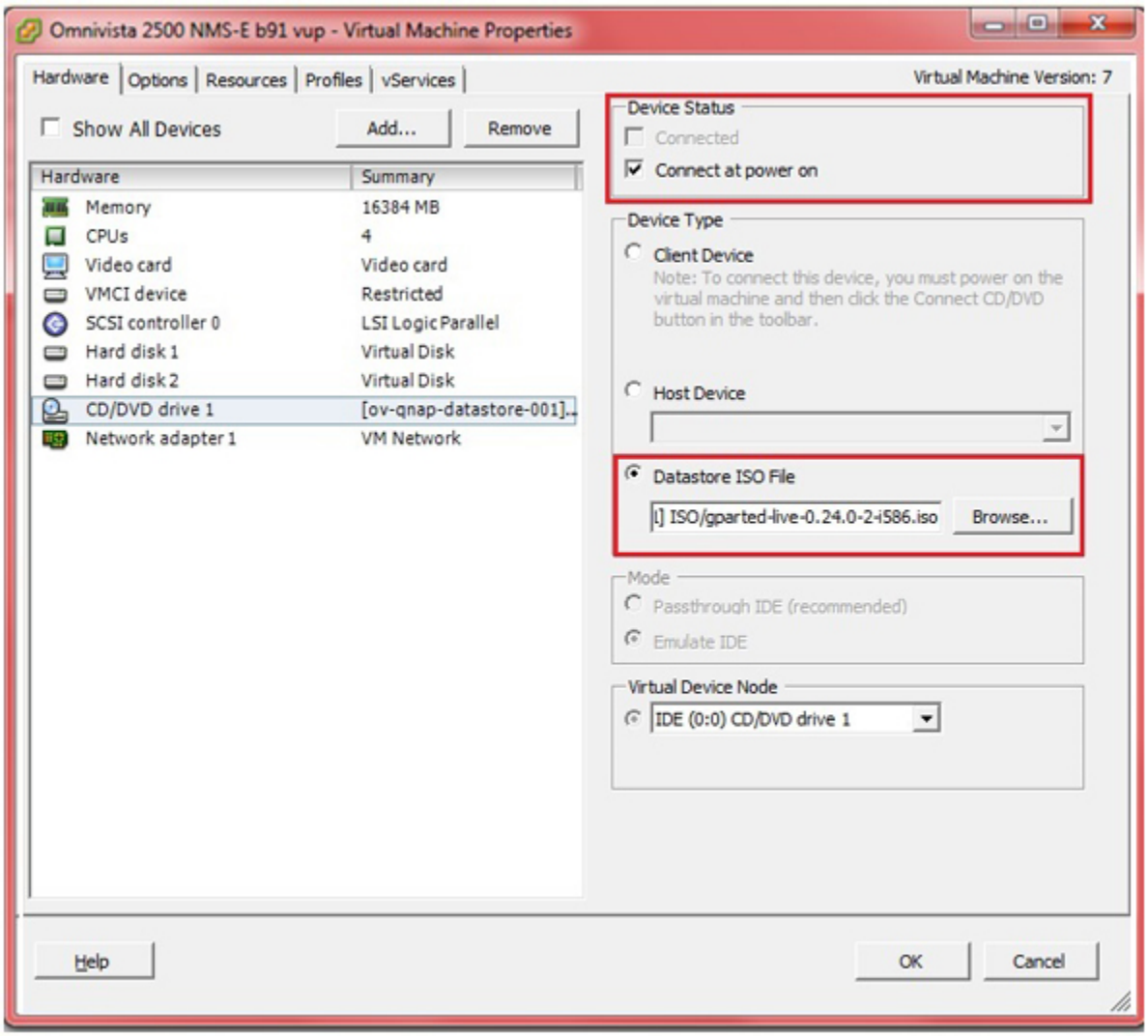
If necessary, you can use the GParted Partition Manager to resize VA partitions. GParted is a free partition manager tool that can be downloaded for free here. After downloading GParted, follow the steps below to extend the partition size of an existing VA installation.

- Step 1: Power off the VA.
- Step 2: Download and mount the GParted Live CD to the CD drive.
- Step 3: Increase the Disk Provisioned Size of the Hard Disk.
- Step 4: Configure the bootup Force BIOS setup.
- Step 5: Change the boot order to boot from the CD-ROM Drive.
- Step 6: Boot the VA from the GParted Live CD.
- Step 7: Open GParted.
- Step 8: Select device /dev/sda and select partition /dev/sda3 then click Resize/Move.
- Step 9: Extend the disk size for /dev/sdb and /dev/sdb1.
- Step 10: Select Apply and confirm.
- Step 11: Wait for the process to finish and reboot the VA.
- Step 12: Reboot from the local drive.

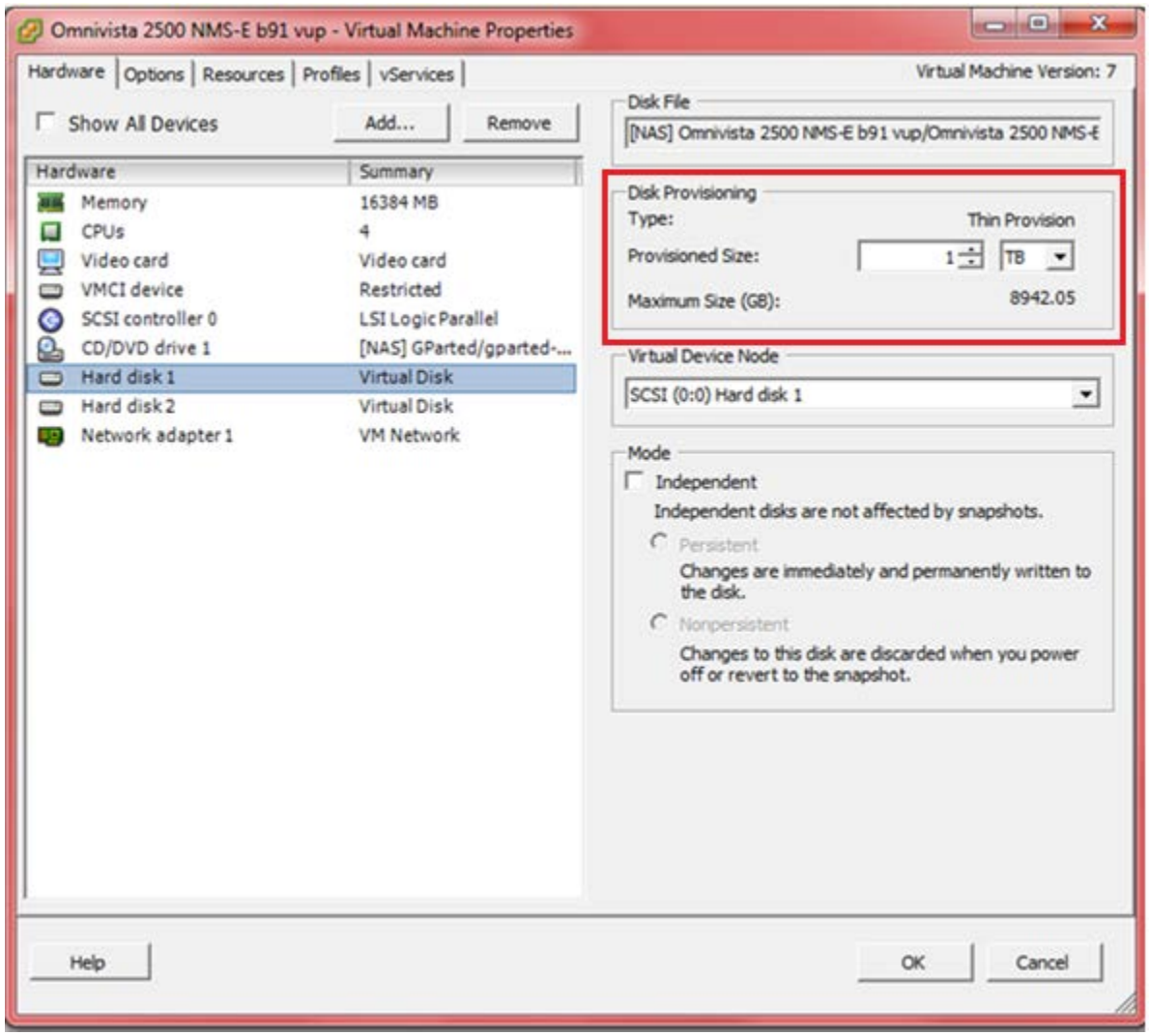
Step 1: Open a Console on the VA with cliadmin account. Use option **8** to power off the VA.



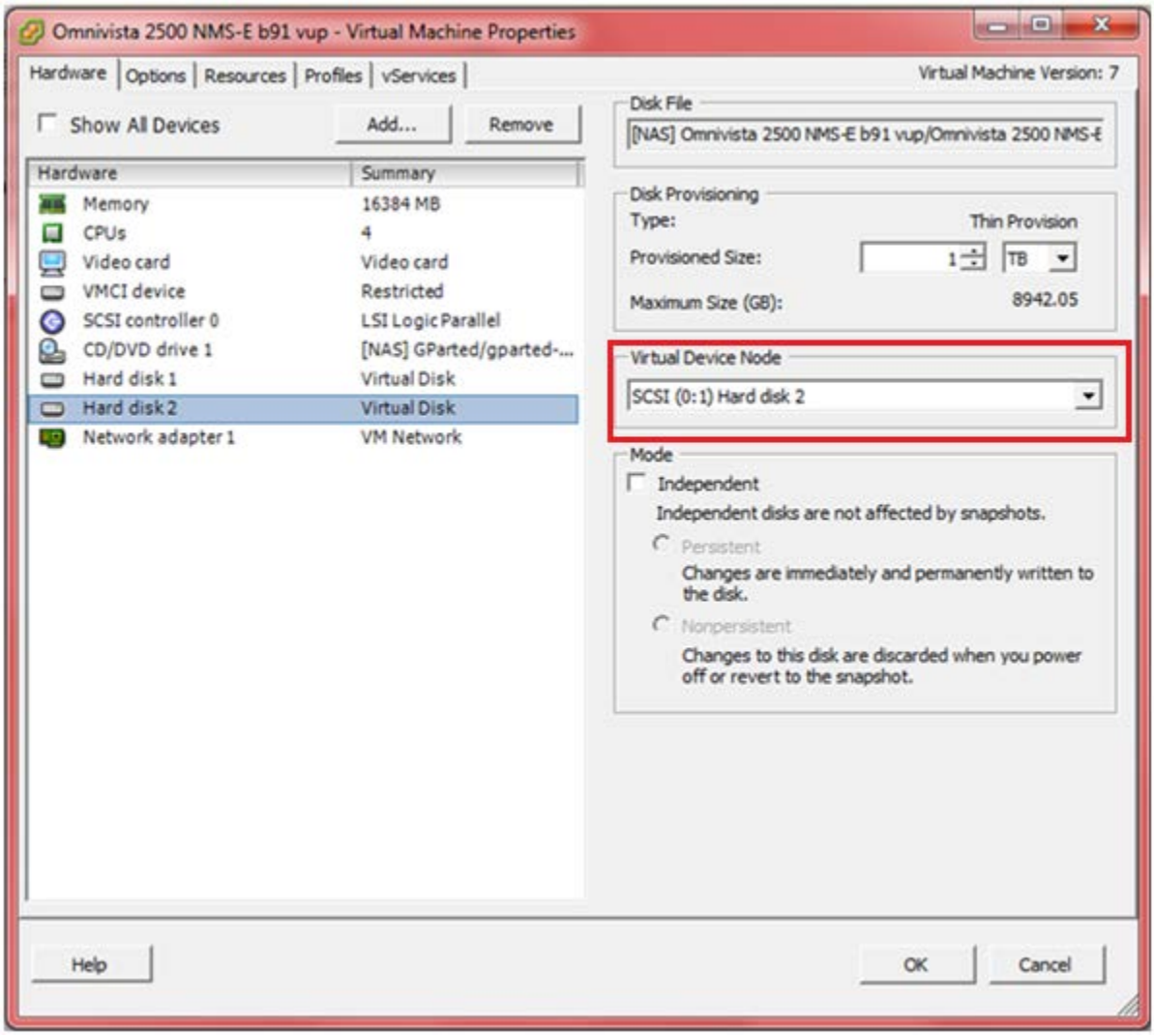
Step 2: Download and mount the GParted Live CD to the CD drive (make sure “Connect at power on” option is selected in the Device Status area).



