

**Installation and Upgrade Guide
for
OmniVista 2500 NMS Enterprise
Version 4.2.2.R01**



August 2017

Revision A

Part Number 033226-00

READ THIS DOCUMENT

**OmniVista 2500 NMS
for**

VMware ESXi: 5.5, 6.0, and 6.5

VirtualBox: 5.0.10

MS Hyper-V: 2012 R2 and 2016

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

Table of Contents

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation Guide	1
Installing OV 2500 NMS-E 4.2.2.R01	2
Deploying the Virtual Appliance in VMware ESXi	2
Deploying the Virtual Appliance in VirtualBox	10
Deploying the Virtual Appliance in Hyper-V	15
Completing the OmniVista 2500 NMS-E 4.2.2.R01 Installation.....	20
Upgrading From OV 2500 NMS-E 4.2.1.R01 (MR2).....	24
Appendix A – Installing Virtual Box.....	A-1
Supported Hosts	A-1
Installing Virtual Box on Windows Hosts	A-1
Installing Virtual Box on Linux Hosts	A-2
Installing Virtual Box From a Debian/Ubuntu Package.....	A-2
Using the Alternative Installer (VirtualBox.run)	A-3
Performing a Manual Installation	A-3
Appendix B – Using the Virtual Appliance Menu	B-1
Help.....	B-2
Configure the Virtual Appliance	B-2
Help.....	B-3
Display Current Configuration.....	B-3
Configure OV IP & OV Ports.....	B-3
Configure UPAM Portal IP & Ports	B-4
Configure Default Gateway.....	B-5
Configure Hostname.....	B-5
Configure DNS Server.....	B-6
Configure Timezone	B-6
Configure Route	B-7
Configure Network Size.....	B-8
Configure Keyboard Layout.....	B-8
Update OmniVista Web Server SSL Certificate	B-10
Configure NTP Client.....	B-11
Configure Proxy.....	B-11
Change Screen Resolution.....	B-12
Configure the Other Network Cards.....	B-12
Exit	B-13
Run Watchdog Command	B-13
Upgrade VA.....	B-14
Change Password	B-16
Logging	B-17
Login Authentication Server.....	B-18
Power Off	B-18
Reboot	B-18
Advanced Mode	B-18
Set Up Optional Tools	B-19
Log Out	B-20

Table of Contents (continued)

Appendix C – Extending the VA Partition Size	C-1
Appendix D – Generating an Evaluation License	D-1

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

This document details the OmniVista 2500 NMS Enterprise 4.2.2.R01 (OV 2500 NMS-E 4.2.2.R01) installation/upgrade process. OV 2500 NMS-E 4.2.2.R01 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 4.2.1.R01 MR2](#) using the OmniVista 2500 NMS Software Repository.

If you are upgrading from an earlier release (3.5.7 – 4.2.1.R01(MR1)), you must first upgrade to 4.2.1.R01 MR2. The Upgrade Matrix below shows the upgrade paths that must be followed to get to 4.2.1.R01 MR2. Click on the links below to download the applicable *OmniVista 2500 NMS Installation Guide* or go to the *application* section in this document for details.

OmniVista 4.2.2.R01 Upgrade Matrix to OV 4.2.1 (MR2)

From	To	
	OV 4.2.1 R01-GA (Build 69)	OV 4.2.1 R01-MR2 (Build 94)
OV 3.5.7	Direct Upgrade	Step 1: Upgrade to OV 4.2.1 R01-GA Step 2: Automatic upgrade to MR2 from VA Menu
OV 4.1.1 R01	Step 1: Upgrade to OV 4.1.2.R02 Step 2: Upgrade to OV 4.1.2 R03* Step 3: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2.R02 Step 2: Upgrade to OV 4.1.2 R03* Step 3: Upgrade to OV 4.2.1 R01-GA* Step 4: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R01	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA* Step 3: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R02	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA*	Step 1: Upgrade to OV 4.1.2 R03* Step 2: Upgrade to OV 4.2.1 R01-GA* Step 3: Automatic upgrade to MR2 from VA Menu
OV 4.1.2 R03	Direct Upgrade*	Step 1: Upgrade to OV 4.2.1 R01-GA Step 2: Automatic upgrade to MR2 from VA Menu
OV 4.2.1 R01-GA (Build 69)		Step 1: Automatic upgrade to MR2 from VA Menu
OV 4.2.1 R01-MR1 (Build 85)		Step 1: Automatic upgrade to MR2 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*.

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 4.2.2.R01

OV 2500 NMS-E 4.2.2.R01 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 4.2.2.R01 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: 5.0.10
- MS Hyper-V: 2012 R2 and 2016.

The sections below detail each of the steps required to deploy OV 2500 NMS-E 4.2.2.R01 as Virtual Appliance on [VMware](#), [VirtualBox](#), and [Hyper-V](#). If you are upgrading from OV 2500 NMS-E 4.2.1.R01 (MR2), see [Upgrading from OV 2500 NMS-E 4.2.1.R01 MR2](#).

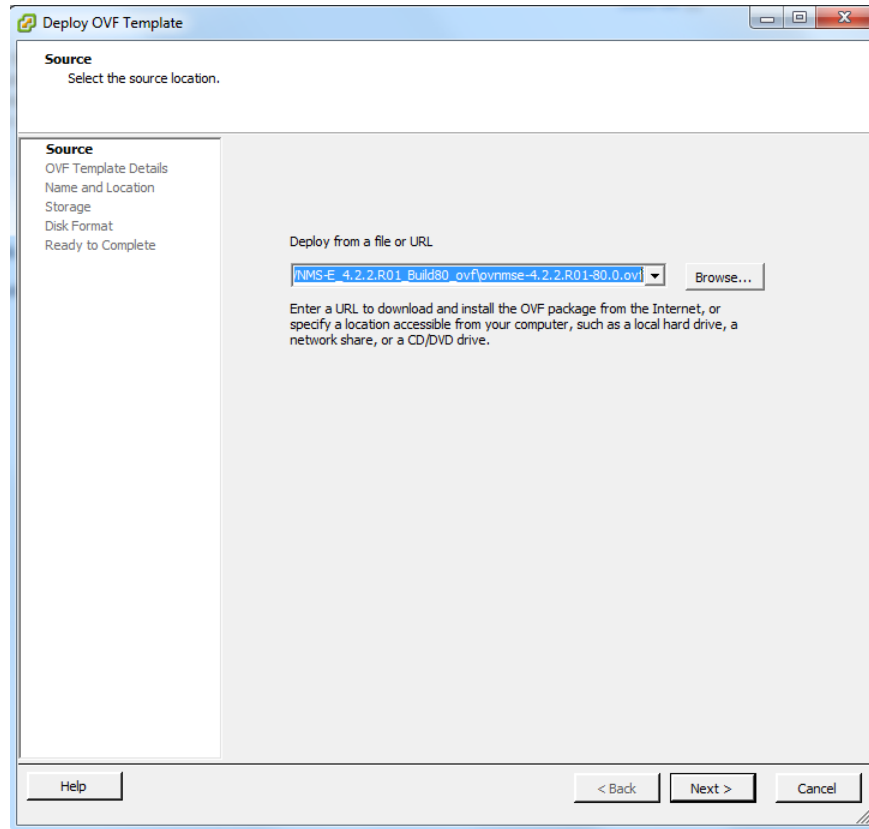
Note: If you are deploying OV 2500 NMS-E 4.2.2.R01 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See [Appendix A](#) for details.

Deploying the Virtual Appliance in VMware ESXi

Note that in the instructions below, vCenter is used for demonstration purposes.

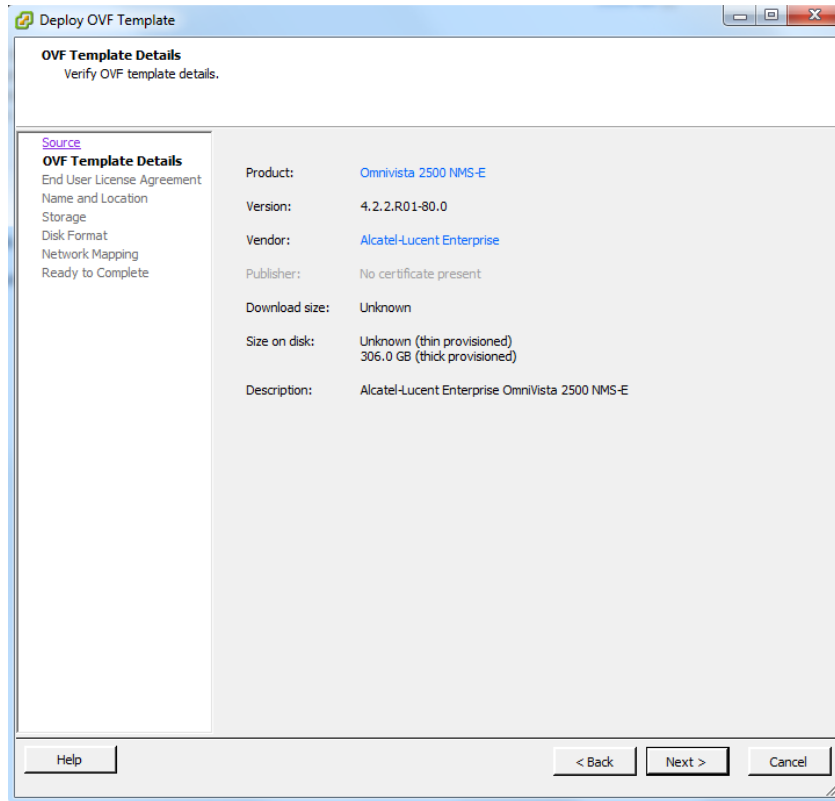
1. Download and unzip the OVF package.
2. Log into vCenter and open the vSphere client.
3. Select the Host on which you want to install OV 2500 NMS-E 4.2.2.R01, click on **File - Deploy OVF Template**. The Deploy OVF Template Wizard appears.

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

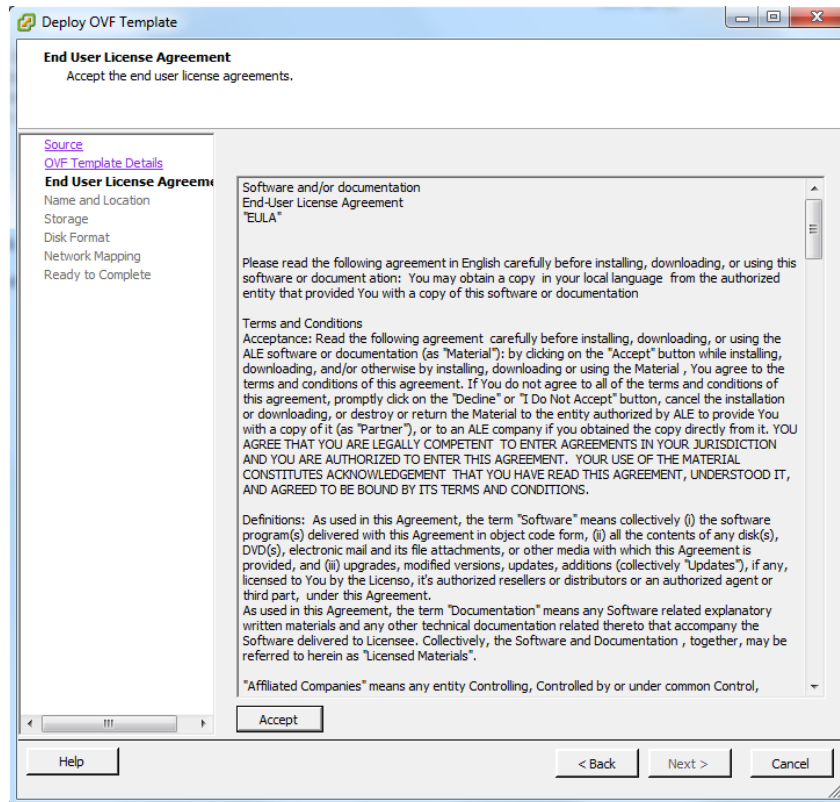


4. Click on the **Browse** button and locate the OV 2500 NMS-E 4.2.2.R01 Application file in the unzipped OVF folder (e.g., ovnmse-4.2.2.R01-80.0.ovf).
5. Select the file and click **Open** (or double click on the file). The file will appear in the “Deploy from a file or URL” field. Click **Next**. The OVF Template Details Screen appears.

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

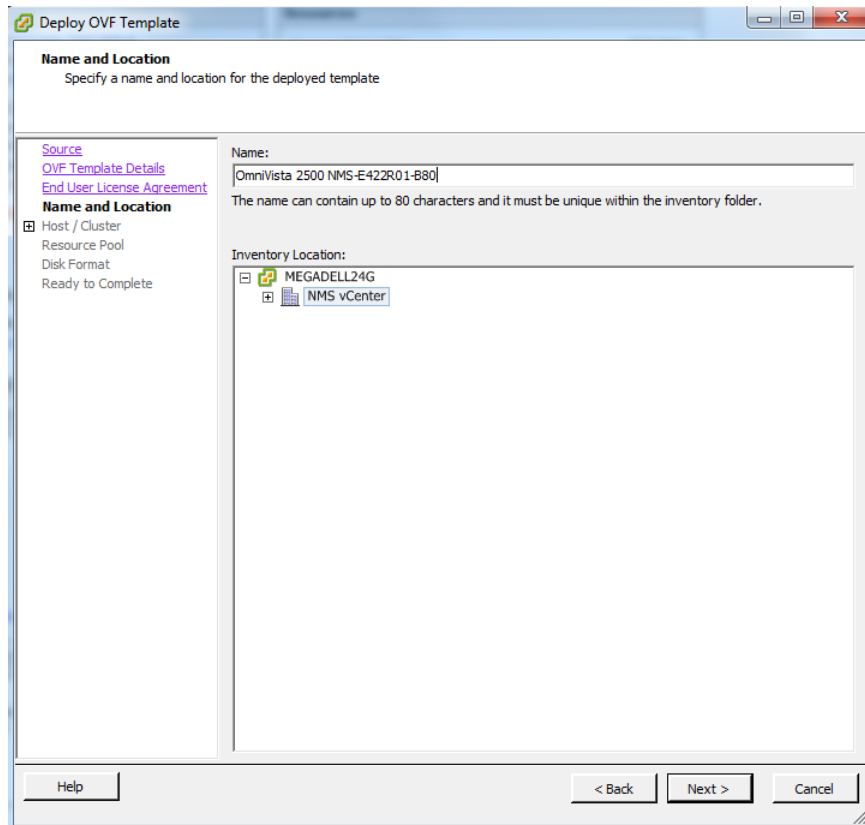


6. Review the OVF details and click **Next**. The End User License Agreement Screen appears.



OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

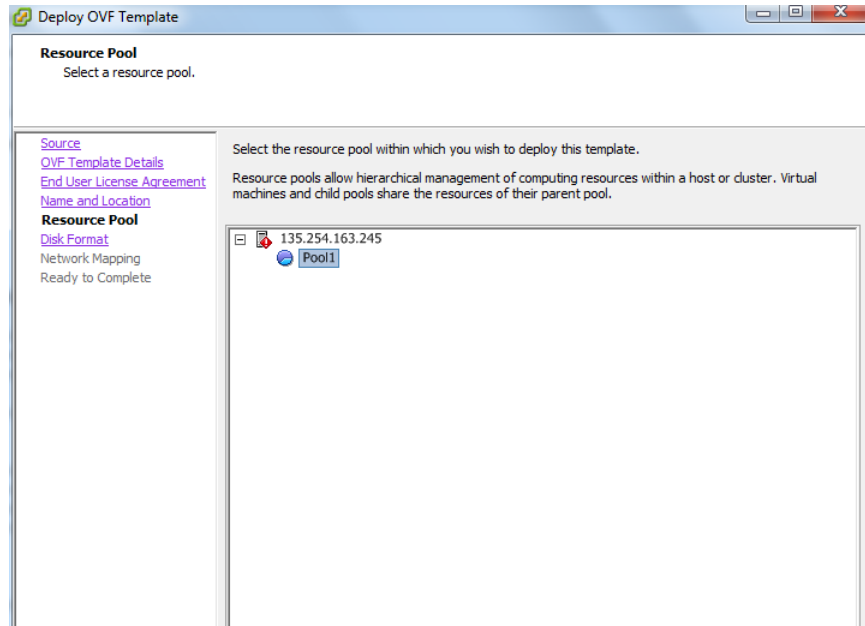
7. Review the License Agreement, click **Accept**, then click **Next**. The Name and Location Screen appears.