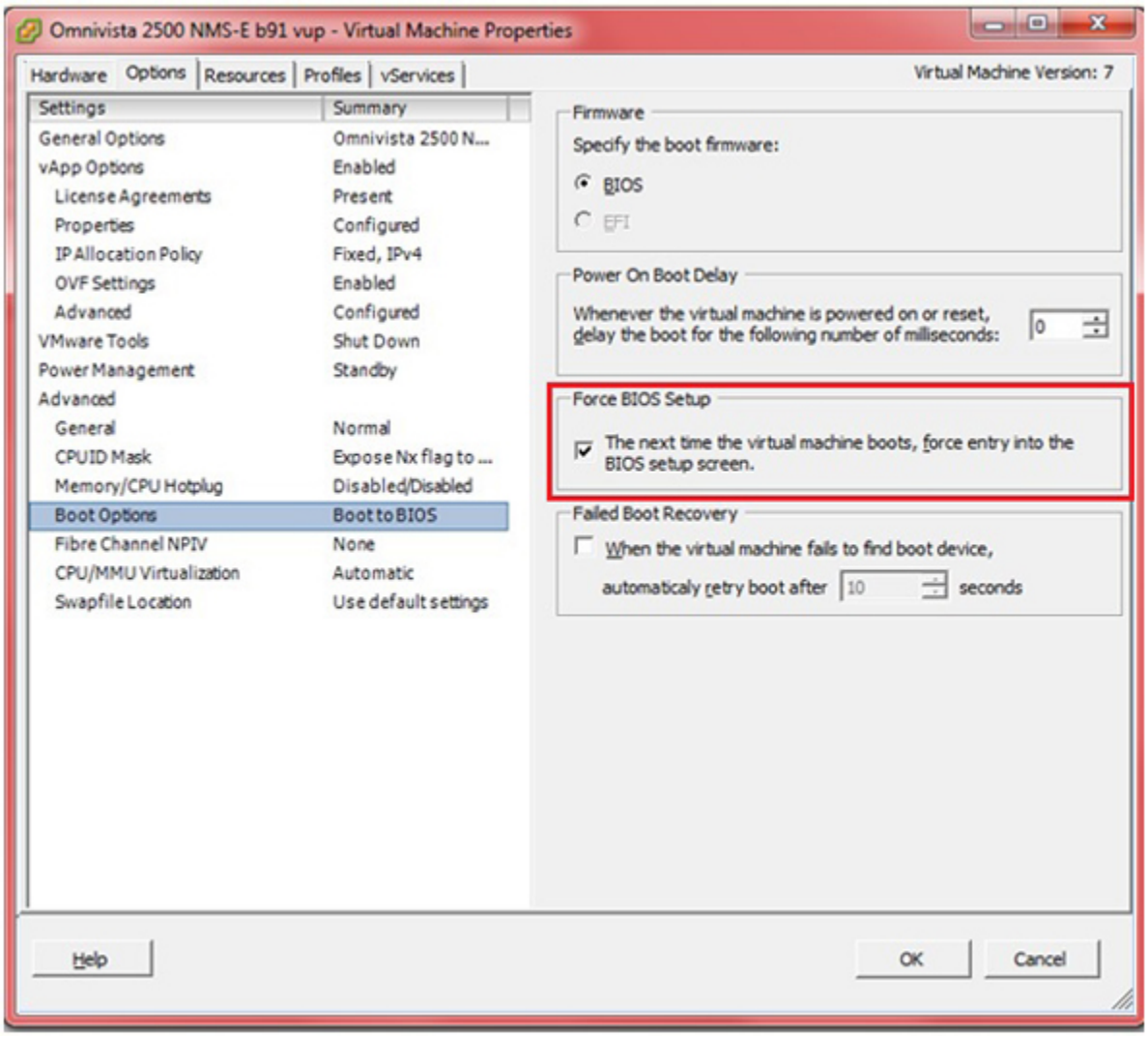
Step 3: Increase the Disk Provisioned Size of the Hard Disk. Select Hard disk 1 and increase the Disk Provisioned Size from the default of 256GB to the recommended size (e.g. 1TB). Data and System files are stored in 2 virtual disks. You must change the provision size for **both** disks. By default, “Hard disk 1” appears in the **Virtual Device Node** drop-down menu. Update the **Provisioned Size** to the recommended size and click **OK**.



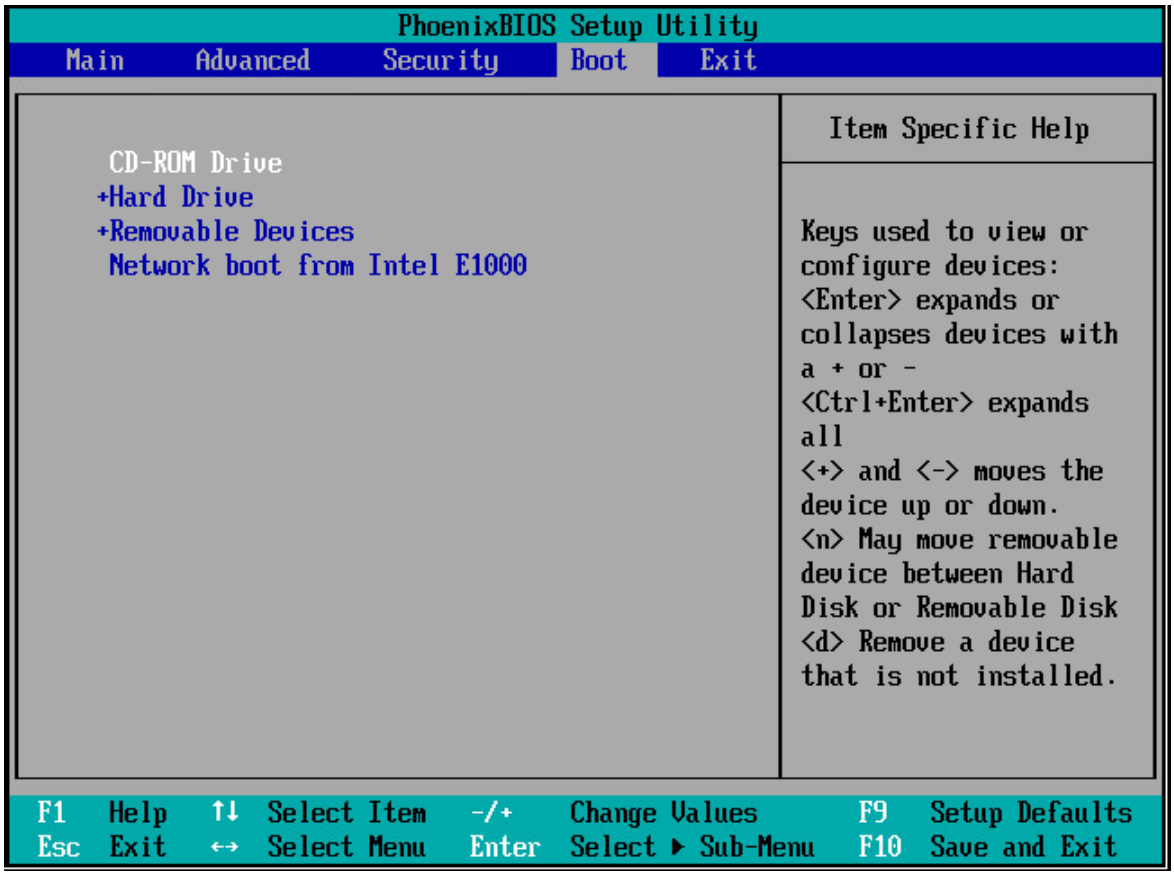
Then select “Hard disk 2” in the **Virtual Device Node** drop-down menu. Change the **Provisioned Size** to the recommended size and click **OK**, as shown below.



Step 4: Configure the bootup Force BIOS setup. Click on the **Options** tab, select **Boot options**, then select the checkbox in the **Force BIOS Setup** area. Click **OK**.