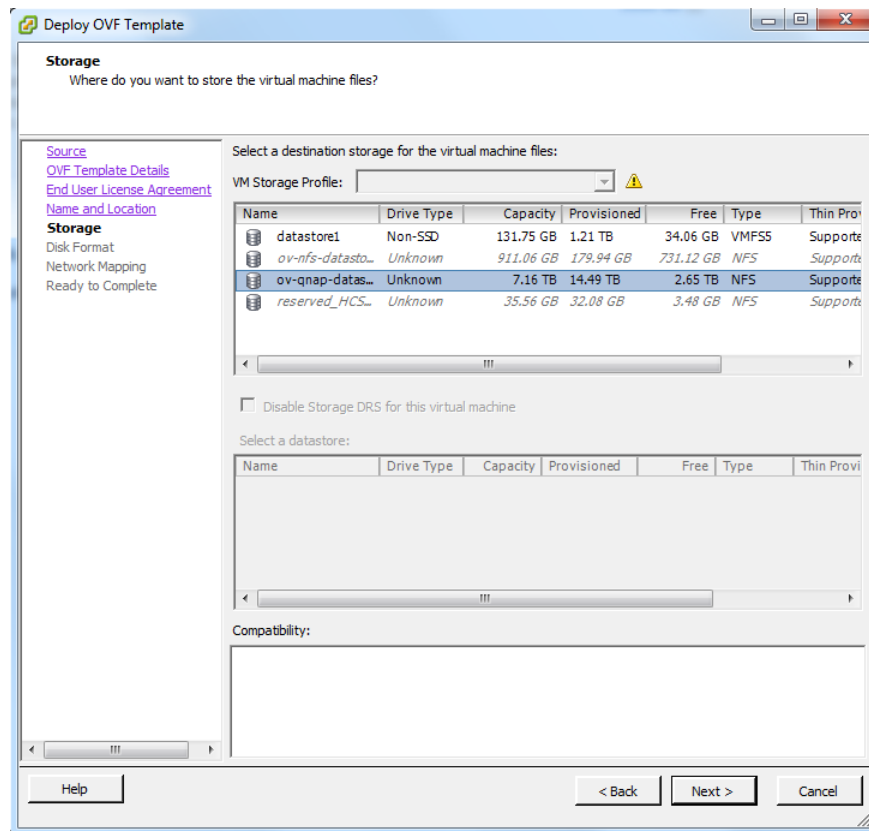
8. Specify a Name and Inventory Location for the deployed template (e.g., OmniVista 2500 NMS-E422R01-Build80), then click **Next**.

9. If you have configured a Resource Pool, the Resource Pool Screen (below) appears. Select the host server and click **Next**.

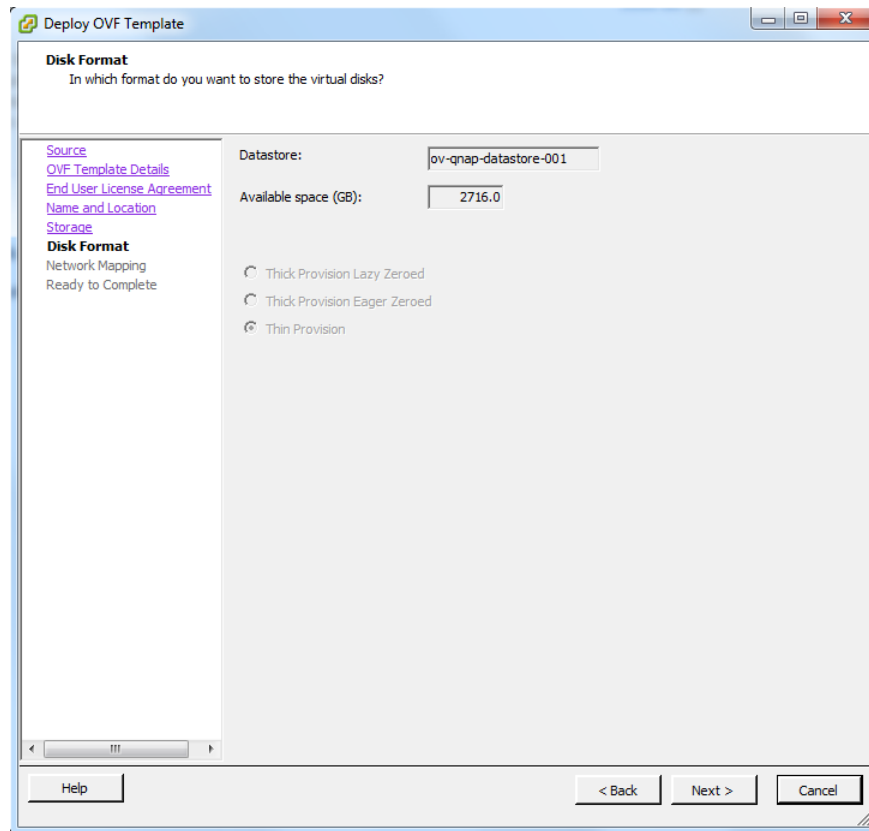
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



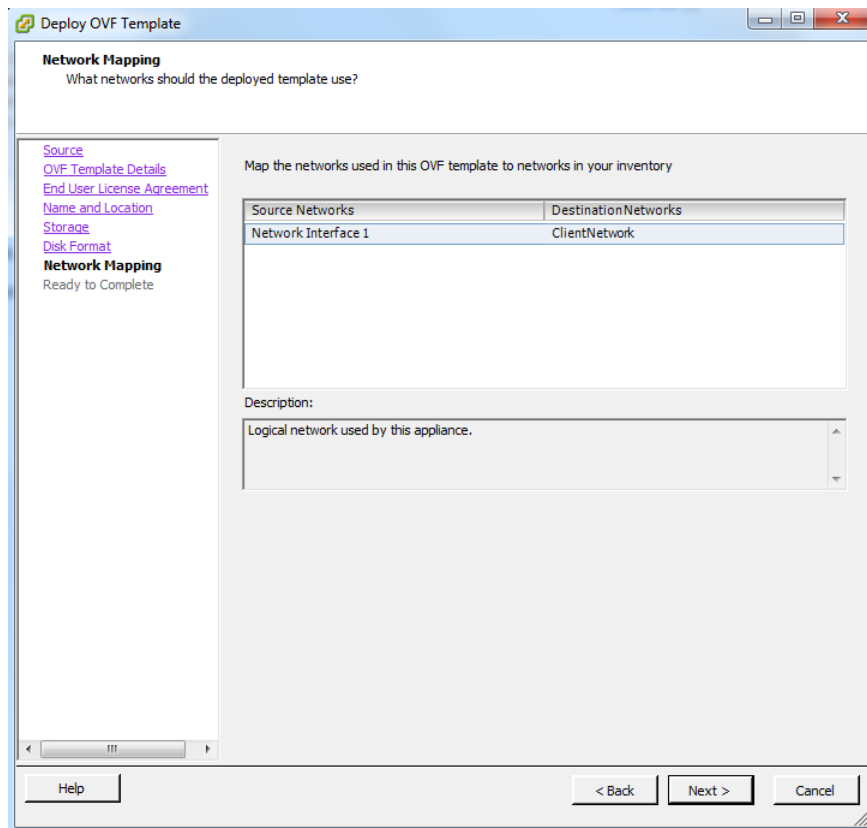
If a host server only has storage configured, the Disk Format Screen will appear. If you have multiple storage locations configured, the Storage Screen (below) appears. Select the destination storage where the template is to be deployed, then click **Next**.



The Disk Format Screen appears.



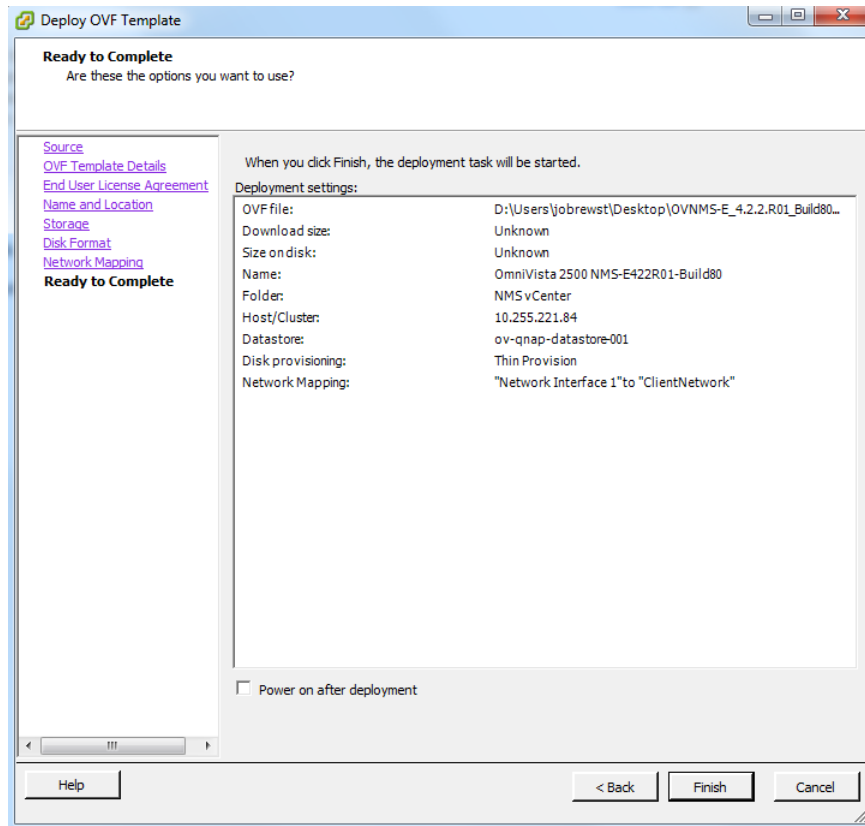
10. Select **Thin Provision**, then click **Next**. The Network Mapping Screen appears.



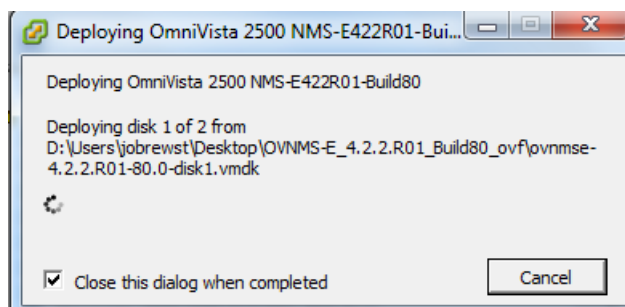
11. Select network that the deployed OVF template will use, then click **Next**. The Ready to Complete Screen appears.

Note: If multiple networks are configured/available, select the network on the screen. Make sure that you select the correct Destination Network.

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



12. Review the configuration and click **Finish**. (You can select the “Power on after deployment” option to automatically power on the VA when deployment is complete.) A status window appears and displays the progress of the deployment. If you select the “Close this dialog when completed” option, the progress window will automatically close when the deployment is complete. If not, click **Close** at the completion of the deployment to close the window.



13. If the new Virtual Appliance was not powered on via the deployment wizard, power on the VM now. Right-click on the VM in the Navigation Tree and select **Power - Power On**.

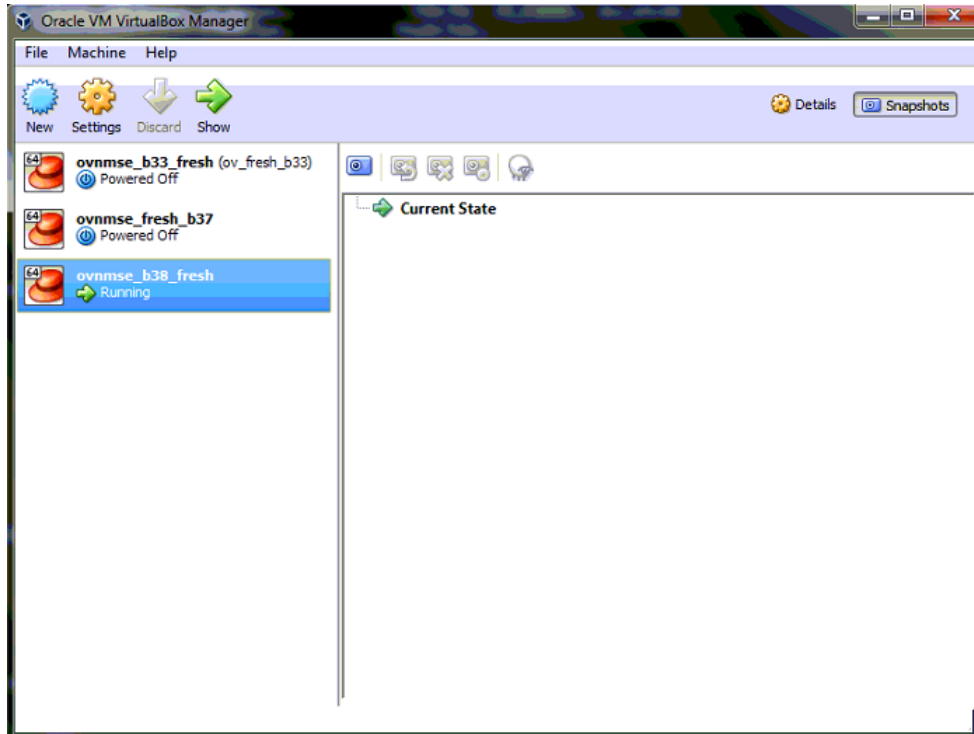
Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.2.R01 Installation](#) to complete the installation.

Deploying the Virtual Appliance in VirtualBox

Note that in the instructions below, VirtualBox 5.0.10 in Windows 7 is used for demonstration purposes. The screens shown may depict an older OmniVista Release.

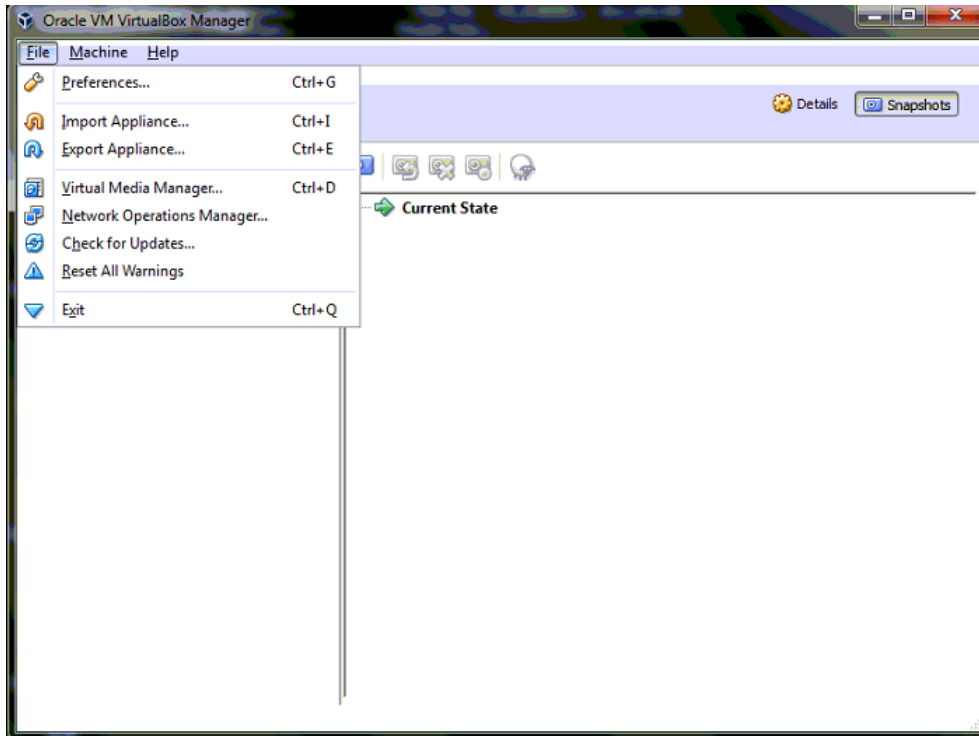
Note: If you are deploying OV 2500 NMS-E 4.2.2.R01 on a standalone Windows or Linux machine, you must first install Virtual Box on the machine. Virtual Box is available as a free download. See [Appendix A](#) for details.