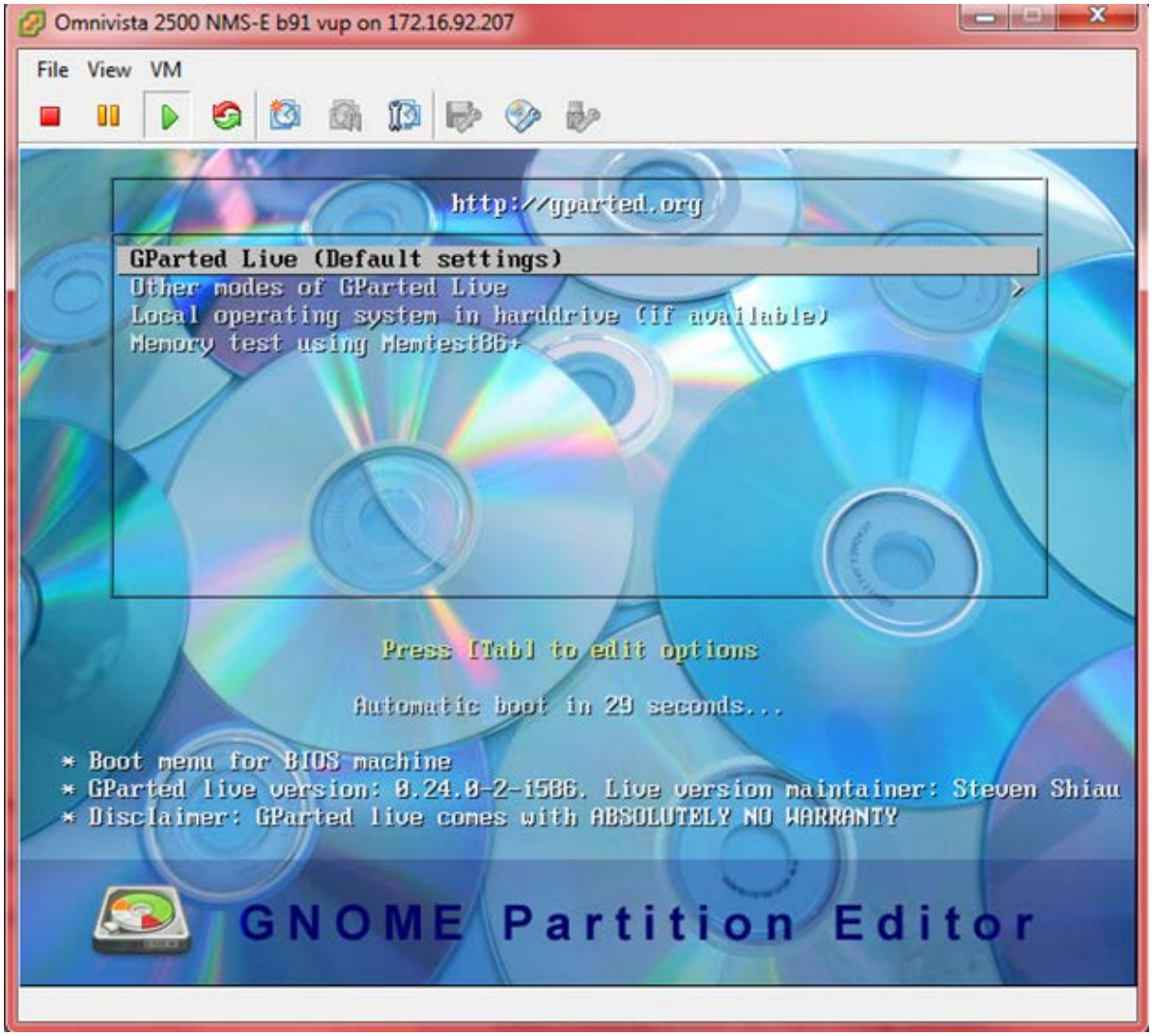


Step 5: Start the VA. Change the boot order to boot from the CD-ROM Drive. Go to the Boot tab and use the **+/-** keys to move the CD-ROM Drive to the top of the list. Press **F10** and select **Yes** at the confirmation prompt to save and exit.

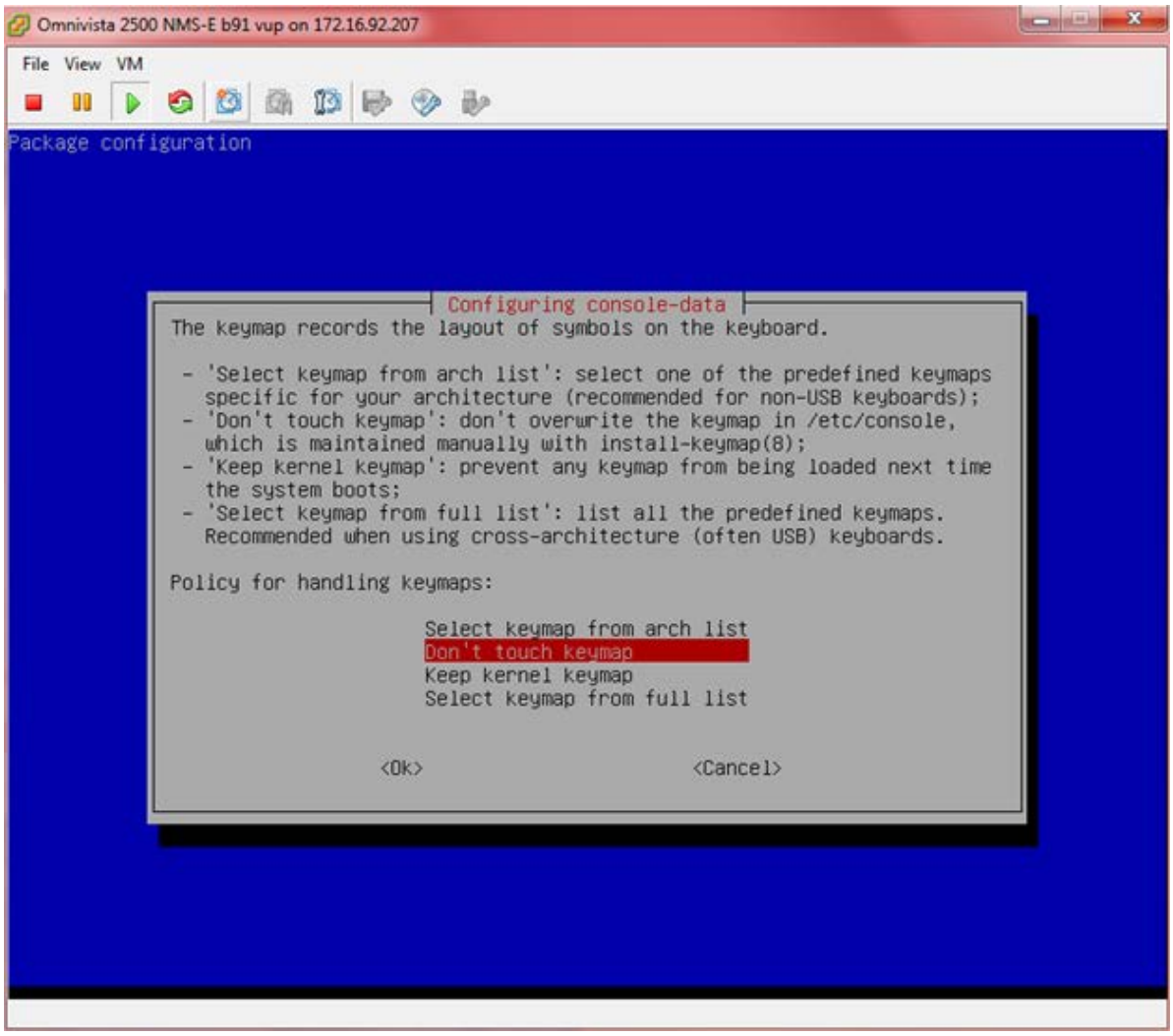


Step 6: Boot the VA from the GParted Live CD.

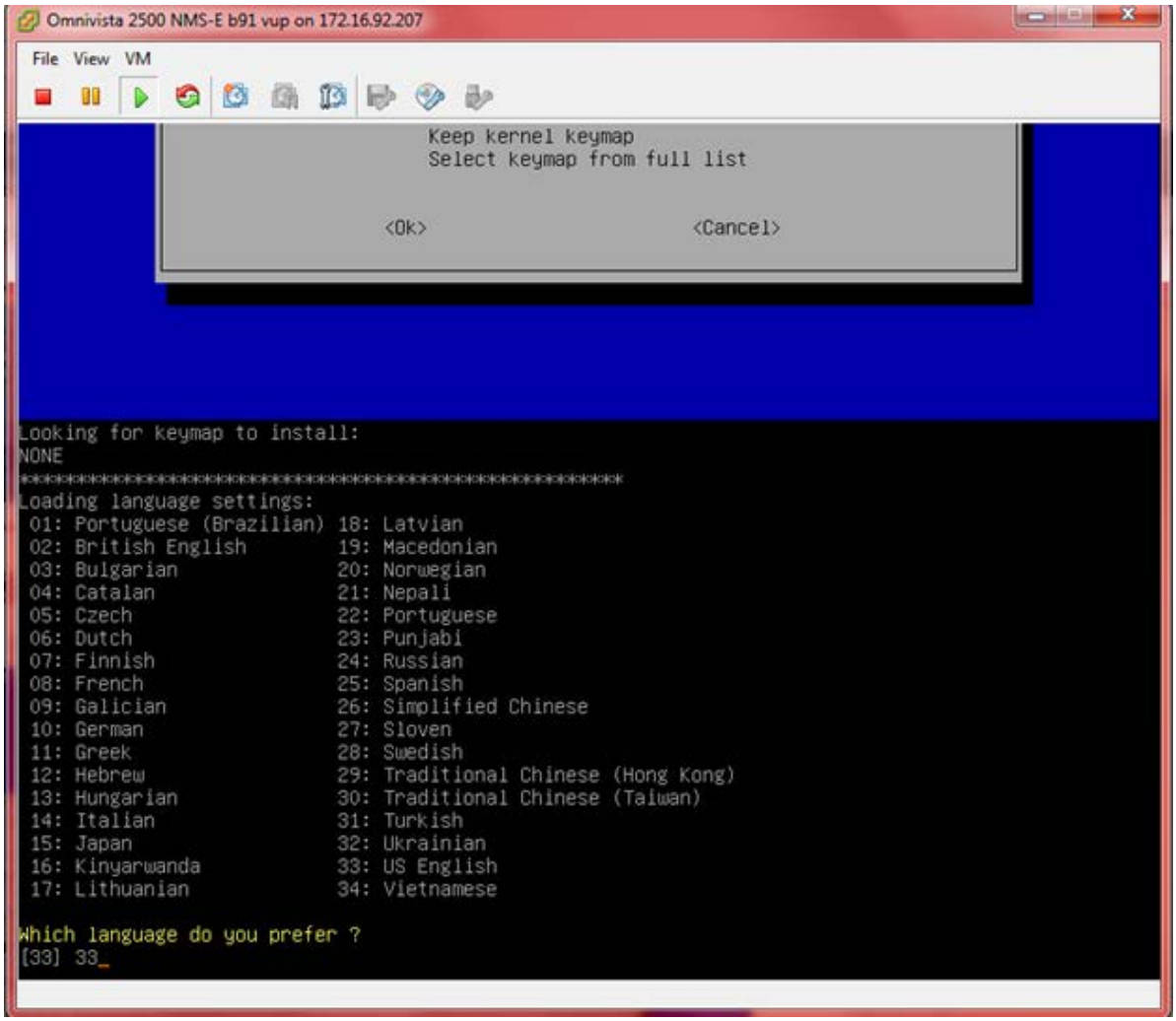
Select **GParted Live (Default Settings)**.