1. Download and unzip the OVF package.
2. Log into Windows 7 and open the Oracle VM VirtualBox tool.

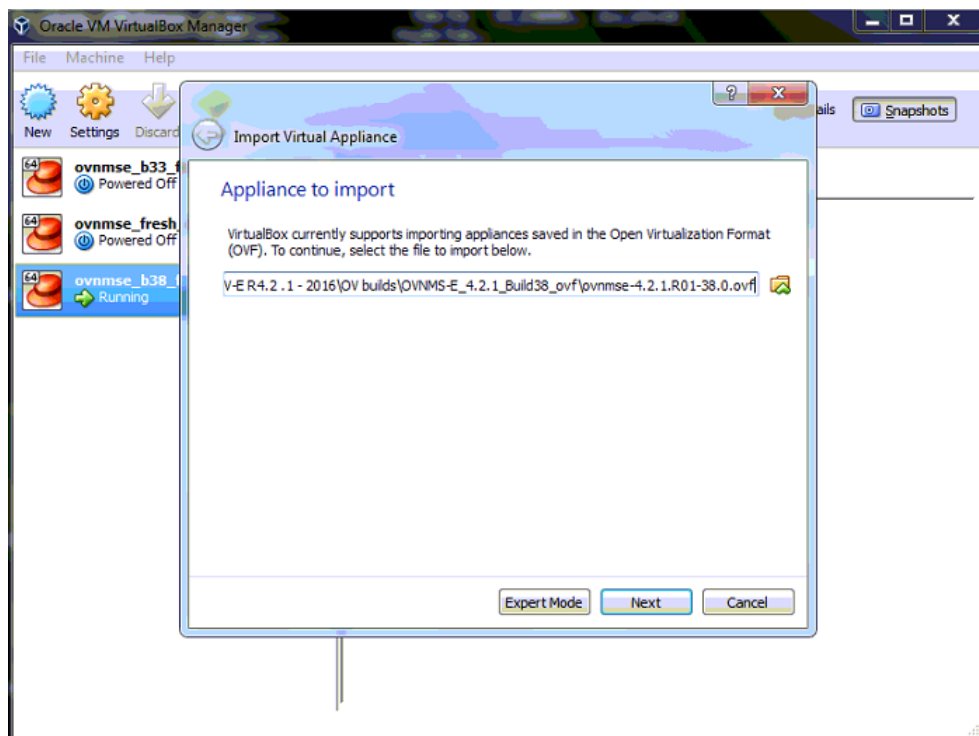


3. Click **File > Import Appliance**.

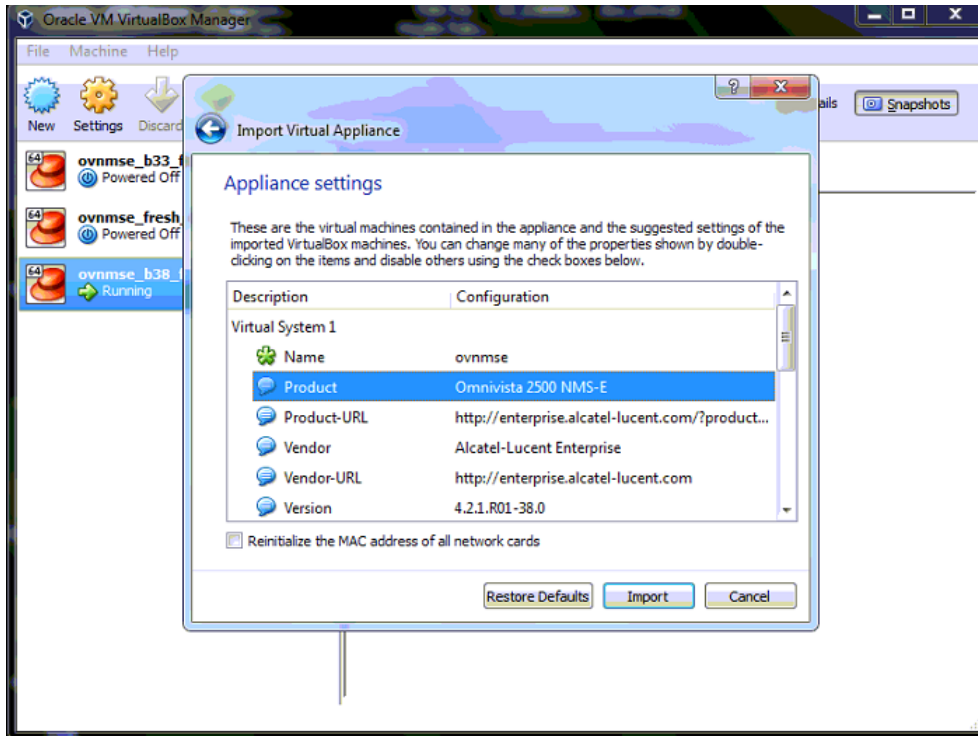
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



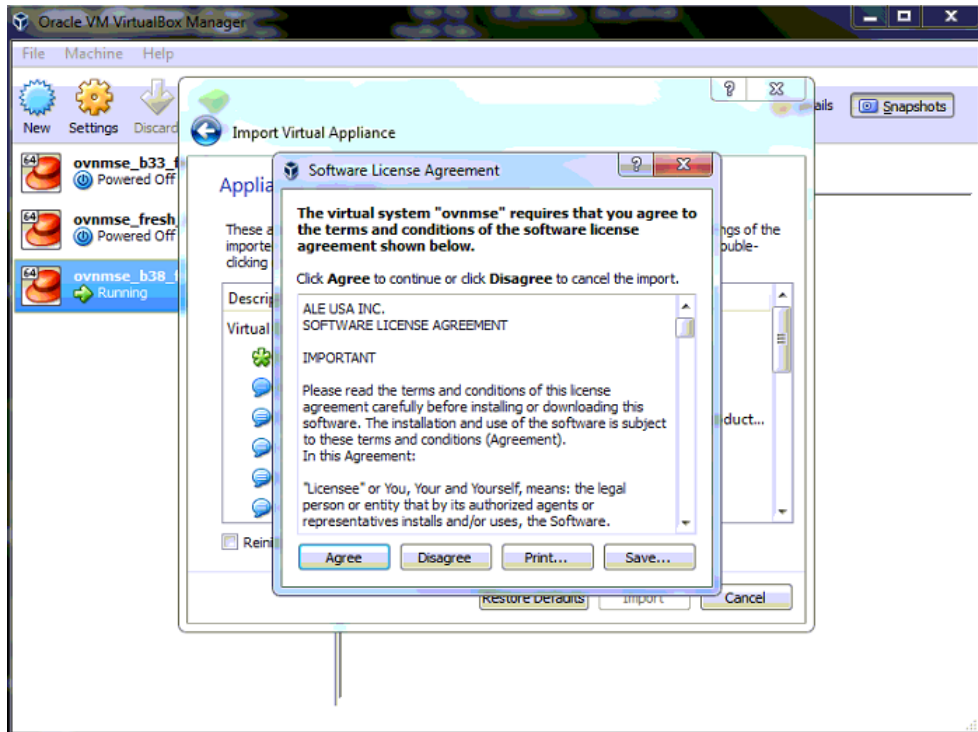
4. Click **browse** icon then select the **folder** which you extracted at step 1 above, then click **Next**.



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

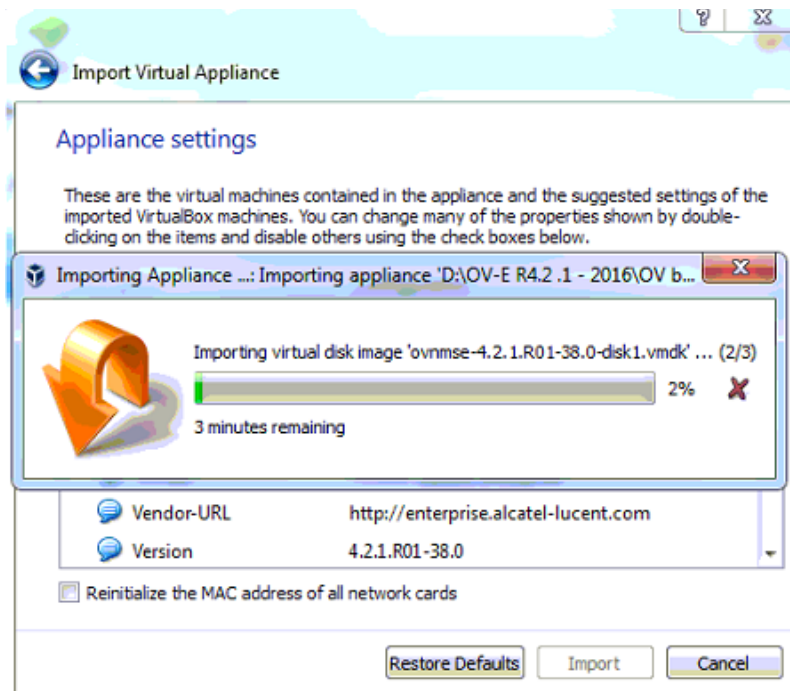


6. The **Software License Agreement** window displays, click on **Agree**.

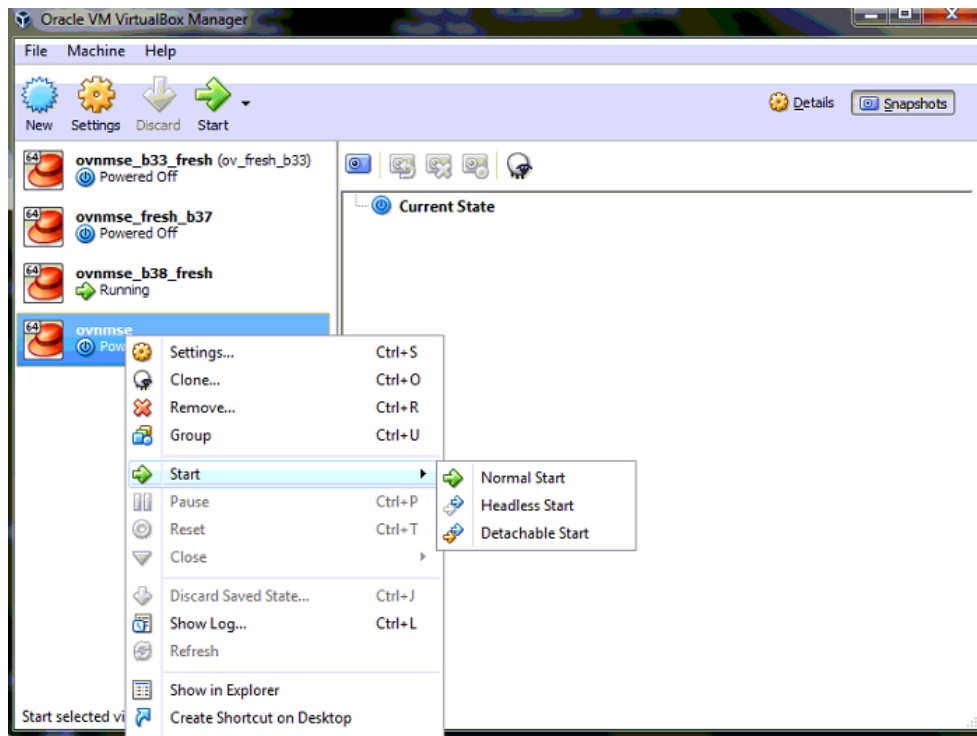


7. A status window appears and displays the progress of the deployment.

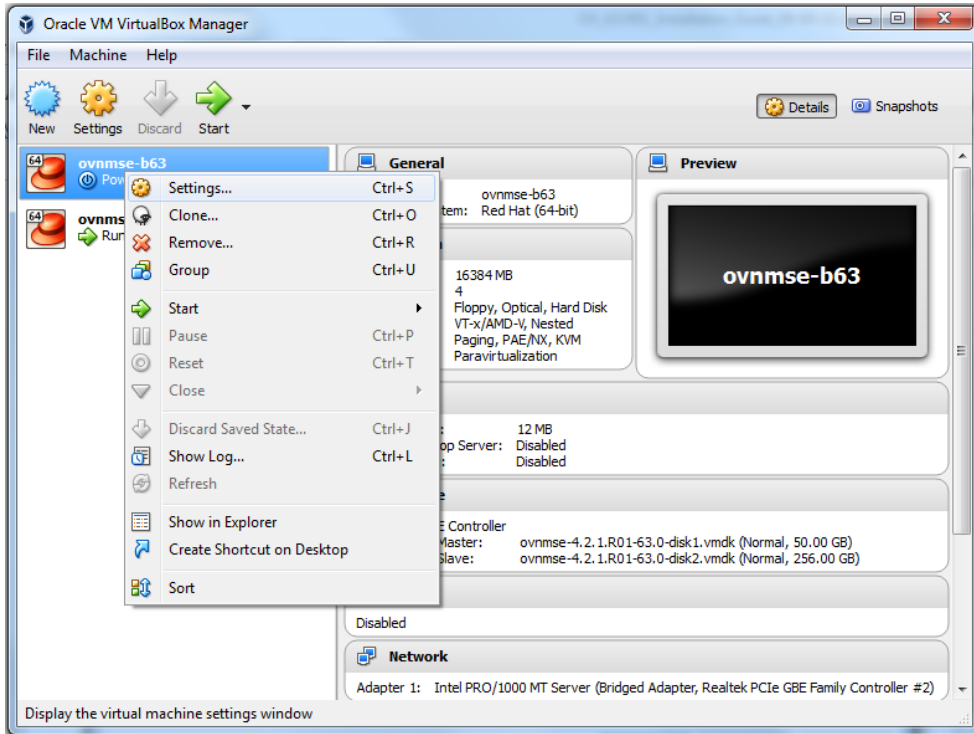
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



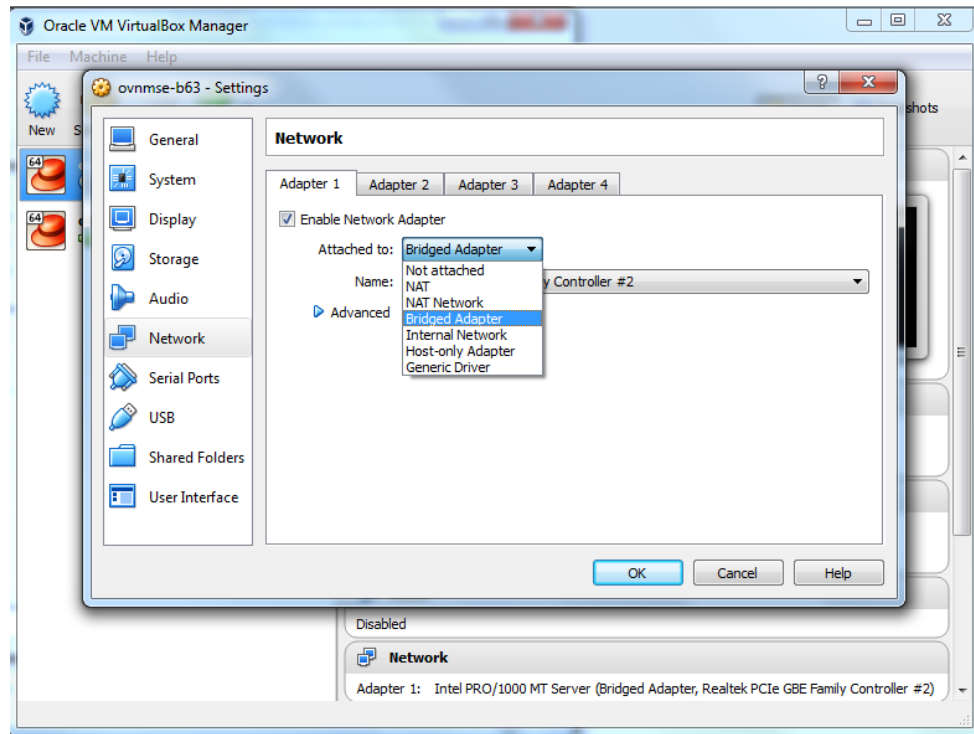
8. After the process is completed, right-click on the VM in the Navigation Panel and select **Start - Normal Start**.