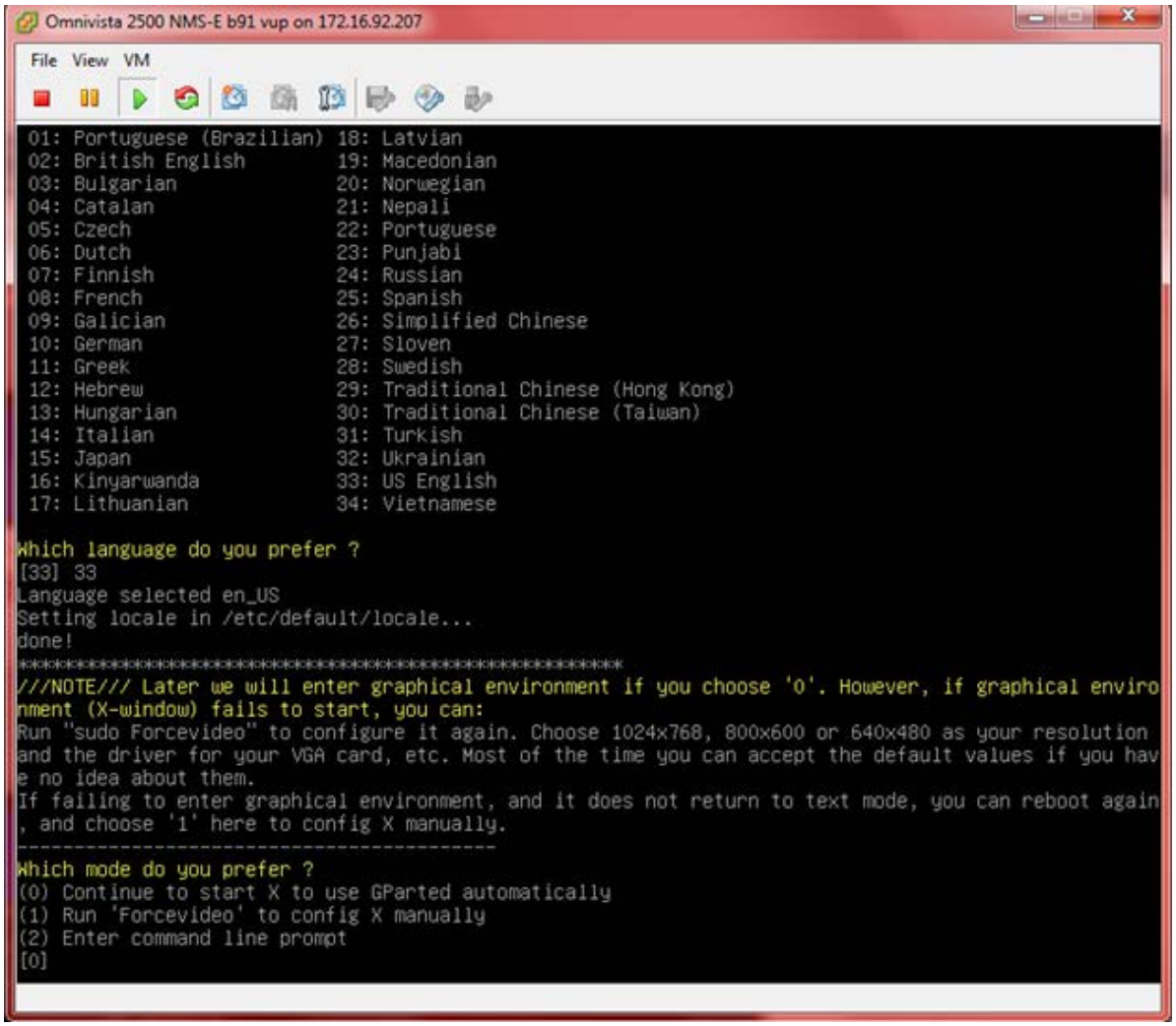
Select **Don't Touch Keymap**



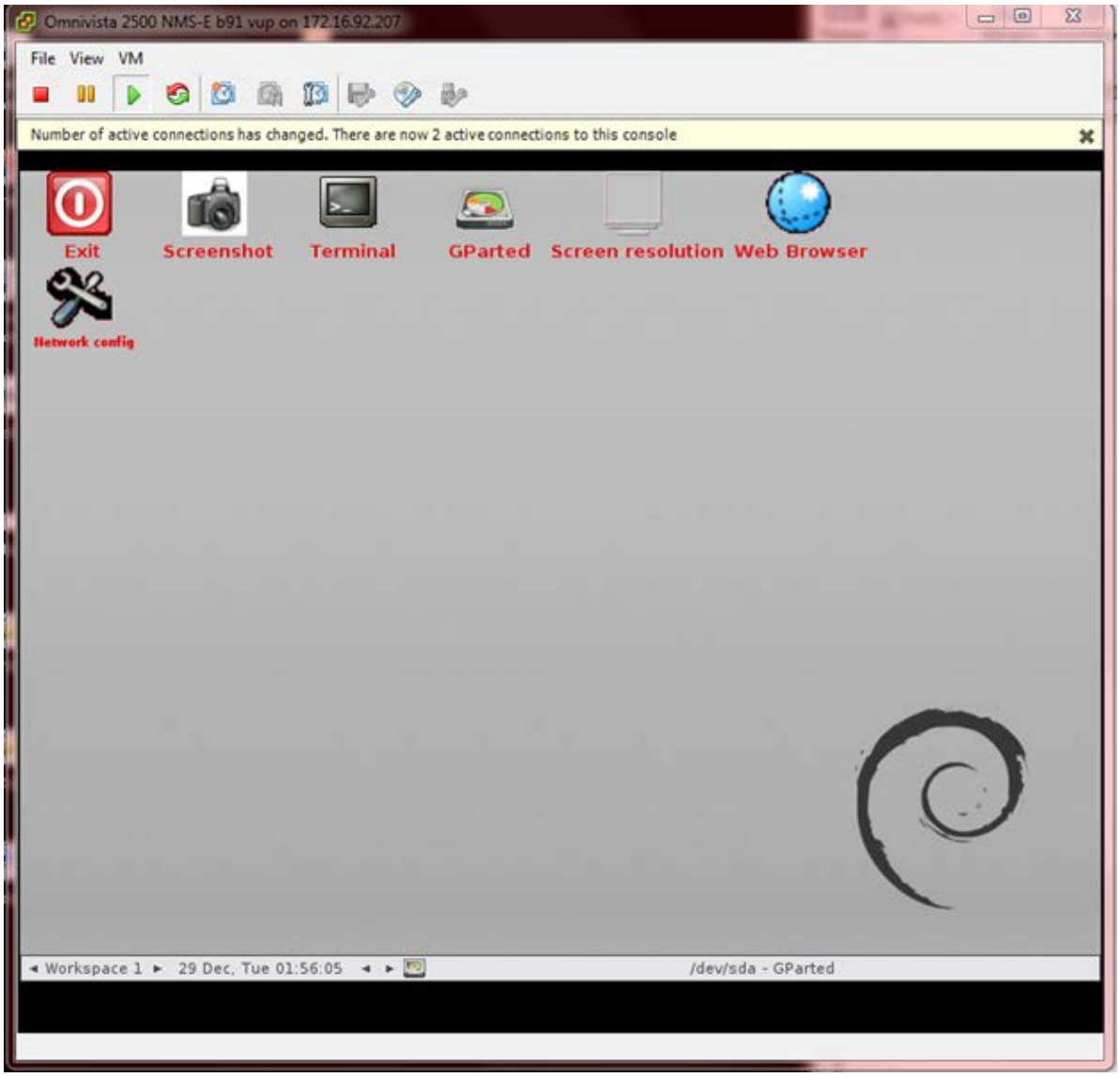
Select the preferred language.



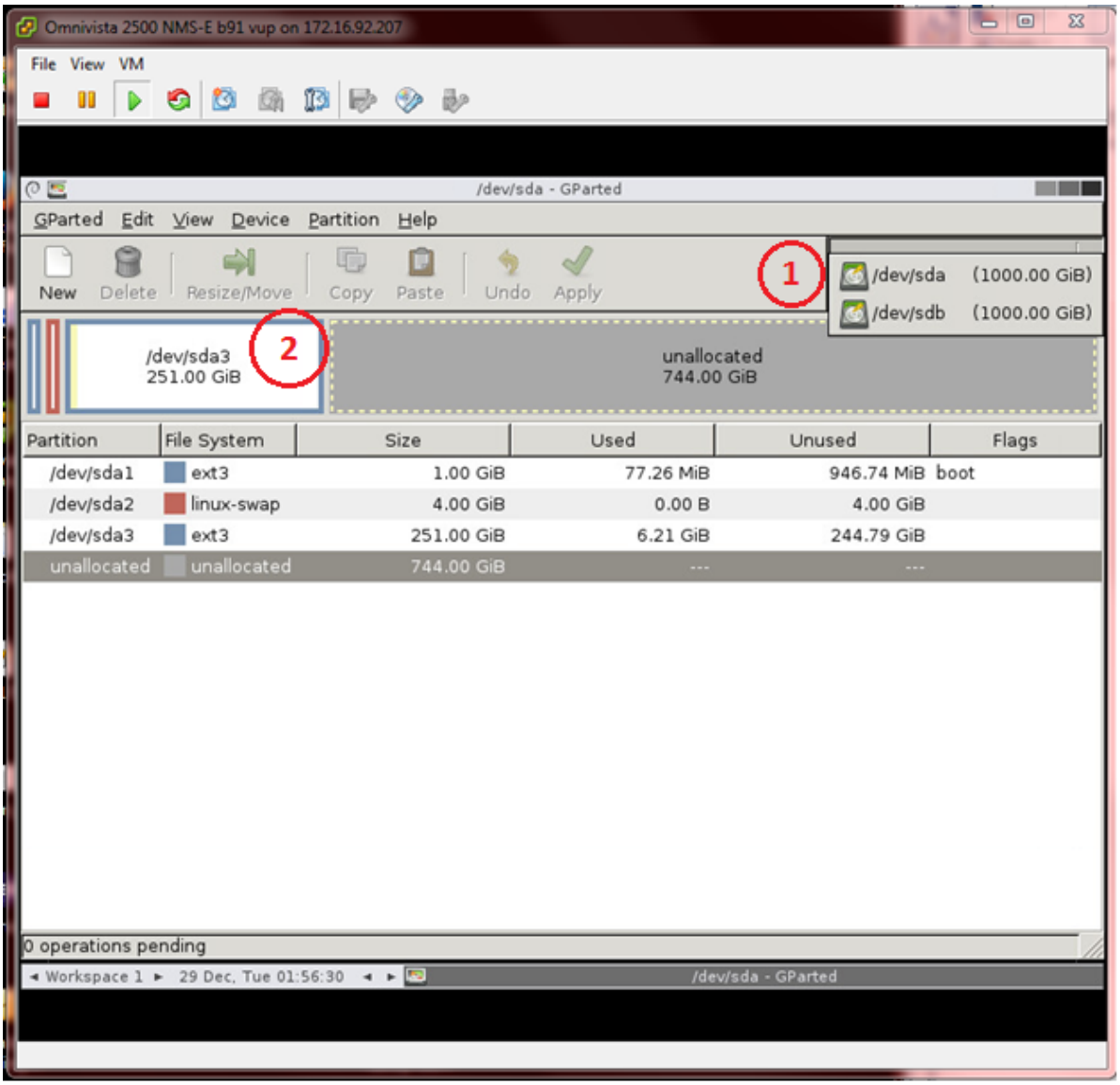
Select **(0) Continue to start X to use GParted automatically.**



Step 7: GParted should launch automatically. If not, click on the **GParted** icon to open GParted, as shown below.

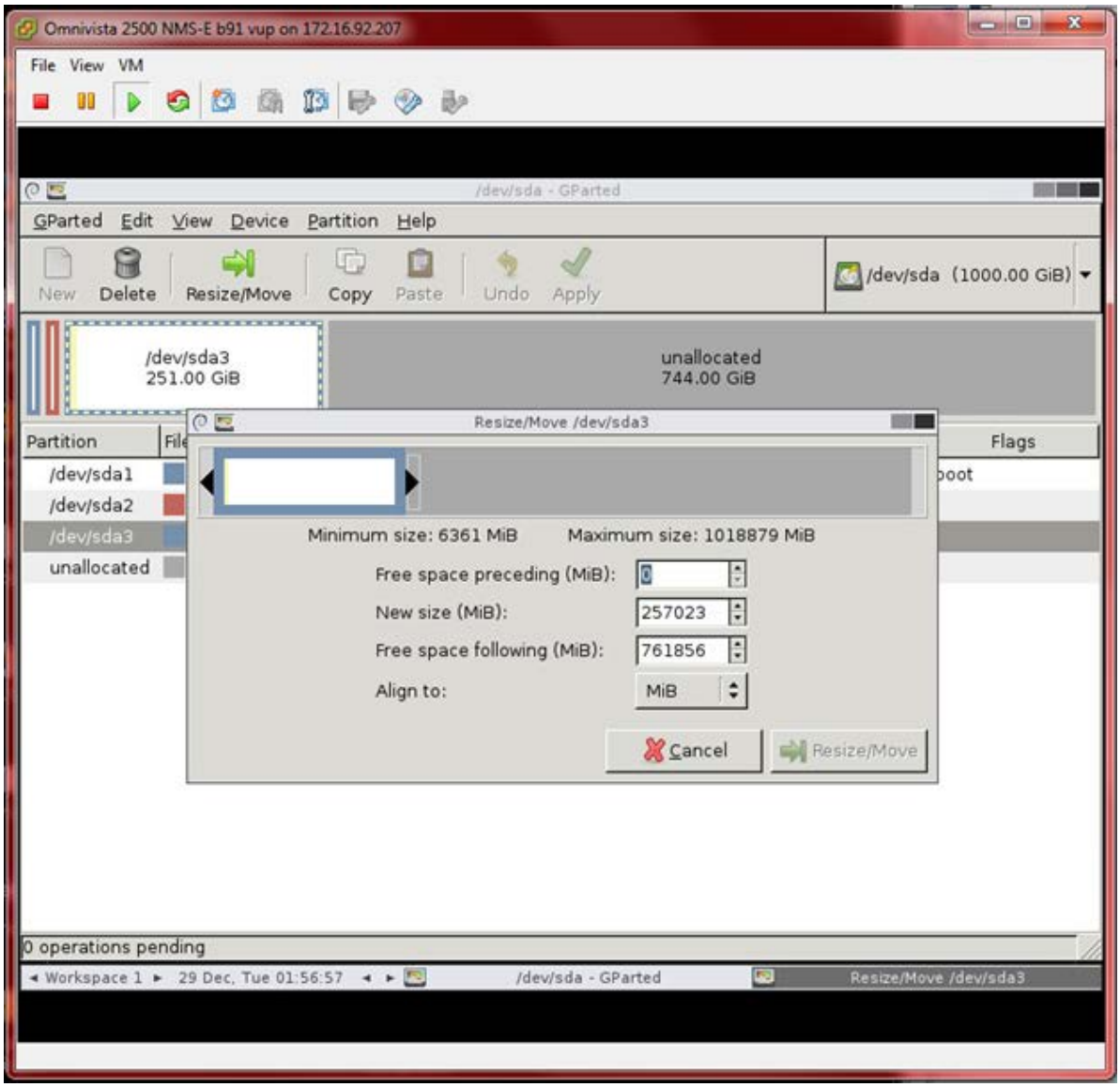


Step 8: Select device /dev/sda and select partition /dev/sda3 then click **Resize/Move**.