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.

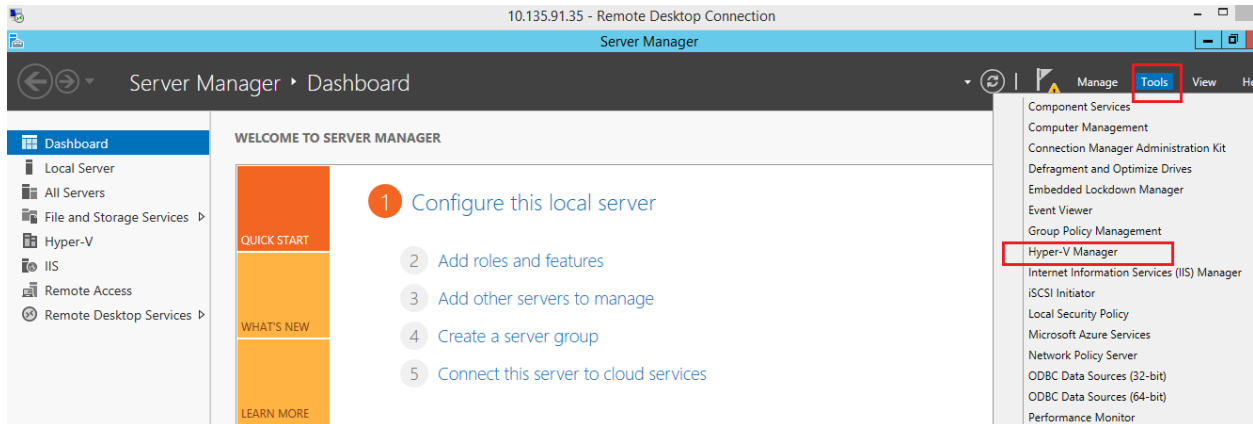


Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.2.R01 Installation](#) to complete the installation.

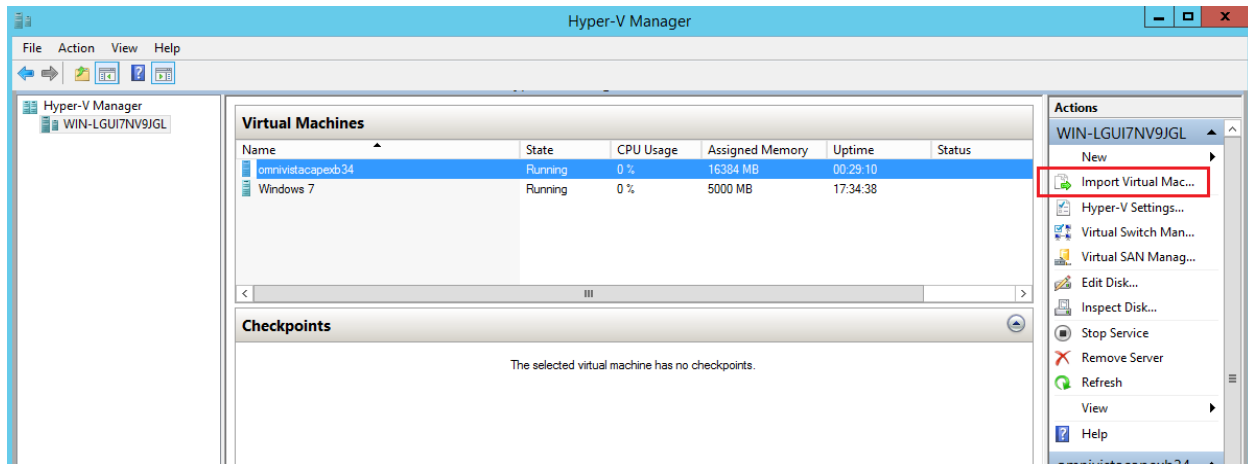
Deploying the Virtual Appliance in Hyper-V

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.

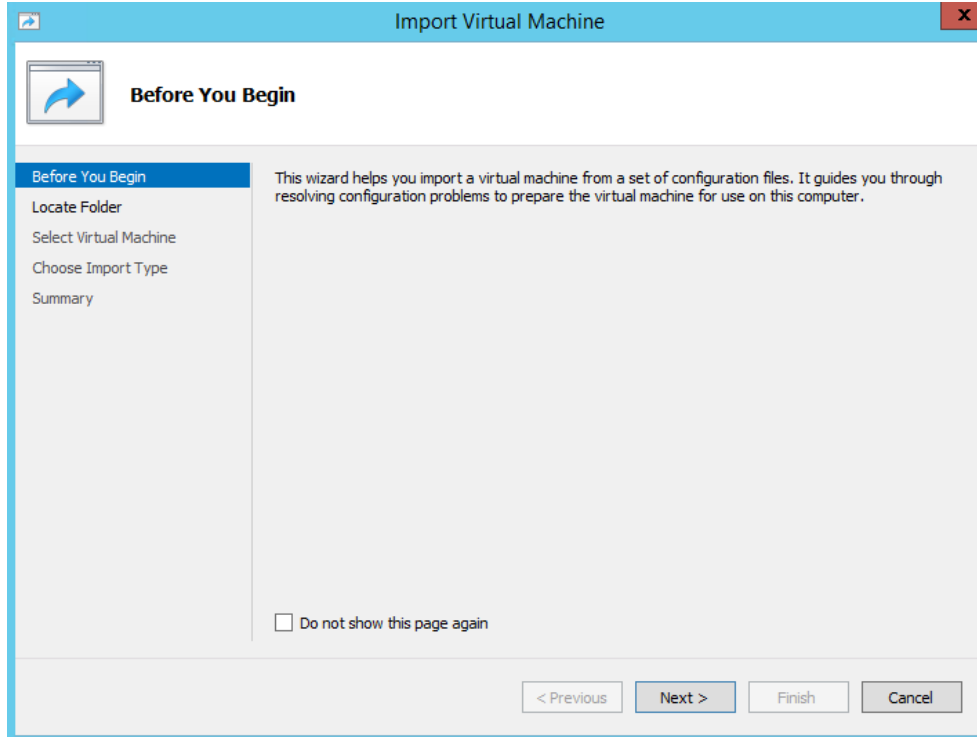
1. Download and unzip the OVF Hyper-V package.
2. Log into Windows 2012 and open the Hyper-V tool.



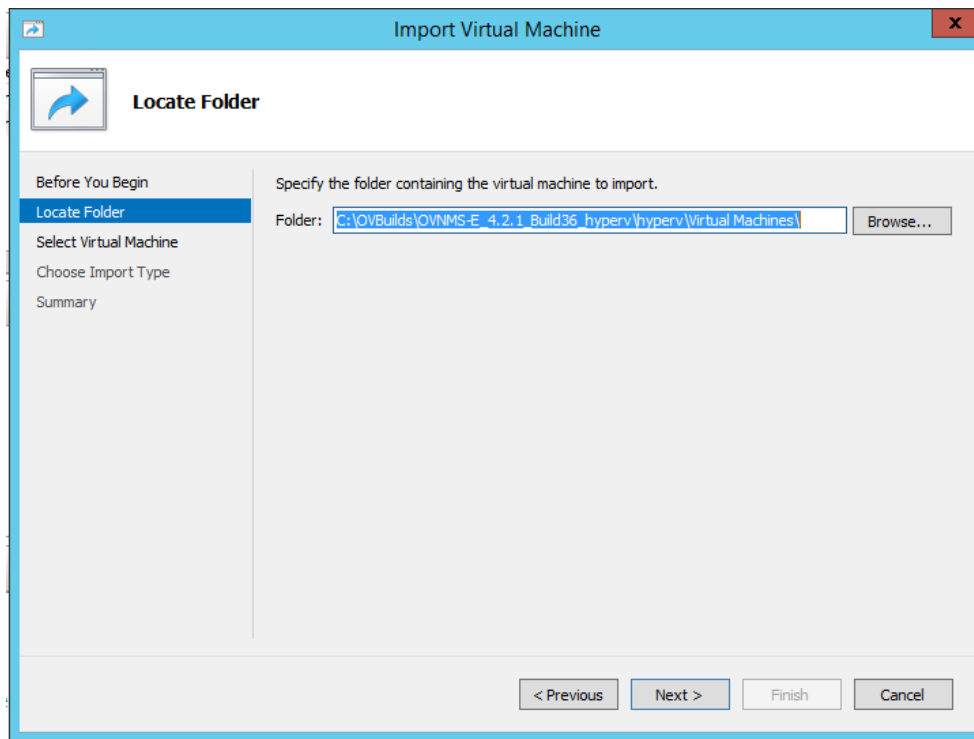
3. Select the Host on which you want to install OmniVista 2500 NMS, click on **Actions > Import Virtual Machine**.



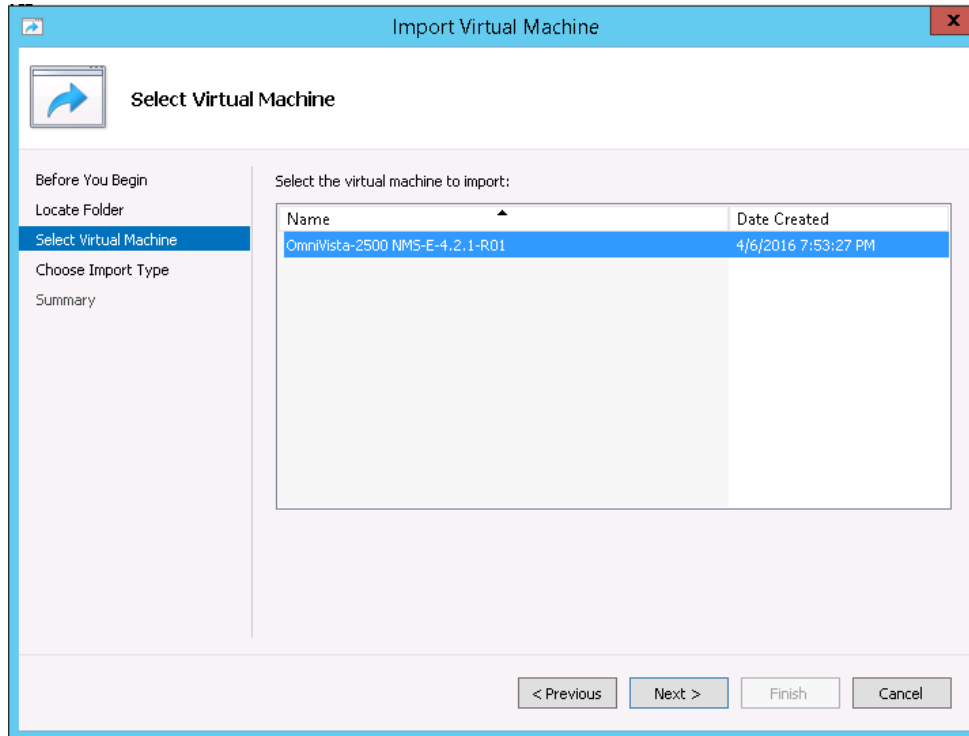
4. The Import Virtual Machine Wizard appears.



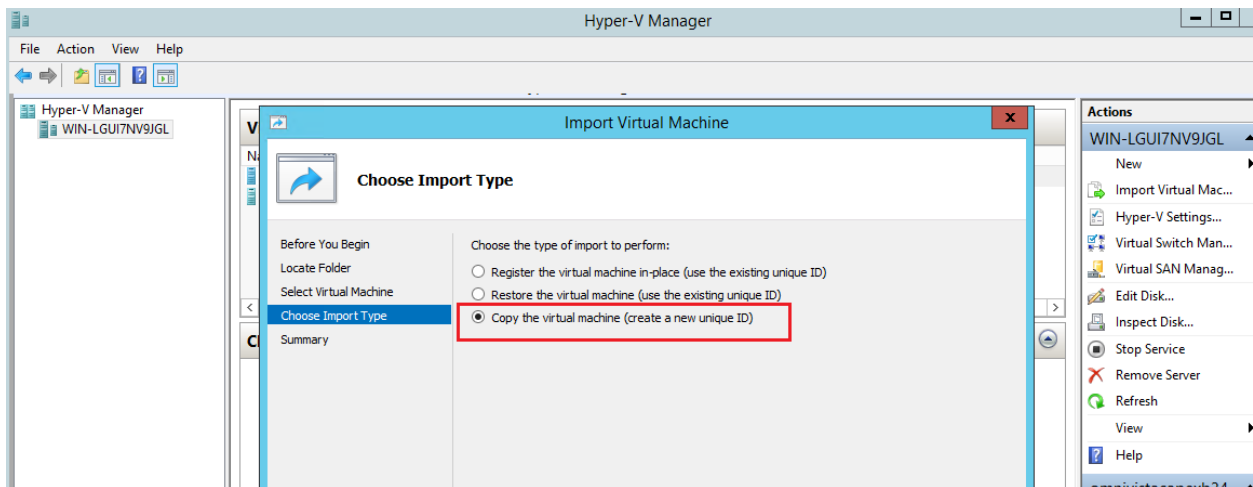
5. Click **Next** to go to the Locate Folder Screen, select the **Folder** that you extracted in Step 1, then click **Next**.



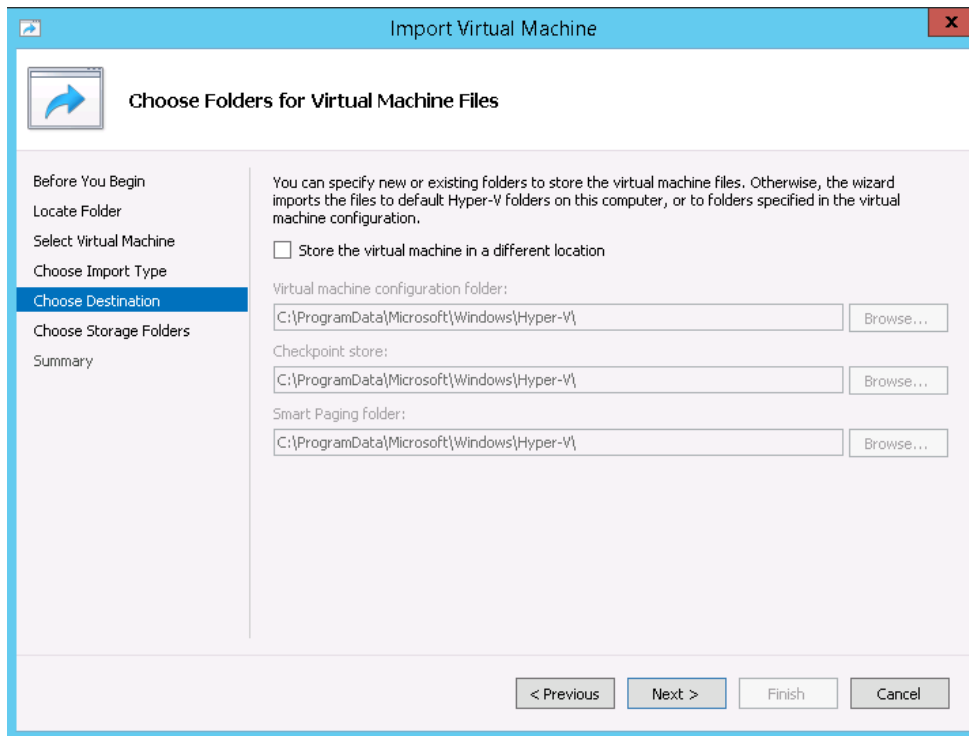
6. Select the Virtual Machine to import (Default = **OmniVista-2500 NMS-E-4.2.2.R01**), then click **Next**.



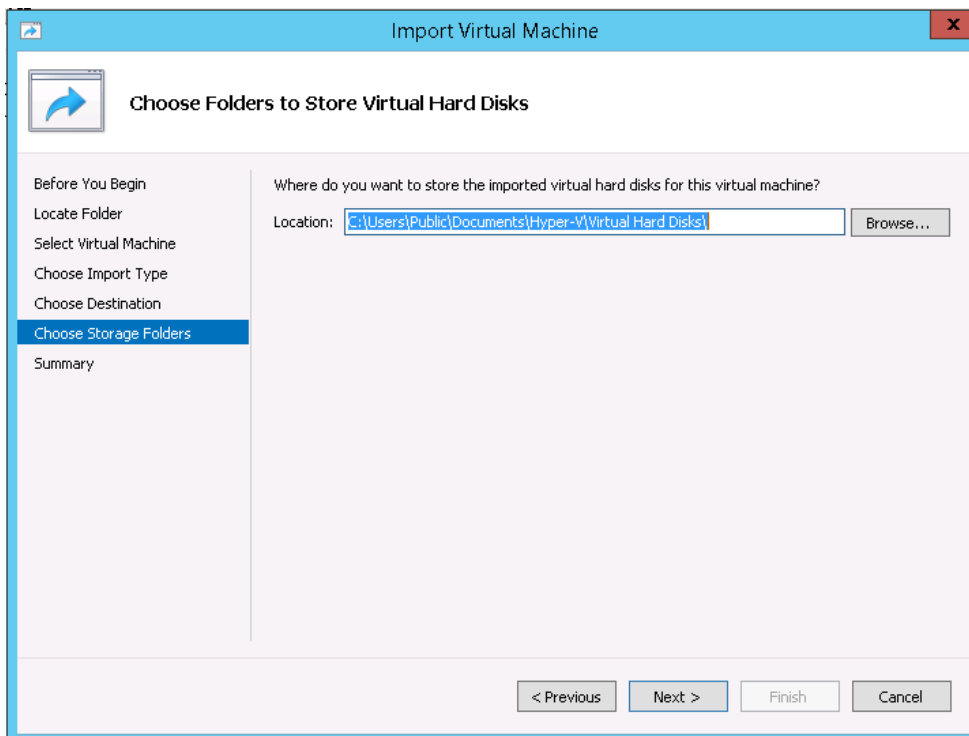
7. Select the default Import Type: **Copy the virtual machine (create a new unique ID)**, then click **Next**.



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



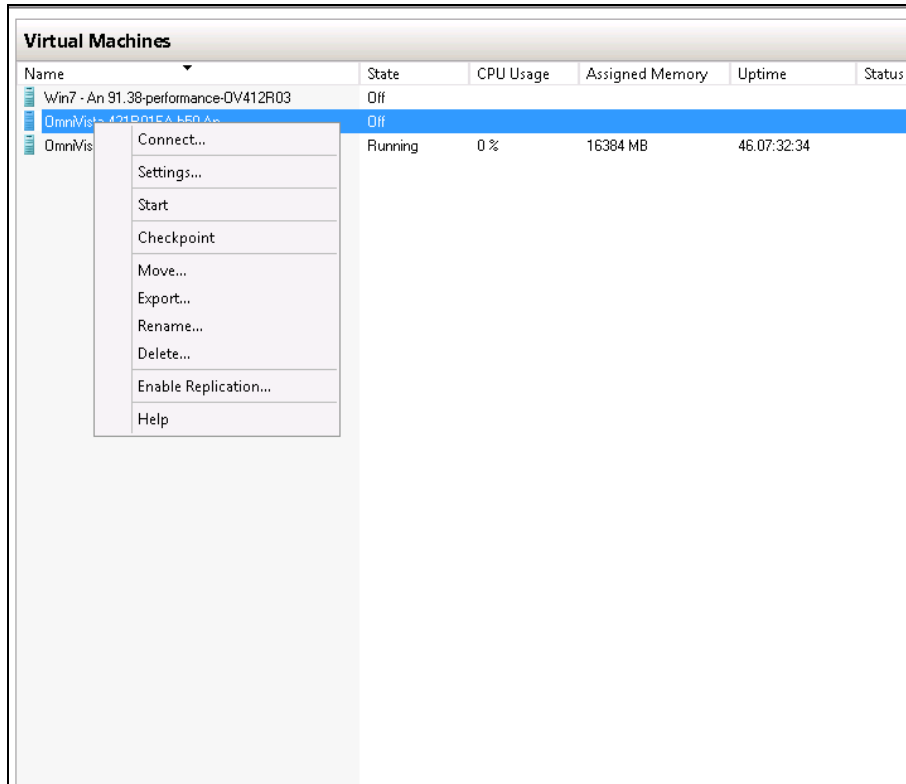
9. Choose folders to store the Virtual Hard Disks or accept the default location and click **Next**.



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

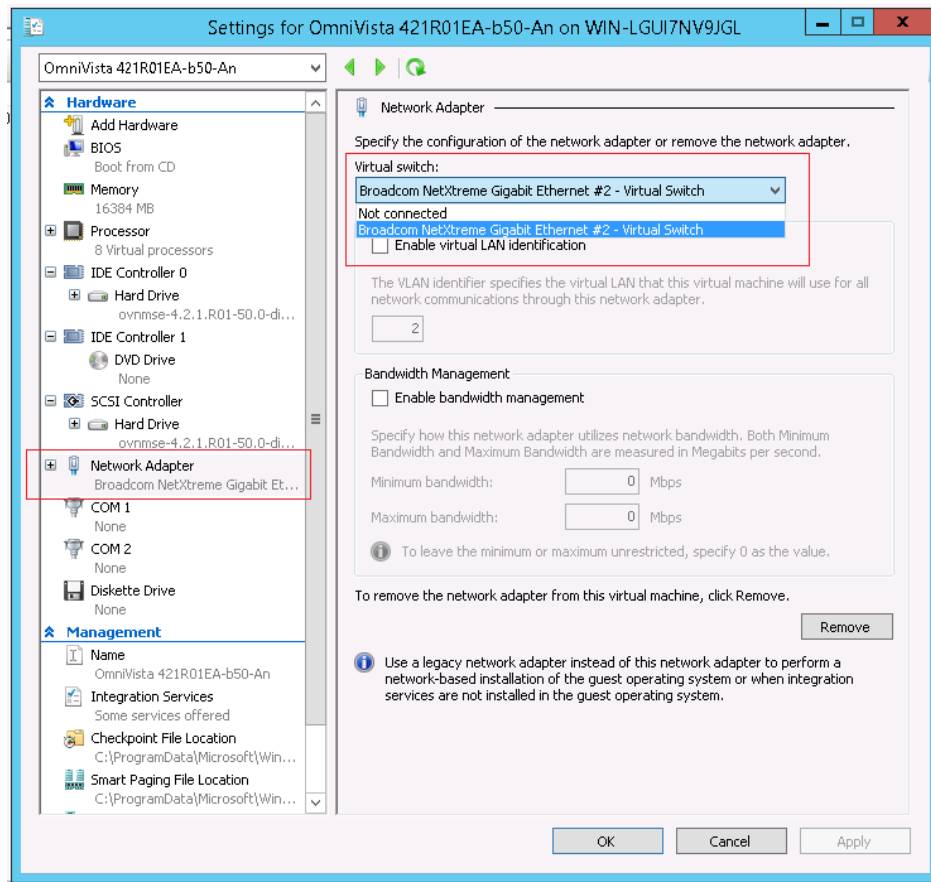
11. Configure the Network Adapter. Right-click on the VA and select **Settings**.

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



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

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



After the process is completed, right-click on the VM in the Navigation Panel and select **Start**. Once the Virtual Appliance is powered on, go to [Completing the OmniVista 2500 NMS-E 4.2.2.R01 Installation](#) to complete the installation.

Completing the OmniVista 2500 NMS-E 4.2.2.R01 Installation

Follow the steps in the following sections to complete the OV 2500 NMS-E 4.2.2.R01 installation.

1. Launch the Console for the new VM. (In vCenter, this can be done by right-clicking on the VM in the Navigation Tree and selecting **Open Console**.) The Keyboard Layout prompt will appear. Enter **n** if you do not want to change the default keyboard layout, enter **y** to change the default keyboard layout, then press **Enter**.

```
Regenerating ssh host keys...  
  
Configured Keyboard Layout: us  
Would you like to configure new Keyboard Layout [yin] (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 <= 32 characters
The new password must contain AT LEAST :
  a. one (1) letter (a-z)
  b. one (1) capitalized letter (A-Z)
  c. one (1) special character (%^*()-_+=[\{}:@#~,.?)
  d. and one (1) digit (0-9)
Enter new password: _
    
```

2. Specify a new administrative password, then re-enter to confirm the new password. Press **Enter** to configure System IP. Follow the guidelines on the screen when creating the password.

Important Note: Be sure to store the password in a secure place. Users 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
    
```

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

```

*****
* Configure OV IP
*****
(*) Please input OV IPv4: 10.255.221.19
Please input subnet mask [255.255.255.0]: 255.255.255.0
Would you like to configure:
  IPv4: 10.255.221.19
  subnet mask: 255.255.255.0
[yin] (y): y
The configuration has been set
Press [Enter] to continue
    
```

4. Enter an IPv4 address.

5. Enter the IPv4 network mask.

6. Enter **y** and press **Enter** to confirm, 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:
    
```

7. 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 **1** is selected in this step, UPAM IP and Ports configuration must be completed (Steps 8 – 9). If **2** is selected, go to Step 10.


```
(*) Please input UPAM Portal IPv4: 10.225.221.21
Please input UPAM Portal HTTP port [80]: 80
Please input UPAM Portal HTTPS port [443]: 443
Would you like to configure:
    UPAM Portal IP: 10.225.221.21
    UPAM Portal HTTP port: 80
    UPAM Portal HTTPS port: 443
[yin] (y): y
The configuration has been set
Press [Enter] to continue
```

8. Enter a UPAM IP address and UPAM HTTP and HTTPS ports. Note that the UPAM IP address **must** be different than the OV IP address.

9. Enter **y** and press **Enter** to confirm, then press **Enter** to continue.

10. The **Memory Configuration Based on Network Size** option is displayed.

```
*****
* Memory Configuration Based on Network Size
*****
Choose the number of devices:
[1] Low (lower than 500)
[2] Medium (500-2000)
[3] High (2000-5000)
[4] Very High (5000-10000)
(*) Type your option:
```

Select the number of devices OV 2500 NMS-E 4.2.2.R01 will manage. To select a range, enter its corresponding number at the command prompt (e.g., enter **2** for Medium). Ranges include:

- Low (fewer than 500 devices, 5,000 wireless clients)
- Medium (500 to 2,000 devices, 10,000 wireless clients)
- High (2,000 to 5,000 devices, 20,000 wireless clients)
- Very High (5,000 to 10,000 devices, 25,000 wireless clients).

Enter **y** and press **Enter** to confirm, then press **Enter** to display 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] Update OmniVista Web Server SSL certificate
* [13] Configure NTP Client
* [14] Configure Proxy
* [15] Change screen resolution
* [16] Configure the other Network Cards
* [0] Exit
*****
```

11. Enter **2** and press **Enter** to display the current configuration.

```

*****
* Current configuration
*****
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.2.R01 GA
Build Number: 80
Patch Number: 0
Build Date: 08/04/2017
WMA Version: 3.0.9.10
UPAM Version: 3.0.27.15

OV IPv4 Address: 10.255.221.19
NetMask: 255.255.255.0
OV Web HTTP Port: 80
OV Web HTTPS Port: 443

UPAM Portal IPv4 Address: 10.225.221.21
UPAM Portal Web HTTP Port: 80
UPAM Portal Web HTTPS Port: 443

Default Gateway v4:

Hostname: omnivista

Timezone: America/Los_Angeles

Data LUM Size: 256G
Data LUM Available (Free) Space: 237G

Network Size: Low (lower than 500) devices

Proxy Status: Disabled
Proxy is not set

Press [Enter] to continue

```

The current OV appliance configuration is displayed. You can go to the Configure The Virtual Appliance Menu to configure additional settings (e.g., Default Gateway, Proxy, DNS) that may be required to access OV 2500 NMS-E 4.2.2.R01 and perform upgrades. Please configure other settings as required. See [Appendix B](#) for VA Menu information.

Note: OV 2500 NMS-E 4.2.2.R01 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 4.2.2.R01 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

12. Press **Enter**. The Virtual Appliance Menu is displayed again.

13. After completing all required settings (and after all services are running), enter `https://<OVServerIPaddress>` in a supported browser to launch OV 2500 NMS-E 4.2.2.R01.

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>`).

14. 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.

Upgrading From OV 2500 NMS-E 4.2.1.R01 (MR2)

Follow the steps below to use the “Upgrade/Restore” option in the Virtual Appliance Menu to upgrade from OV 2500 NMS-E 4.2.1.R01 (MR2) to OV 2500 NMS-E 4.2.2.R01. Remember, if you are upgrading from an older version (3.5.7 or 4.2.1.R01 (MR1)), you must first upgrade to 4.2.1.R01 (MR2) before upgrading to 4.2.2.R01.

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 may take up to a day to purge the older data, but it is recommended as a way to save disk space.
- Note that Analytics Performance Monitoring statistics, the last failed backup reason in the Backup Summary report of Resource Manager, and the Scheduler Job Description on your current OV4.2.1.R01 (MR2) system will be lost after upgrading to OV4.2.2.R01. You can perform a .csv export of them prior to the upgrade for later reference. Please refer Release Notes for known issues.

Also note that OV 2500 NMS-E 4.2.2.R01 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**.

1. Open a Console on the OV 2500 NMS-E 4.2.1.R01 (MR2) Virtual Appliance.

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

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

```
*****
* Upgrade VA
*****
* [1] Help
* [2] 4.2.1.R01 (Current Release)
* [3] 4.2.2.R01 (New Release)
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
```

3. Enter 5 and press **Enter** to configure a Custom Repository. By default, the OV Virtual Appliance points to the ALE Central Repository. **However, to upgrade to OV4.2.2.R01 from OV4.2.1.R01 (MR2), you must configure a custom repository containing the latest OV4.2.2.R01 build.**

```
*****
* Configure Custom Repositories
*****
* [1] Help
* [2] "421PatchRepo" Repository
* [3] "Custom Repo 2" Repository
* [4] "Custom Repo 3" Repository
* [0] Exit
*****
(*) Type your option:
```

4. Select a Custom repository (e.g., 3 – “Custom Repo 2” Repository) and press **Enter**.

```

Current configuration
Repository Name:
Repository URL host:
Repository URL location:
Repository Full URL:

Please input Repository name [Custom Repo 2]: 422Repo
(*) Please input Repository URL host: ovrepo.fluentnetworking.com
Please input Repository URL location : ov/422R01Repo
Would you like to configure Repository with:
    Name: 422Repo
    URL host: ovrepo.fluentnetworking.com
    URL location: ov/422R01Repo
[yin] (y): _
    
```

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

- Repository Name – 422Repo
- Repository URL Host – ovrepo.fluentnetworking.com
- Repository URL Location – ov/422R01Repo

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] 4.2.1.R01 (Current Release)
* [3] 4.2.2.R01 (New Release)
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

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

```

*****
* Enable Repository
*****
* [1] Help
* [2] "ALE Central Repo" Repository (Selected)
* [3] "421PatchRepo" Repository
* [4] "422Repo" Repository
* [5] "Custom Repo 3" Repository
* [0] Exit
*****
(*) Type your option: _
    
```

7. Select the Custom Repository you just created (e.g., **4** – “422Repo” 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] "421PatchRepo" Repository
* [4] "422Repo" Repository (Selected)
* [5] "Custom Repo 3" Repository
* [0] Exit
*****
(*) Type your option: _
    
```

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

```

*****
* Upgrade VA
*****
* [1] Help
* [2] 4.2.1.R01 (Current Release)
* [3] 4.2.2.R01 (New Release)
* [4] Enable Repository (Selected - ALE Central Repo)
* [5] Configure Custom Repositories
* [6] Configure "Update Check Interval" (Selected - Disabled)
* [7] Backup/Restore OmniVista 2500 NMS Data
* [0] Exit
*****
(*) Type your option:
    
```

9. Enter **3** (4.2.2 (New Release)) and press **Enter** to begin the upgrade. Information on the current installation is displayed and OmniVista checks the Repository for the latest upgrade packages.

Note: 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).