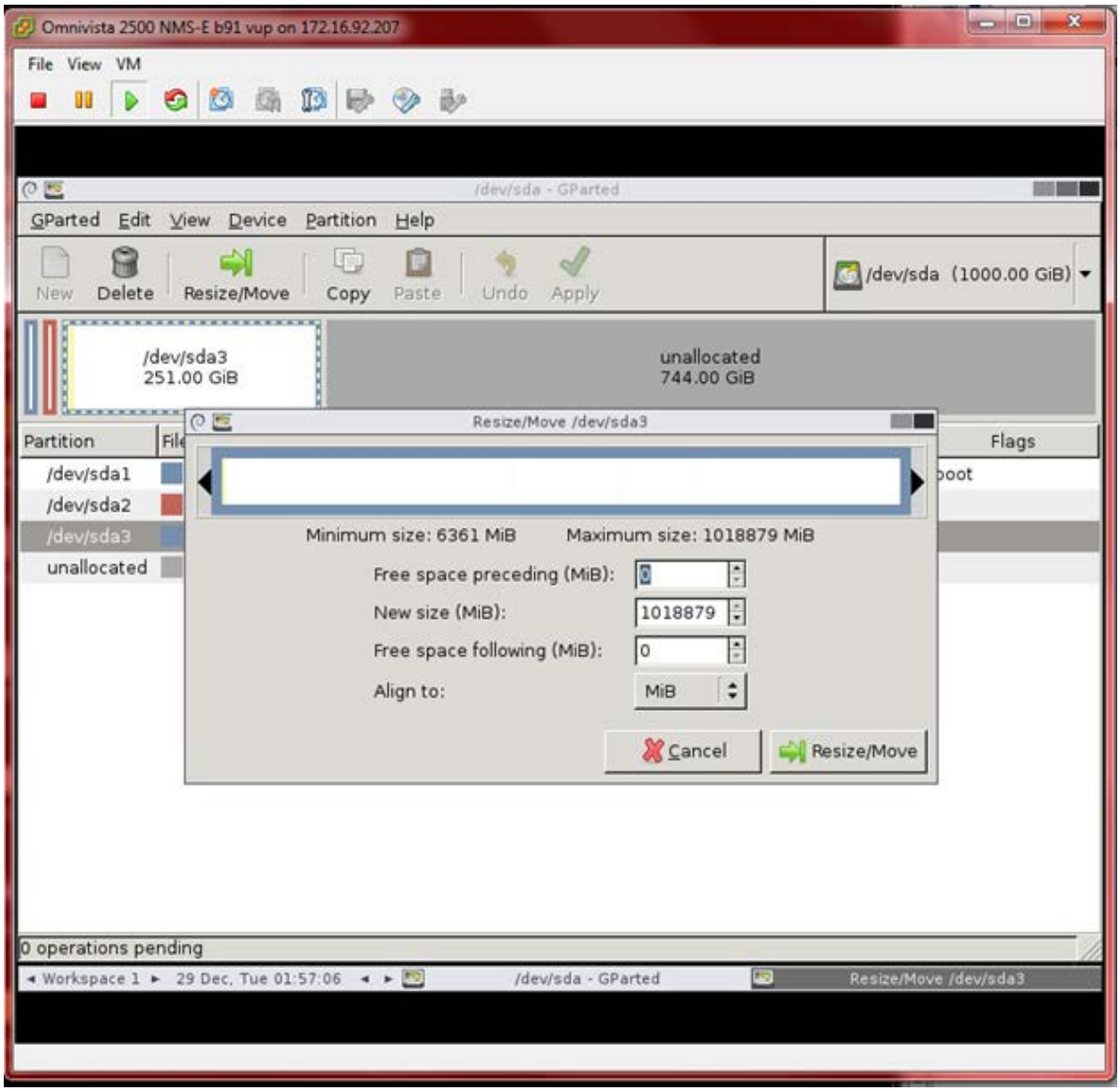


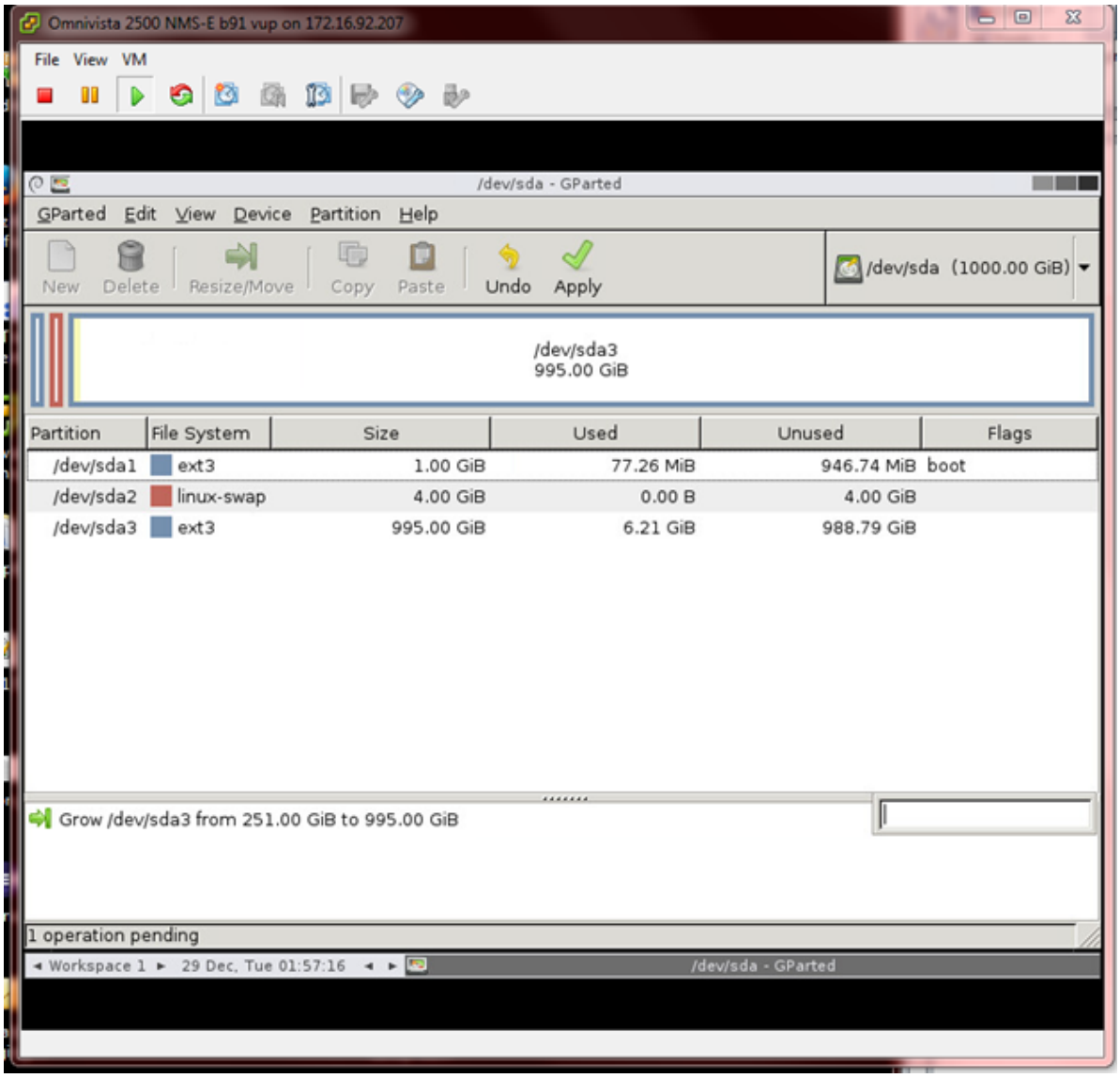
Use the UI menu to change the partition size. Or use the input menu below to enter the size for the partition. When complete, click on the **Resize/Move** button.

Before

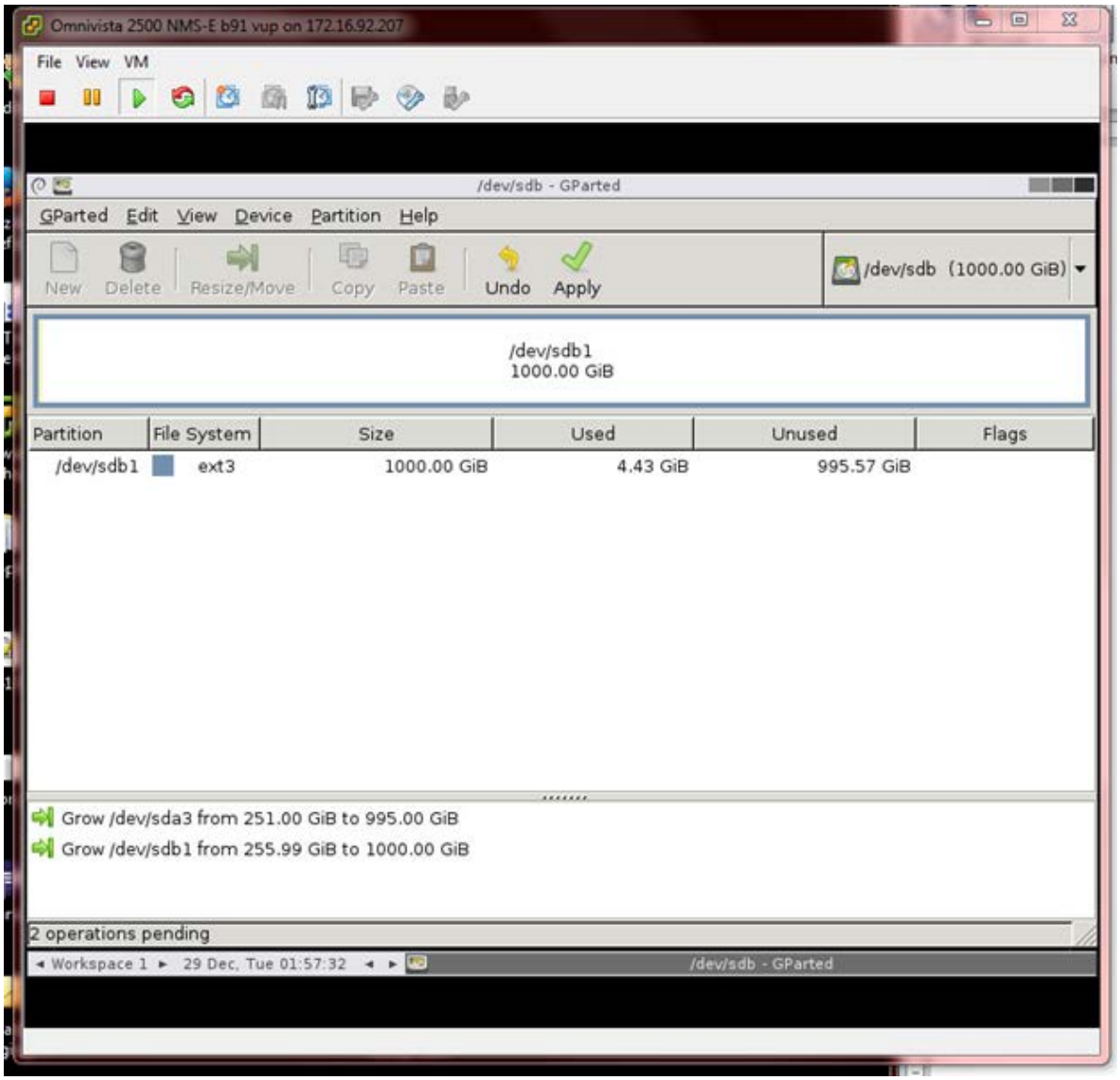

Omnivista 2500 NMS-E b91 vup on 172.16.92.207
File View VM
/dev/sda - GParted
GParted Edit View Device Partition Help
New Delete Resize/Move Copy Paste Undo Apply
/dev/sda (1000.00 GiB)
/dev/sda3
251.00 GiB
unallocated
744.00 GiB
Resize/Move /dev/sda3
Partition
Flags
/dev/sda1
/dev/sda2
/dev/sda3
unallocated
Minimum size: 6361 MiB
Maximum size: 1018879 MiB
Free space preceding (MiB): 0
New size (MiB): 257023
Free space following (MiB): 761856
Align to: MiB
Cancel
Resize/Move
0 operations pending
Workspace 1
29 Dec, Tue 01:56:57
/dev/sda - GParted
Resize/Move /dev/sda3

After

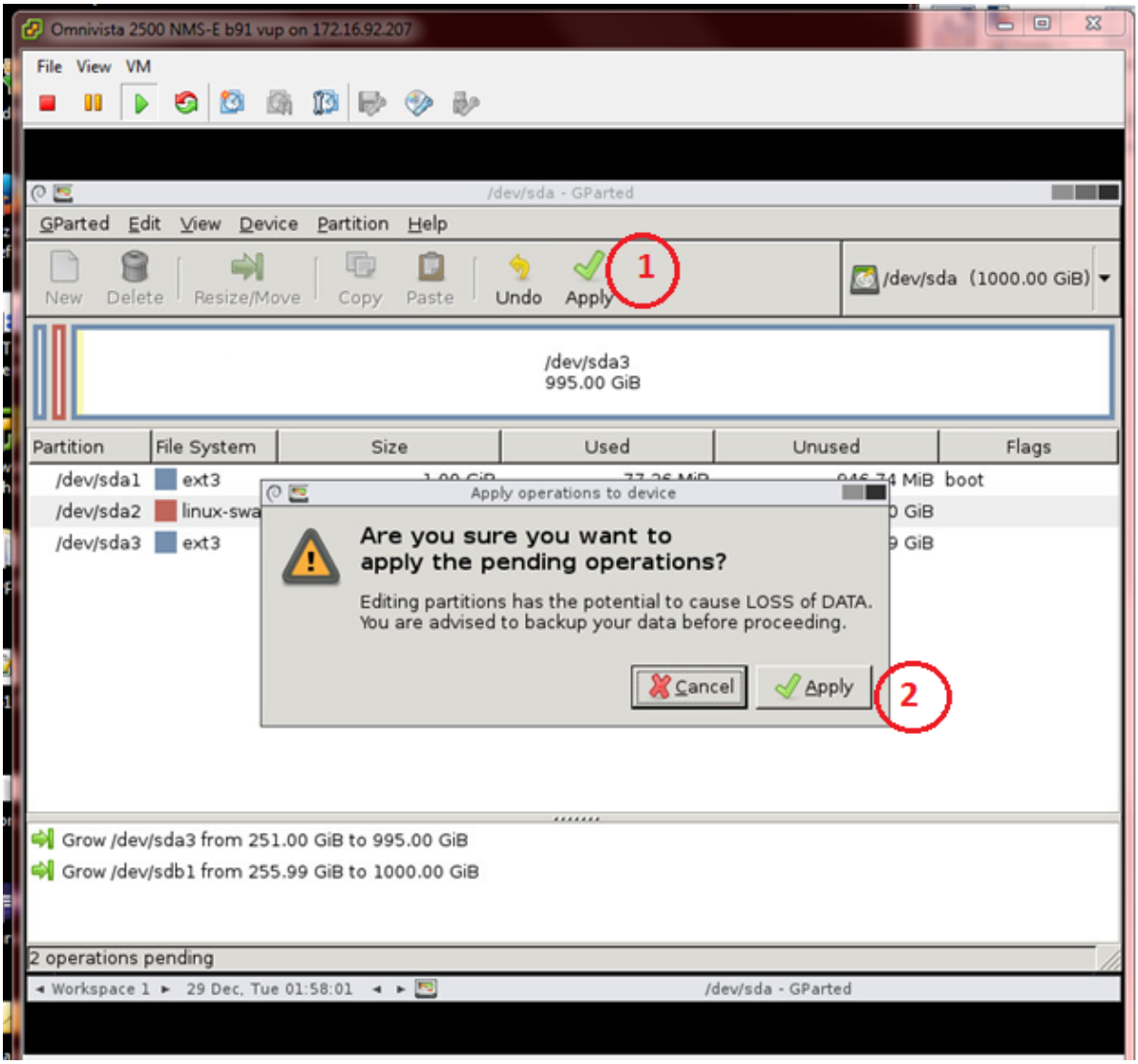

Omnivista 2500 NMS-E b91 vup on 172.16.92.207
File View VM
/dev/sda - GParted
GParted Edit View Device Partition Help
New Delete Resize/Move Copy Paste Undo Apply
/dev/sda (1000.00 GiB)
/dev/sda3
251.00 GiB
unallocated
744.00 GiB
Resize/Move /dev/sda3
Partition
Flags
/dev/sda1
/dev/sda2
/dev/sda3
unallocated
Minimum size: 6361 MiB
Maximum size: 1018879 MiB
Free space preceding (MiB):
New size (MiB):
1018879
Free space following (MiB):
Align to:
MiB
Cancel
Resize/Move
0 operations pending
Workspace 1
29 Dec, Tue 01:57:06
/dev/sda - GParted
Resize/Move /dev/sda3