You can only upgrade from the latest version of 4.2.1.R01 (MR2). If you are not running the latest version you will be prompted to install it as shown below. Enter **y** and press **Enter** to install the latest 4.2.1.R01 (MR2) software.

```

Current version of Virtual Appliance
Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.1.R01 MR-2
Build Number: 95
Patch Number: 1

Checking available packages for 4.2.2.R01 operation is in progress...
Upgrade to 4.2.2.R01 release is available after upgrading latest build of 4.2.1.R01 release
Do you want to continue check upgrade for 4.2.1.R01 release now [y/n] (n):
    
```

When the latest 4.2.1.R01 (MR2) software is installed, you will be prompted to install 4.2.2.R01, as shown below.

```

Installed:
  ovmnmsepatchb95.x86_64 0:4.2.1.R01-95.2.e17

Complete!

Getting upgrade information for 4.2.2.R01...
Upgrade information for 4.2.2.R01
Available Packages
Name       : ovmnmse
Arch      : x86_64
Version   : 4.2.2.R01
Release   : 80.0.e17
Size      : 964 M
Repo      : CustomRepo2_4.2.2.R01
Summary   : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E
URL       : http://enterprise.alcatel-lucent.com/?product=OmniVista2500NetworkManagementSystem&page=overview
License   : ALE USA Inc.
Description : Alcatel-Lucent Enterprise OmniVista 2500 NMS-E

You have selected to upgrade to latest build of 4.2.2.R01 release. Please refer to Release Notes and
Installation Guide of the new release before continuing with this upgrade
Do you want to continue with upgrade now [y/n] (n):
  
```

10. Enter **y** and press **Enter** to install OV 4.2.2.R01. You will be reminded to perform a backup before proceeding with the upgrade.

Note: The upgrade usually takes between 30 minutes to one hour to complete. But, it may take 3 - 4 hours based on network speed, OmniVista network size and OmniVista data size. When the upgrade is complete, a “Completion” message will appear and the VM will automatically reboot.

11. When the reboot is complete, log into the VM. You can verify the upgrade by going to the Virtual Appliance Menu and selecting option **2 – Configure the Virtual Appliance**, then selecting option **2 – Display the Current Configuration**.

12. Log into OmniVista and go to the License application to activate the Stellar AP License Starter Pack. This will enable you to manage 10 Stellar APs, 10 Guest Devices, and 10 BYOD Devices.

13. Go to **Administrator – License – Add/Import License**. Copy the license keys below and past them into **License Key** field, and click on the **Submit** button.

(Copy and paste **all 3 lines** below).

OV-AP-NM-10-N-F, V5ijCigh-K\$uHVmdv-j6XL2J7z-oB@\$7M#J-DC!GA87r-\$chkeSb%-tNqfrZ94-F9ogdTyz

OV-BYOD-10-N-F, z2fYJMsU-jnQuGT3m-zeX\$2J7z-oB@t7y#C-DC!GA87r-\$crkeHbL-pnQSTeHn-HtEWjs9e

OV-GA-10-N-F, nTdetTaE-dMFF1VQ3-neX\$2J7z-oB@t7y#C-DC!GA87r-\$c#keHbL-#9wqnc9a-ZfYCUj%y

Appendix A – Installing Virtual Box

If you are deploying OV 2500 NMS-E 4.2.2.R01 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/Download_Old_Builds_5_0_pre18. Scroll down to **Virtual Box 5.0.10** and click on the applicable download link (e.g., Windows Hosts, Linux 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 5.0.10 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_5.0.10_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 the 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`).

```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

Product Name: Alcatel-Lucent Enterprise OmniVista 2500 NMS 4.2.2.R01 GA
Build Number: 80
Patch Number: 0
Build Date: 08/04/2017
omnivista login: _
```

1. Enter the login (**cliadmin**) and press **Enter**.
2. Enter the password and press **Enter**. The password is the one you created when you first [launched the VM Console](#) at the beginning of the installation process. The Virtual Appliance Menu is displayed.

```
*****
* The Virtual Appliance Menu
*****
* [1] Help
* [2] Configure The Virtual Appliance
* [3] Run Watchdog Command
* [4] Upgrade/Backup/Restore VA
* [5] Change Password
* [6] Logging
* [7] Login Authentication Server
* [8] Power Off
* [9] Reboot
* [10] Advanced Mode
* [11] Set Up Optional Tools
* [0] Log Out
*****
```

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 - Configure NTP Client](#)
- [14 - Configure Proxy](#)
- [15 - Change Screen Resolution](#)
- [16 - Configure the Other Network Cards](#)
- [0 - Exit](#)

```
*****
* 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] Update OmniVista Web Server SSL certificate
* [13] Configure NTP Client
* [14] Configure Proxy
* [15] Change screen resolution
* [16] 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 4.2.2.R01 GA
Build Number: 80
Patch Number: 0
Build Date: 08/04/2017
LMA Version: 3.0.9.10
UPAM Version: 3.0.27.15

OV IPv4 Address: 10.255.221.19
NetMask: 255.255.255.0
OV Web HTTP Port: 80
OV Web HTTPS Port: 443

UPAM Portal IPv4 Address: 10.225.221.21
UPAM Portal Web HTTP Port: 80
UPAM Portal Web HTTPS Port: 443

Default Gateway v4:

Hostname: omnivista

Timezone: America/Los_Angeles

Data LUM Size: 256G
Data LUM Available (Free) Space: 234G

Network Size: Low (lower than 500) devices

Proxy Status: Disabled
Proxy is not set

Press [Enter] to continue
```

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.

```

*****
* Configure OV Ports
*****
Please input OV Web HTTP port [80]:
Please input OV Web HTTPS port [443]:
Would you like to configure:
    OV Web HTTP Port: 80
    OV Web HTTPS Port: 443
[yin] (y):
    
```

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.

```

*****
* Configure UPAM Portal IP & Ports
*****
* [1] Configure new IP & Ports
* [2] Disable UPAM Portal
* [0] Exit
*****
    
```

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

```

(*) Please input UPAM Portal IP: 10.225.221.21
Please input UPAM Portal HTTP port [80]: 80
Please input UPAM Portal HTTPS port [443]: 443
Would you like to configure:
    UPAM Portal IP: 10.225.221.21
    UPAM Portal HTTP port: 80
    UPAM Portal HTTPS port: 443
[yin] (y): y
The configuration has been set
Press [Enter] to continue
    
```

3. Enter an IPv4 IP address. Note that the UPAM Portal IP address **must** be different than the OV IP address.
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.

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

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**.

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

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 [yin] (n): y
(*) Please input dns server 1: 192.168.70.226
Would you like to use dns server 2 [yin] (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
[yin] (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 [yin] (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
 2) Cook Islands
 3) Ecuador
 4) Fiji
 5) French Polynesia
 6) Guam
 7) Kiribati
 8) Marshall Islands
 9) Micronesia
10) Nauru
11) New Caledonia
12) New Zealand
13) Niue
14) Norfolk Island
15) Northern Mariana Islands
16) Palau
17) Papua New Guinea
18) Pitcairn
19) Samoa (American)
20) Samoa (western)
21) Solomon Islands
22) Tokelau
23) Tonga
24) Tuvalu
25) United States
26) US minor outlying islands
27) Vanuatu
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 - Amette 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.

```
*****  
* Configure Route   
*****  
* [1] Help   
* [2] Show Current Routes   
* [3] Add Route v4   
* [4] Del Route v4   
* [0] Exit   
*****
```

3. Enter the subnet, netmask and gateway.
4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.

Configure Network Size

1. At the Main Menu prompt, enter **10** and press **Enter** to begin configuring a Network Size.

```
*****  
* Configure Network Size   
*****  
* [1] Help   
* [2] Configure OV2500 Memory   
* [3] Configure Swap File   
* [4] Extend Data Partition   
* [0] Exit   
*****
```

2. You can re-configure OV 2500 NMS-E 4.2.2.R01 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 4.2.2.R01 is partitioned as follows: HDD1:50GB and HDD2:256GB. If you are managing more than 500 devices it is recommended that you increase to provisioned hard disk using the Configure Network Size option in the Configure The Virtual Appliance Menu (Configure The Virtual Appliance Menu – Configure Network Size (10) - Configure Data Partition (4)).

Configure Keyboard Layout

1. Enter **11** and press **Enter** to specify a keyboard layout.

```
*****  
* Configure Keyboard Layout   
*****  
The available keyboard layouts will be shown (press [q] to exit view mode)  
Press [Enter] to continue
```

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

2. Press **Enter** to see the list of keyboard layouts.

3. Enter **q** and press **Enter** to quit the view mode. At the prompt, enter a keyboard layout then press **Enter**. Enter **y** at the confirmation prompt and press **Enter**.

```
Please input keyboard layout [us]:
Would you like to set:
    keyboard layout: us
[y;n] (y): _
```

The table below lists all supported keyboard layouts.

amiga-de	amiga-us	atari-uk-falcon	atari-se
atari-us	atari-de	pt-olpc	es-olpc
sg-latin1	hu	sg	fr_CH
de-latin1-nodeadkeys	fr_CH-latin1	de-latin1	de_CH-latin1
cz-us-qwertz	sg-latin1-lk450	croat	slovene
sk-prog-qwertz	sk-qwertz	de	cz
wangbe	wangbe2	fr-latin9	fr-old
azerty	fr	fr-pc	be-latin1
fr-latin0	fr-latin1	tr_f-latin5	trf-fgGlod
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):

```

Configure NTP Client

1. Enter **13** and press **Enter** to configure an NTP Server.

```
*****  
* Configure NTP Client   
*****  
* [1] Help  
* [2] Configure NTP Server IP  
* [3] Status NTP Client  
* [4] Disable NTP Client  
* [5] Enable NTP Client  
* [0] Exit  
*****
```

2. Enter **2** and press **Enter**.

3. Enter the IP address of the NTP Server and press **Enter**.

4. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu. You can enable the server when you create it, or enable it at a later time using option **5**.

Configure Proxy

OV 2500 NMS-E 4.2.2.R01 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 4.2.2.R01 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 4.2.2.R01 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 **14** and press **Enter** to specify whether the VM will use a Proxy Server. Enter **2** and press **Enter** to configure a Proxy Server.

```
*****  
* Configure Proxy   
*****  
* [1] Help  
* [2] Setup Proxy  
* [3] Enable/Disable Proxy  
* [0] Exit  
*****
```

2. If the VM will use a proxy server, enter the Proxy Server IP address, along with the port (e.g., 8080).

```
Proxy is not set
(*) Please input proxy IP: 10.255.10.80
(*) Please input proxy port: 8080
Please input proxy username :

Would you like to configure proxy with:
    IP: 10.255.10.80
    Port: 8080
    Username:
    Password:
[y;n] (y):
```

15

Note: If **n** (No) is selected, all proxy servers will be disabled.

3. Enter **y** and press **Enter** to confirm the settings. Press **Enter** to return to the Configure The Virtual Appliance Menu.
4. Enter **3** and press **Enter** to enable the Proxy.

Change Screen Resolution

1. Enter **15** and press **Enter** to configure the VA screen resolution.

```
*****
* Change screen resolution
*****
* [1] 800x600
* [2] 1024x768
* [3] 1280x1024
* [0] Exit
*****
```

2. Select a screen resolution and press **Enter**. Enter **y** and press **Enter** at the confirmation prompt. You will be prompted to restart the VA for the settings to take effect.
3. Enter **y** and press **Enter** at the confirmation prompt to restart the VA.

Configure the Other Network Cards

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

```
*****
* 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.

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 4.2.2.R01. 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.

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

To view information about the currently-installed version of the OV 2500 NMS-E 4.2.2.R01 VA, and to update the VM, enter **4** at the command prompt. The following options are available:

- **4.2.2R01 (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. Also note that if a new version is available (e.g., R01 to R02), and you 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.
- **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-yyy-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 4.2.2.R01 configuration using a 4.2.2.R01 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 4.2.2.R01 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.

```
*****
* Change Password
*****
* [1] Help
* [2] Change "cliadmin" Password
* [3] Change Mongo Database Password
* [4] Change Root Password
* [5] Change FTP server Password
* [0] Exit
*****
```

To change the VA cliadmin password, enter **2**, then press **Enter**. At the prompts, enter the current password, then enter the new password.

To change the mongo database password, enter **3**, then press **Enter**. You have two options when changing the mongo database password.

```
(*) Type your option: 3
You must remember the new passwords in order to manage the MongoDB.
Press [Enter] to continue

Would you like to change password for
  [1] Mongo administrator
  [2] Ngnms application user
Provide your option [1 OR 2]:
```

Enter **1** to change the mongo administrator password. Enter **2** to change the application user password. At the prompts, enter the current password, then enter the new password.

To change the 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 4.2.2.R01 Logs using the “Logging” option. Enter **6**, then press **Enter**.

```
*****
* Configure Logging
*****
* [1] Help
* [2] Change Log Level
* [3] Collect Log Files
* [4] Collect JVM Information
* [0] Exit
*****
```

The following options are available:

- **Change Log Level** - Changes the logging level for OV services. Enter the number corresponding to the OV service for which you want to change the logging level (e.g. 13 - ovsip) and press **Enter**. Enter the number corresponding to the package for which you want to change the logging level (e.g. 1 - com.alu.ov.ngms.sip.service) and press **Enter**. Enter the number corresponding to the log level you want to set (e.g., 2 - DEBUG) and press **Enter**.
- **Collect Log Files** - Collects all log files from a specific date to the current date. Enter the date from which you want to collect log files in dd-MM-yyyy format (e.g., 10-15-2016) 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-15-10-2016_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-02016-10-15-12-08-43.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 4.2.2.R01 Login Authentication Server.

```

*****
* Login Authentication Server
*****
* [1] Help
* [2] Current Login Authentication Server
* [3] Change Login Authentication Server to local
* [0] Exit
*****
    
```

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.R01 services using the **Stop All Services** option in the **Run Watchdog Command**. After all the services are stopped, enter **8** at the command line to power off the VM. Confirm the power is off by entering **y**. The power off may take several minutes to complete.

Note: OV 2500 NMS-E 4.2.2.R01 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 4.2.2.R01 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 4.2.2.R01 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.

```
*****  
* Optional Tool Of Supervisors Menu  
*****  
* [1] Help  
* [2] VMWare Tools  
* [3] VirtualBox Guest Additions  
* [4] Hyper-V Linux Integration Services  
* [0] Exit  
*****
```

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

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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" message 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 4.2.2.R01 functions continue following logout.

Appendix C – 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.