Omnivista 2500 NMS-E b91 vup on 172.16.92.207
File View VM
/dev/sda - GParted
GParted Edit View Device Partition Help
New Delete Resize/Move Copy Paste Undo Apply
/dev/sda (1000.00 GiB)
/dev/sda3
995.00 GiB
Partition File System Size Used Unused Flags
/dev/sda1 ext3 1.00 GiB 77.26 MiB 946.74 MiB boot
/dev/sda2 linux-swap 4.00 GiB 0.00 B 4.00 GiB
/dev/sda3 ext3 995.00 GiB 6.21 GiB 988.79 GiB
Grow /dev/sda3 from 251.00 GiB to 995.00 GiB
1 operation pending
Workspace 1 29 Dec, Tue 01:57:16
/dev/sda - GParted

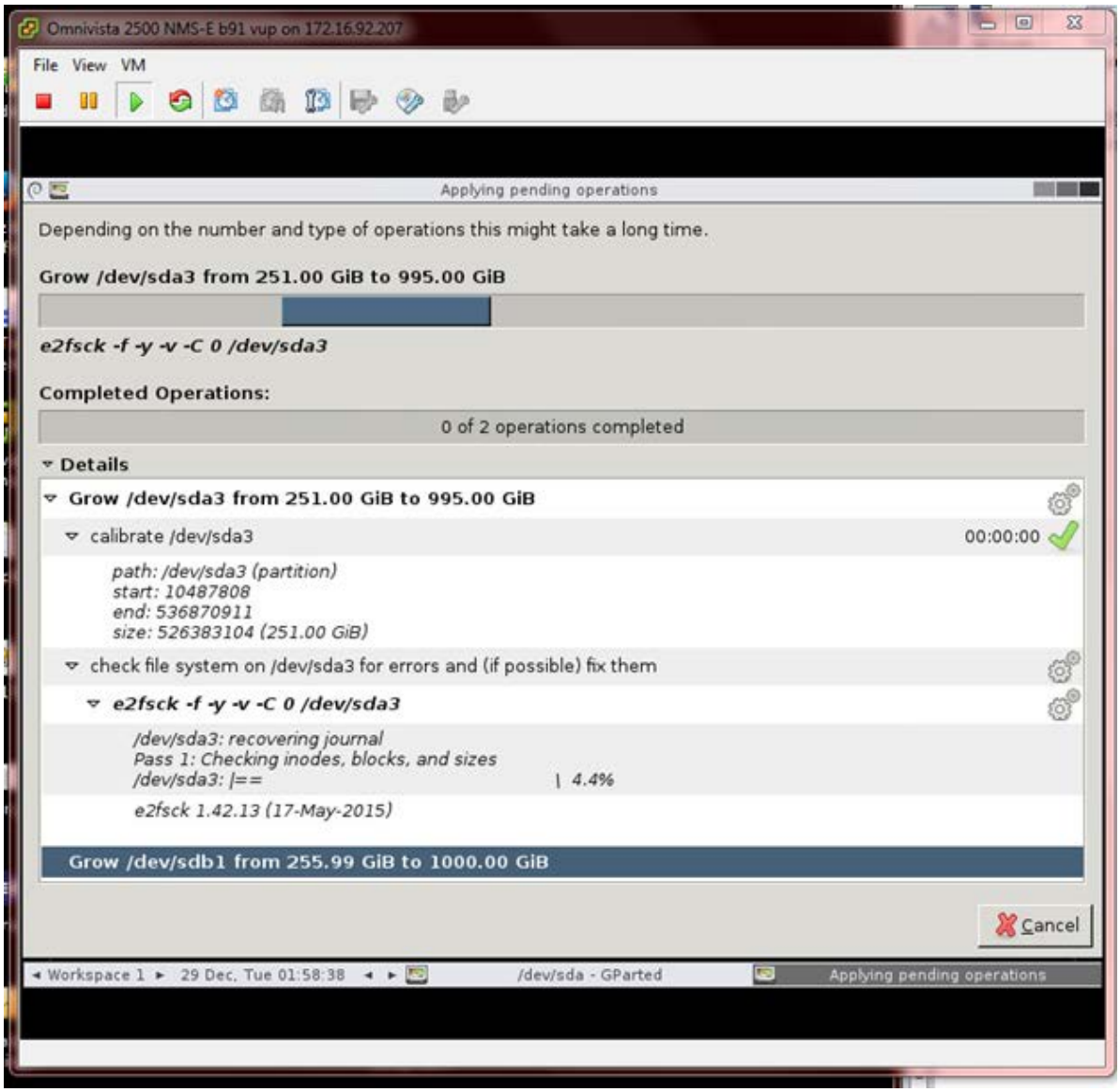
Step 9: Extend the disk size for /dev/sdb and /dev/sdb1.

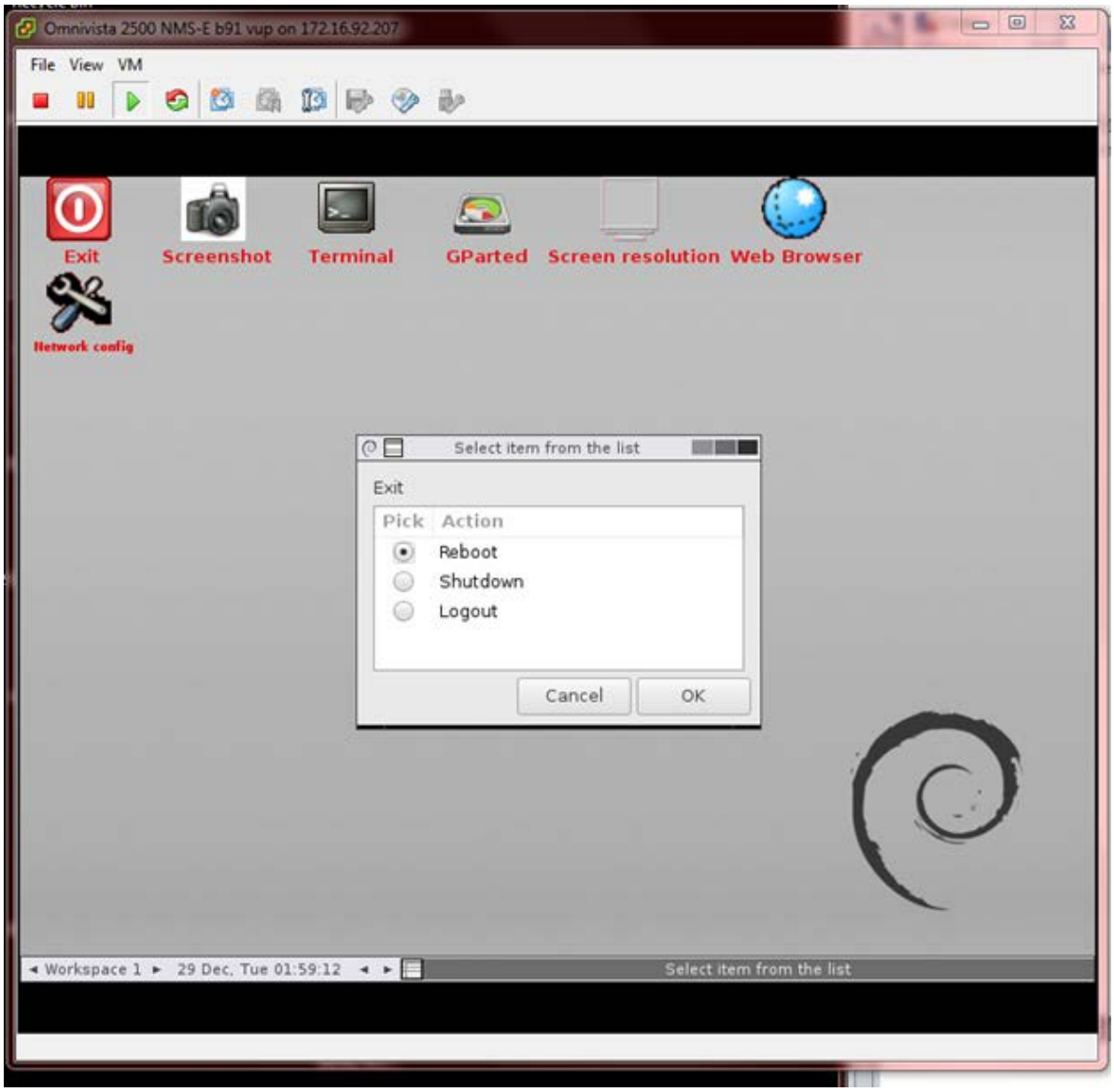


Step 10: Select **Apply** and confirm.

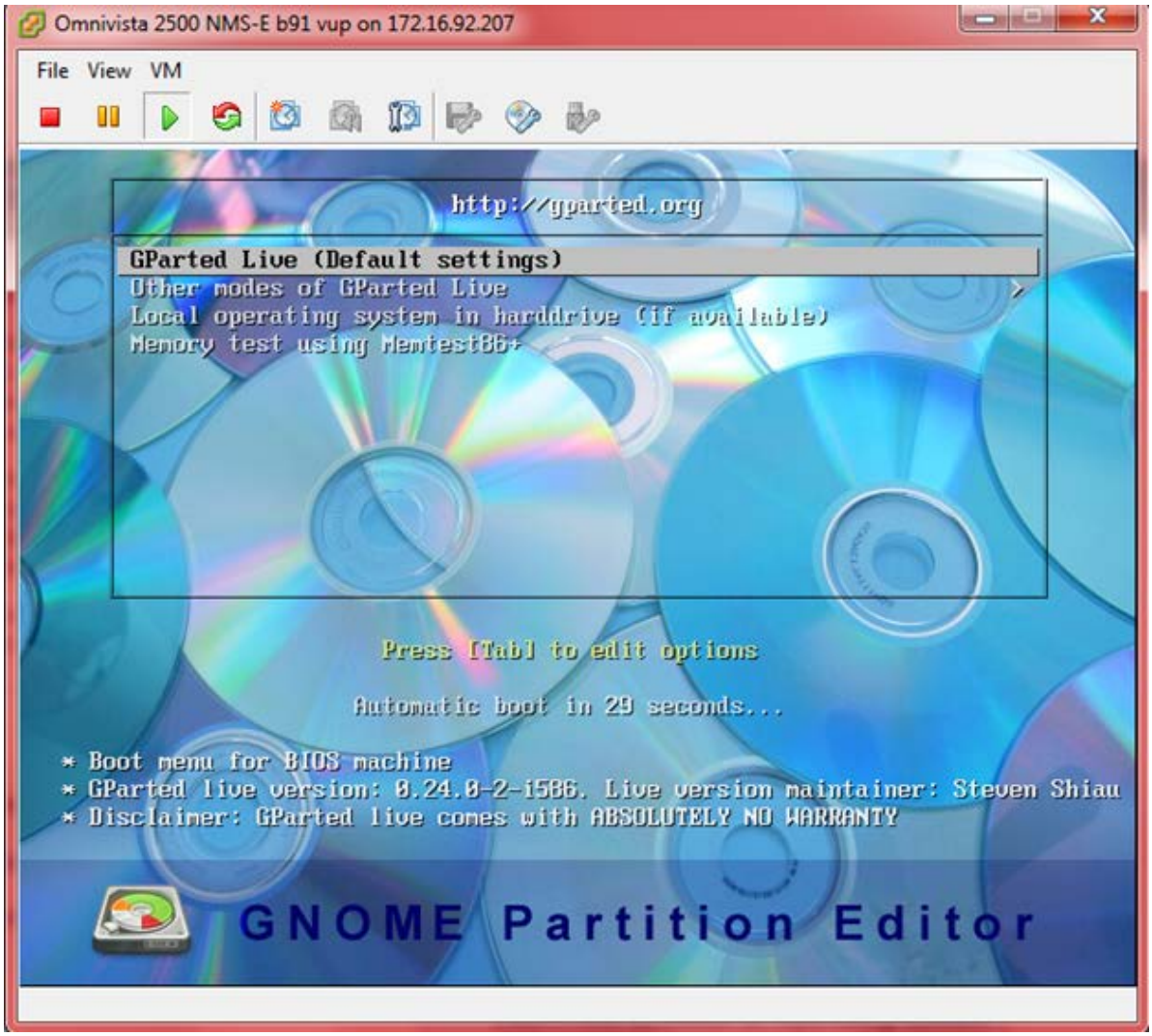


Step 11: Wait for the process to finish, then reboot the VA.





Once the VA is rebooted, the main GParted Screen will appear.



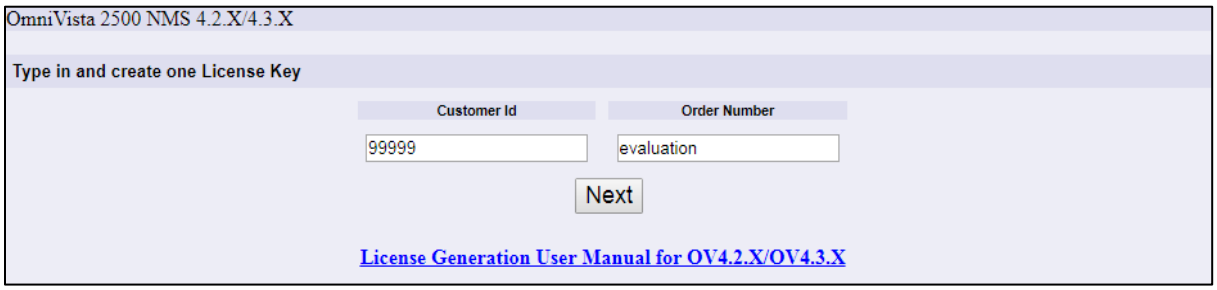
Step 12. Reboot from the local drive. Select **Local operating system in hard drive**, and press **Enter**. The system will reboot from the local drive and the new disk partition size will take effect.

Note: To prevent the VA from loading from GParted on the next reboot, can change the boot order from the BIOS as shown in steps 4 – 5 above; or reset the CD/DVD drive 1 Device Type to **Host Device** by right-clicking on the VA to bring up the Virtual Machine Properties Screen.

Appendix E – Generating an Evaluation License

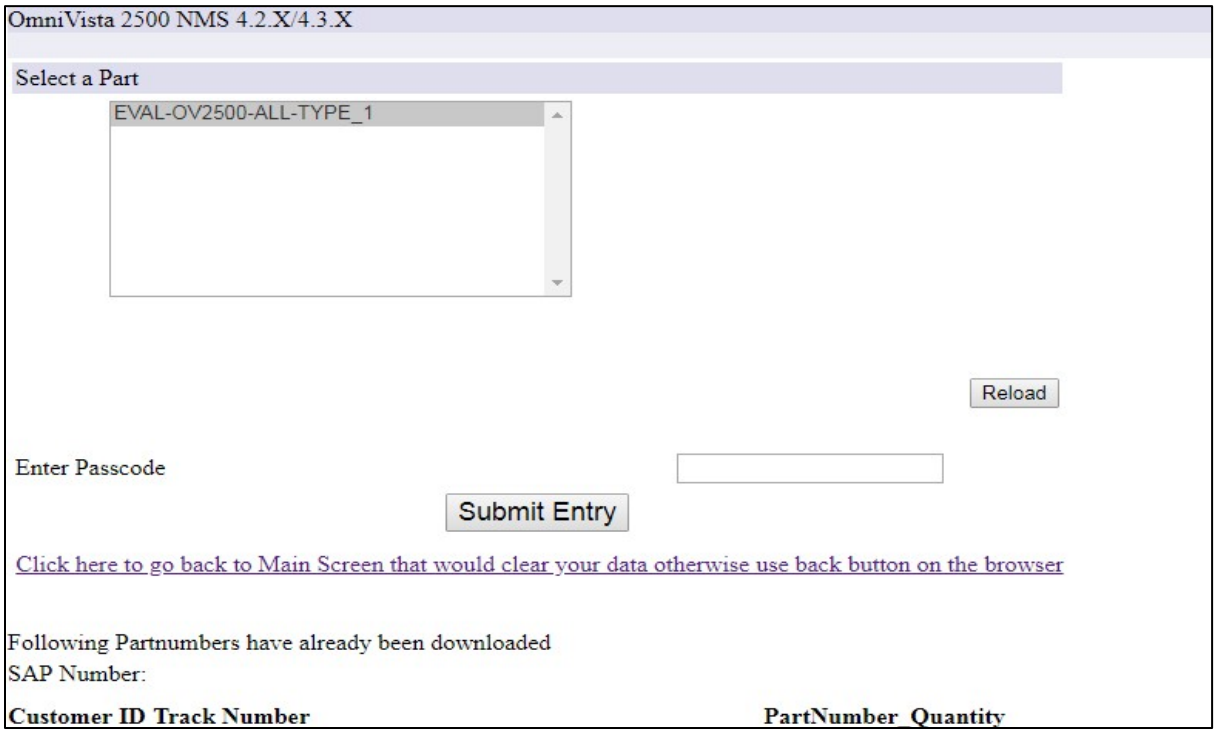
An Evaluation License provides full OV 2500 NMS-E 4.3R1 feature functionality, but is valid only for 90 Days (starting from the date the license is generated). There is one file that contains all of the Device (AOS, Third-Party, Stellar APs) and Service Licenses (VM, Guest, BYOD). Follow the steps below to generate an Evaluation License Key.

1. Go to https://lds.al-enterprise.com/ov25411/enterLicenseData.jsp

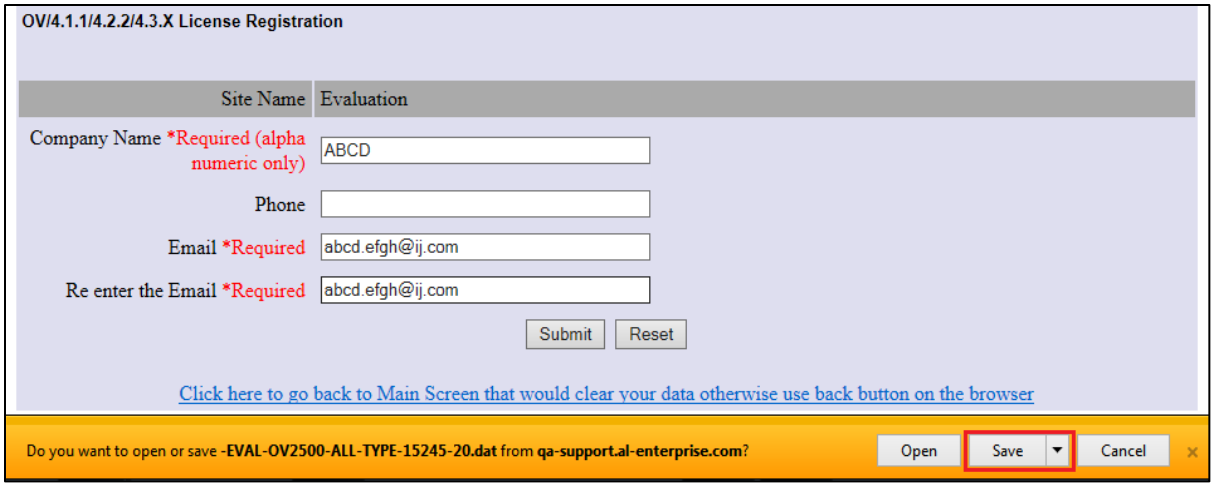


3. Enter the **Customer ID** and **Order Number**, then click **Next**.

- **Customer ID –** 99999
- Order Number – evaluation



4. Select the License Type (EVAL-OV2500-ALL-TYPE_1). Enter **omnivista** in the **Enter Passcode** field, and click on the **Submit Entry** button.



5. Complete all of the required fields on the License Registration Form and click **Submit**, then click **Save** at the confirmation prompt to download the license to your computer.

6. Go to the **License – Add/Import License Screen** in OmniVista to import the license file you just downloaded.