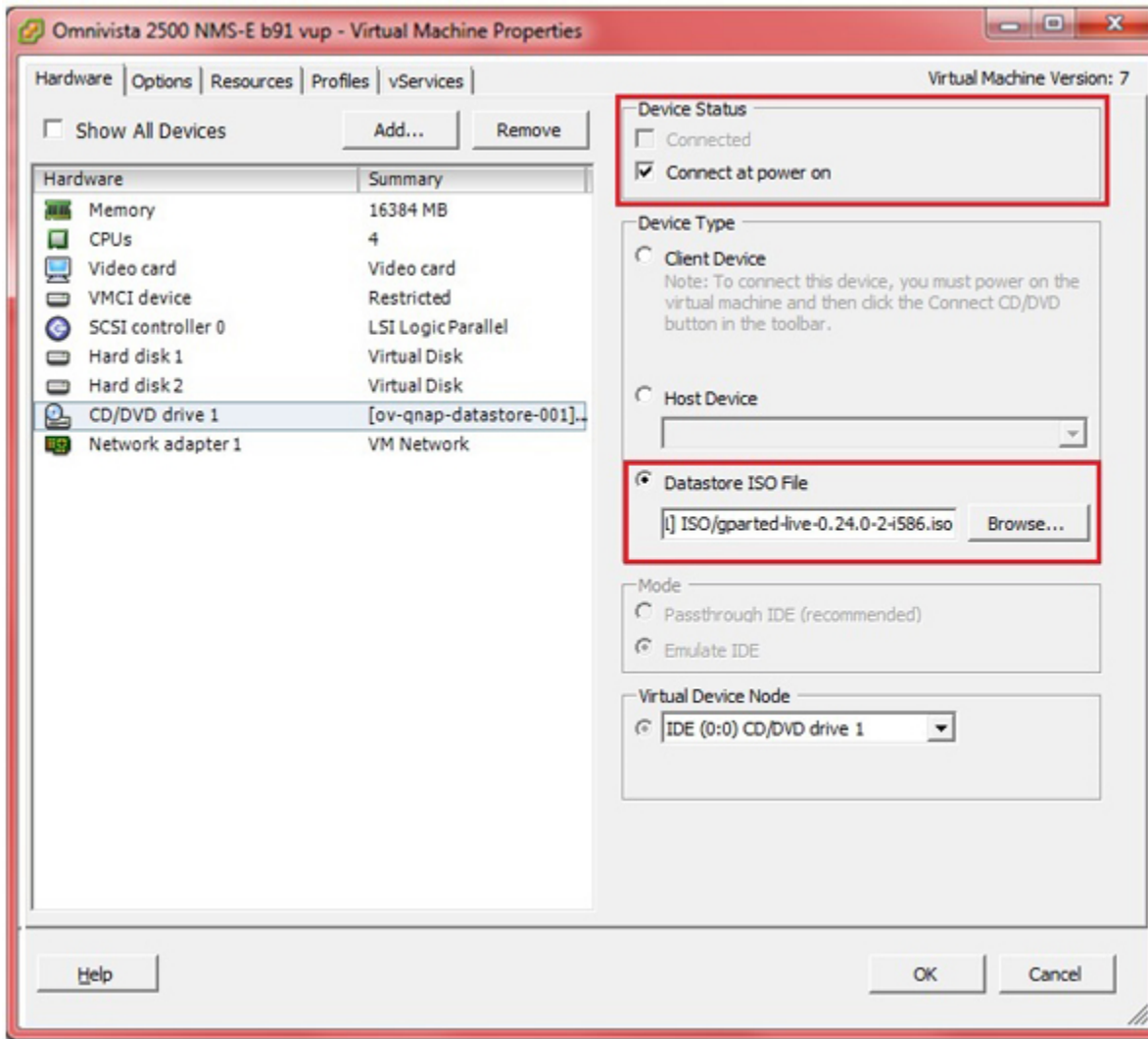
```

*****
* The Virtual Appliance Menu
*****
* [1] Help
* [2] Configure The Virtual Appliance
* [3] Run Watchdog Command
* [4] Upgrade/Backup/Restore VA
* [5] Change Password
* [6] Logging
* [7] Login Authentication Server
* [8] Power Off
* [9] Reboot
* [10] Advanced Mode
* [11] Set Up Optional Tools
* [0] Log Out
*****

```

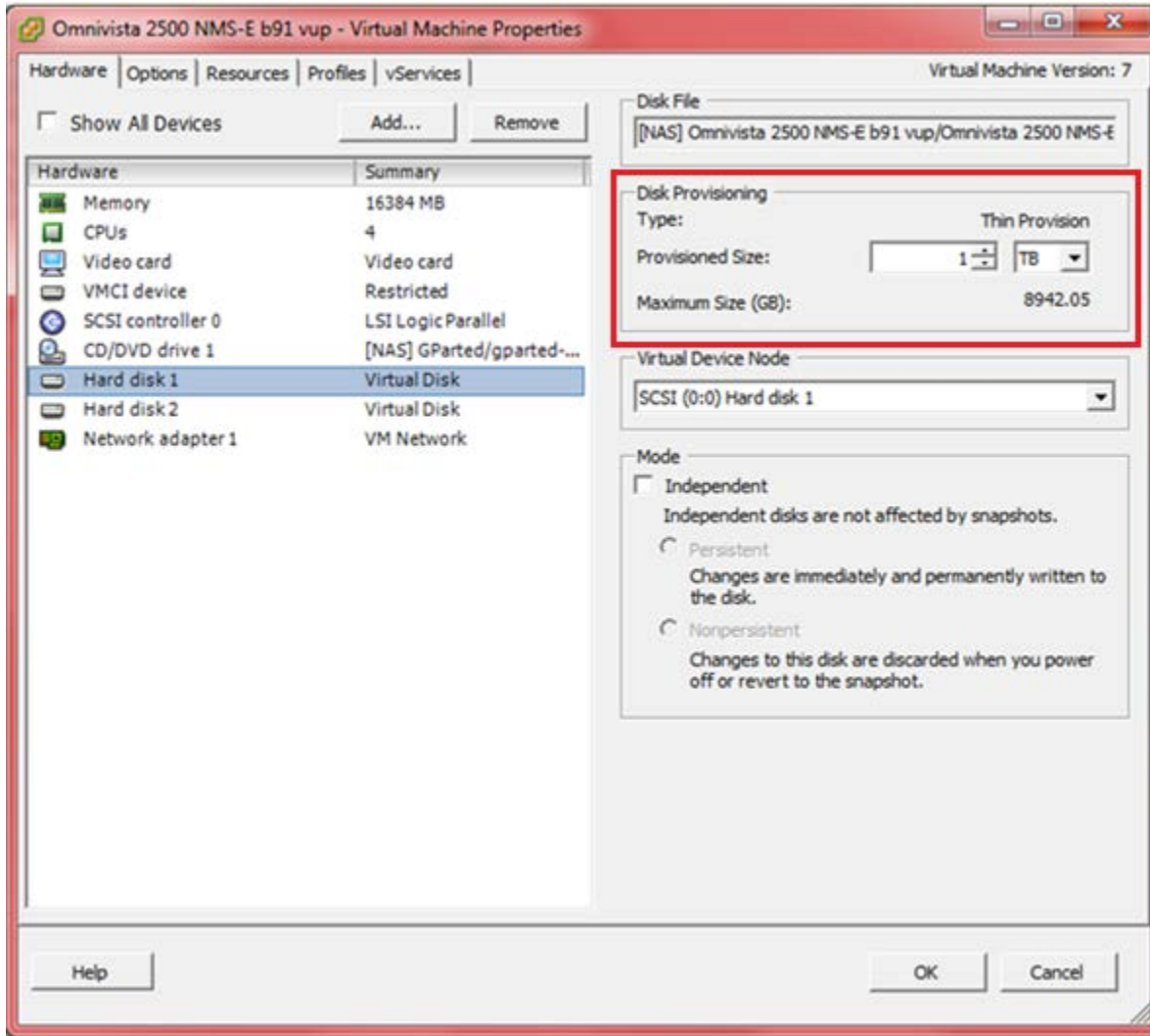

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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).



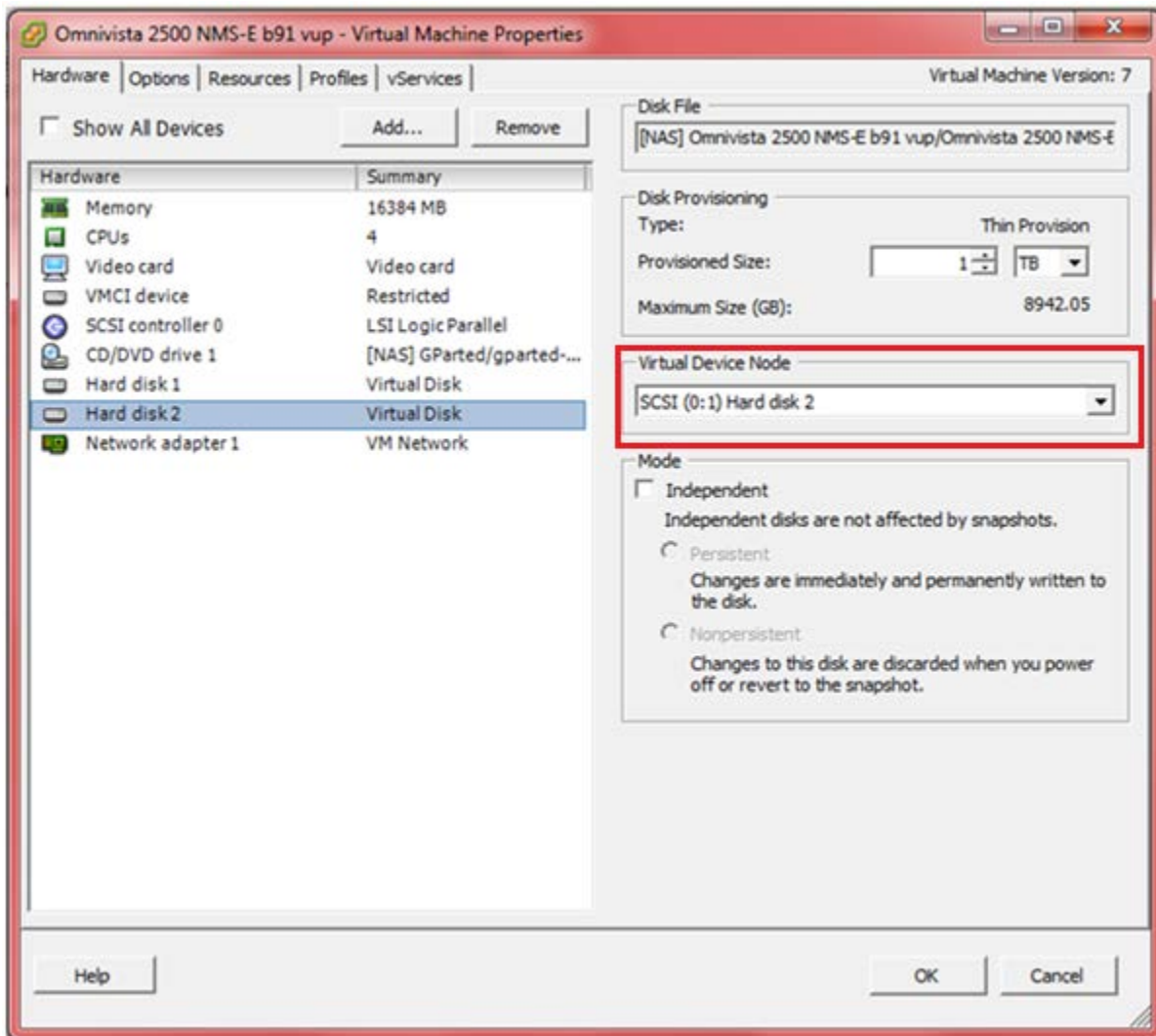
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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**.



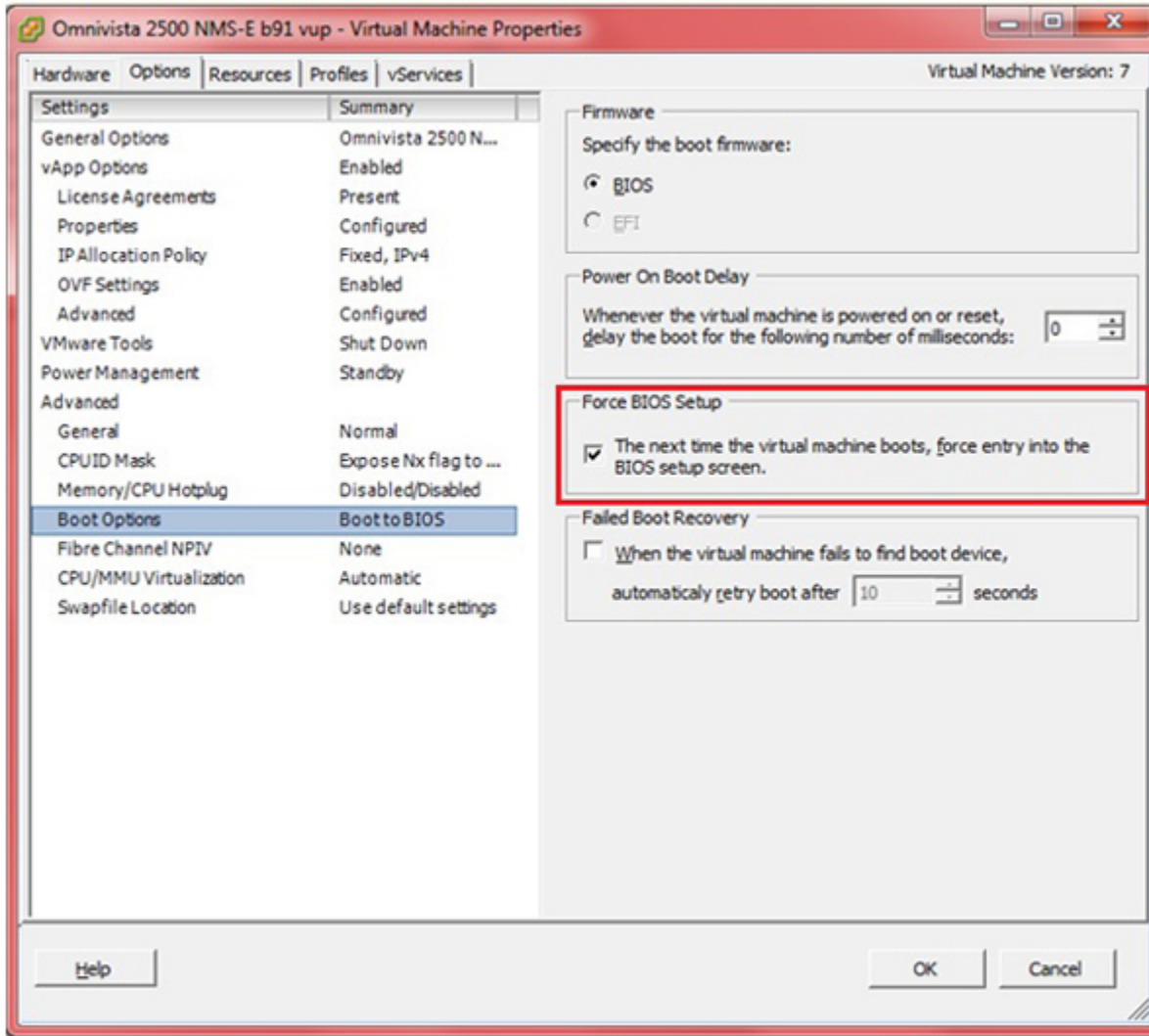
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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.

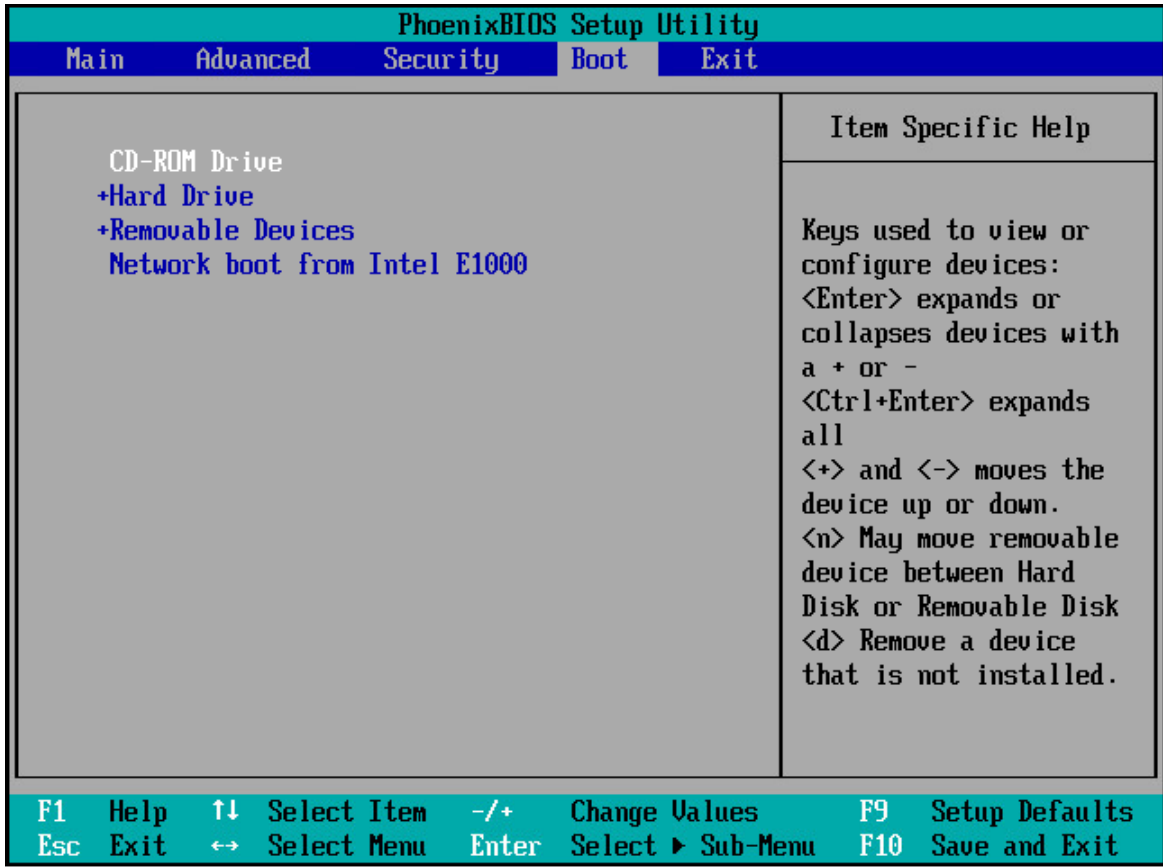


OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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**.

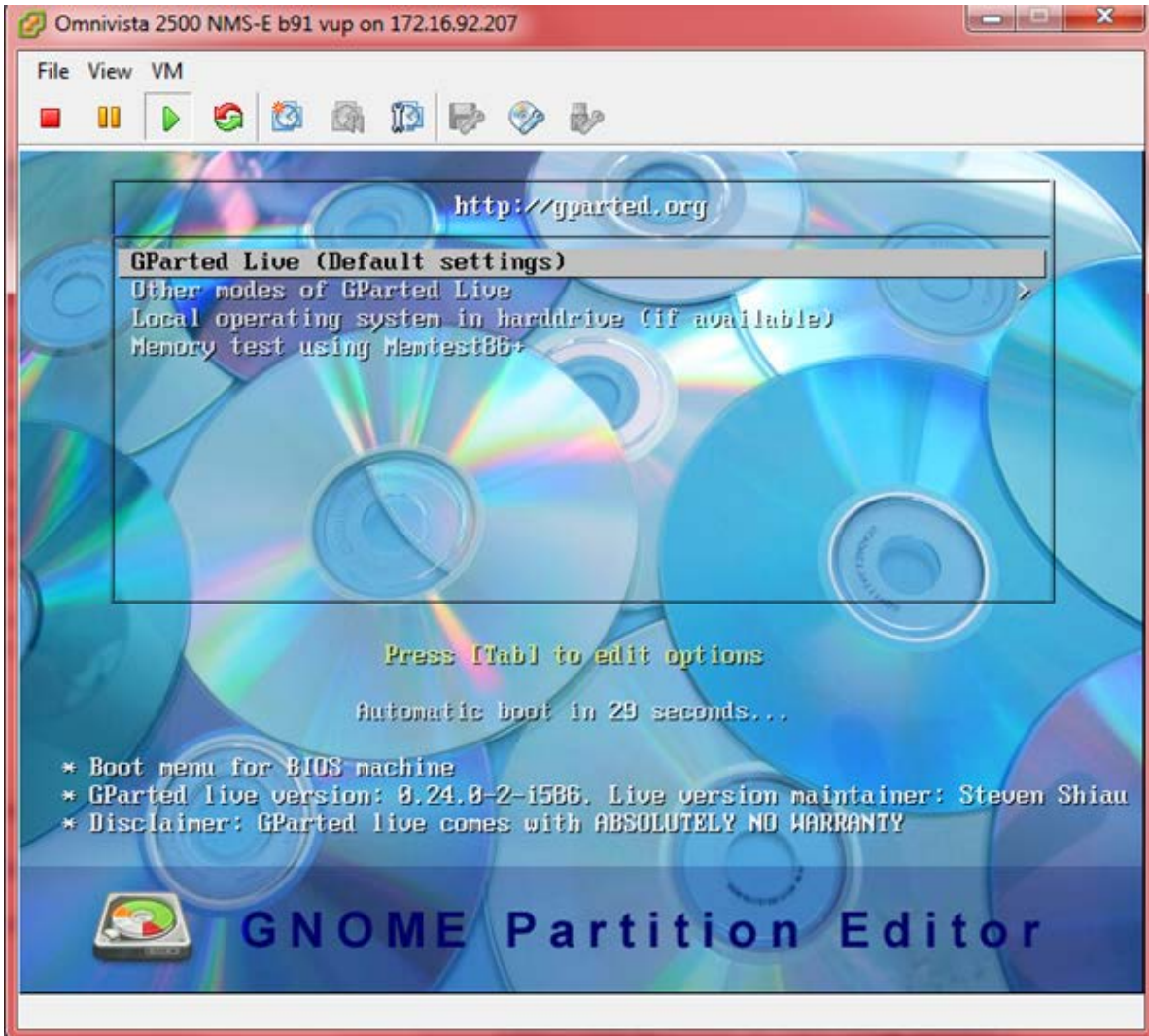


Step 5: Start the VA. Change the boot order to boot from the CD-ROM Drive. Go to the Boot tab and use the +/- keys to move the CD-ROM Drive to the top of the list. Press **F10** and select **Yes** at the confirmation prompt to save and exit.

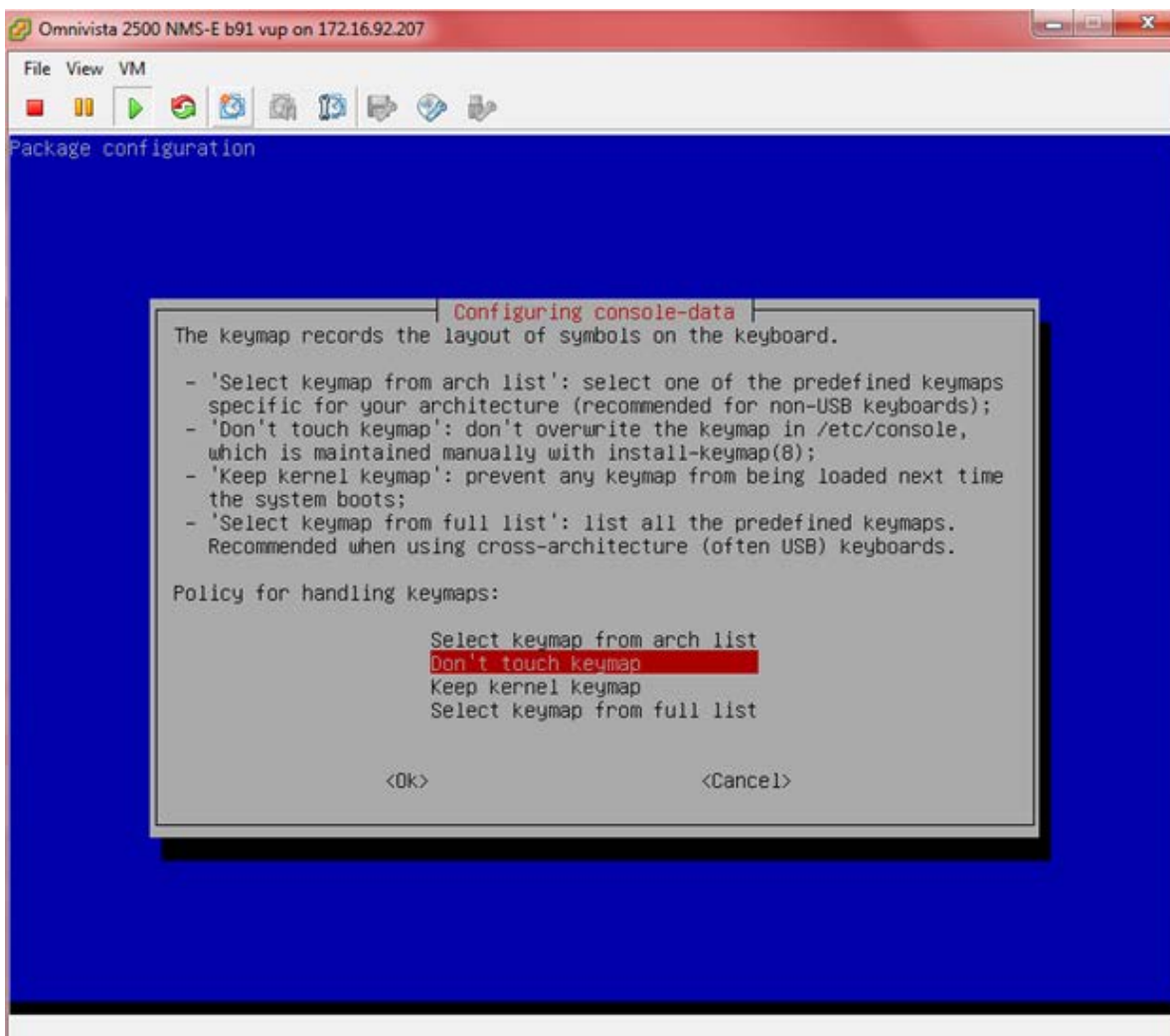


Step 6: Boot the VA from the GParted Live CD.

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

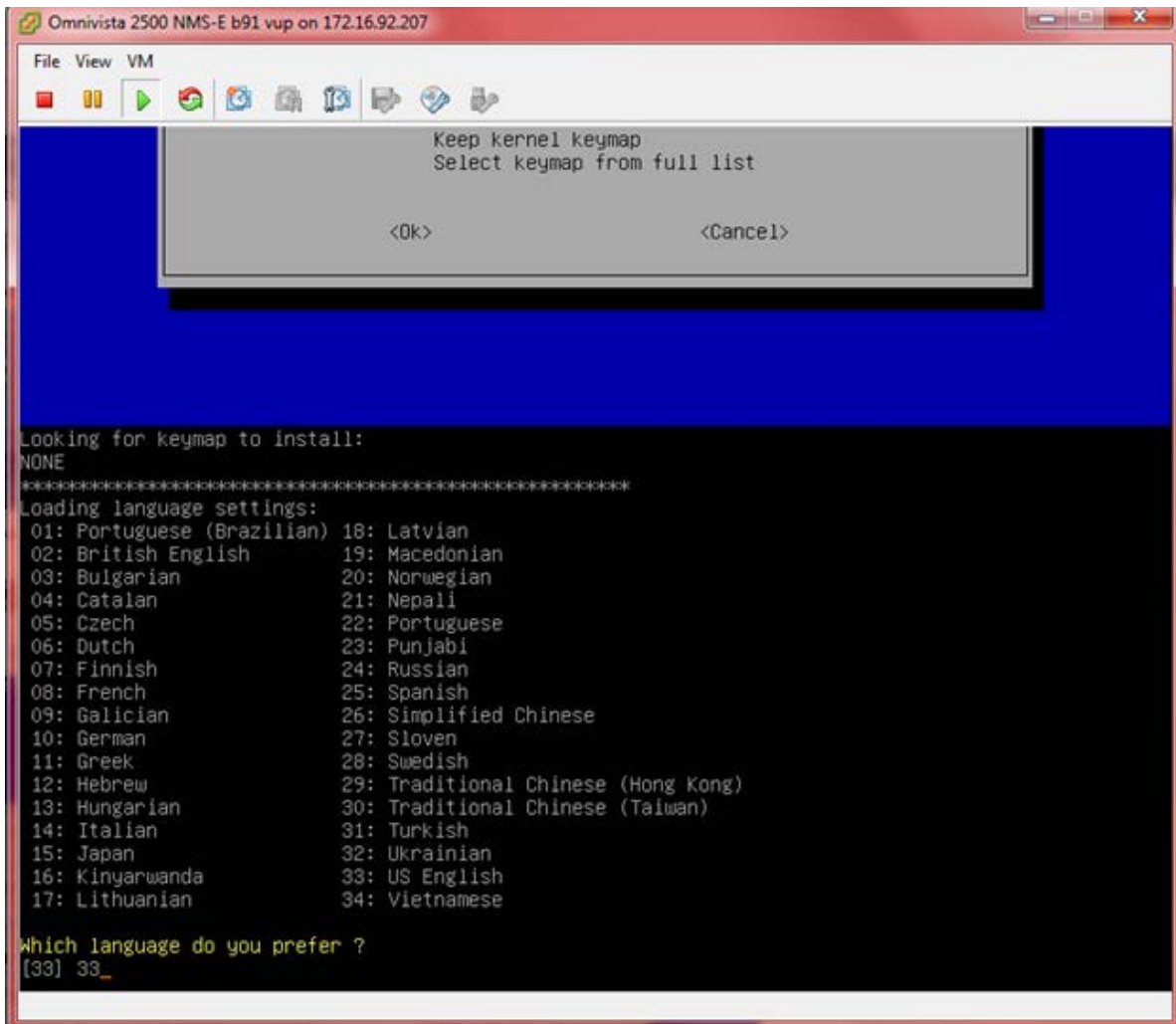


Select Don't Touch Keymap

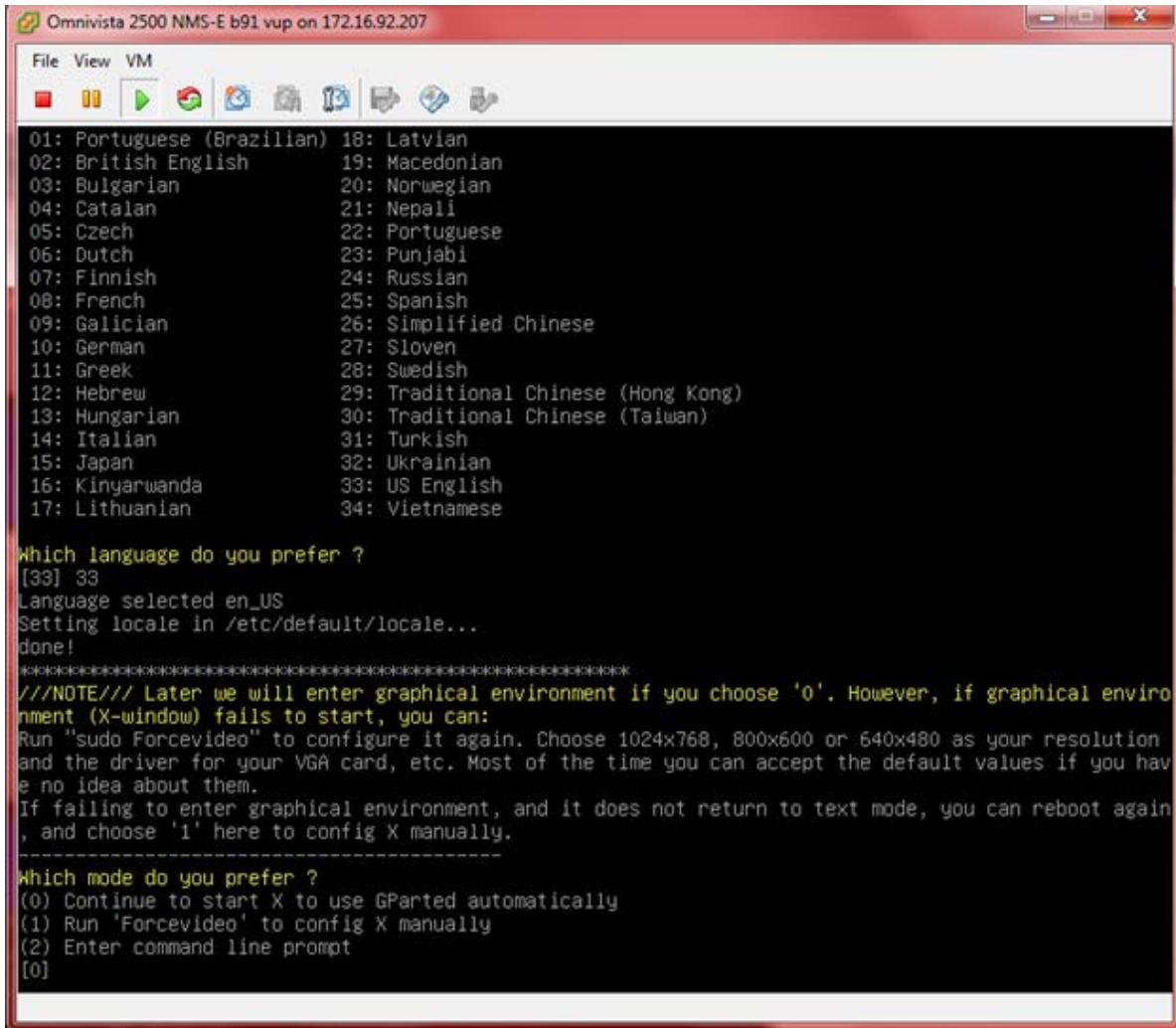


OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

Select the preferred language.

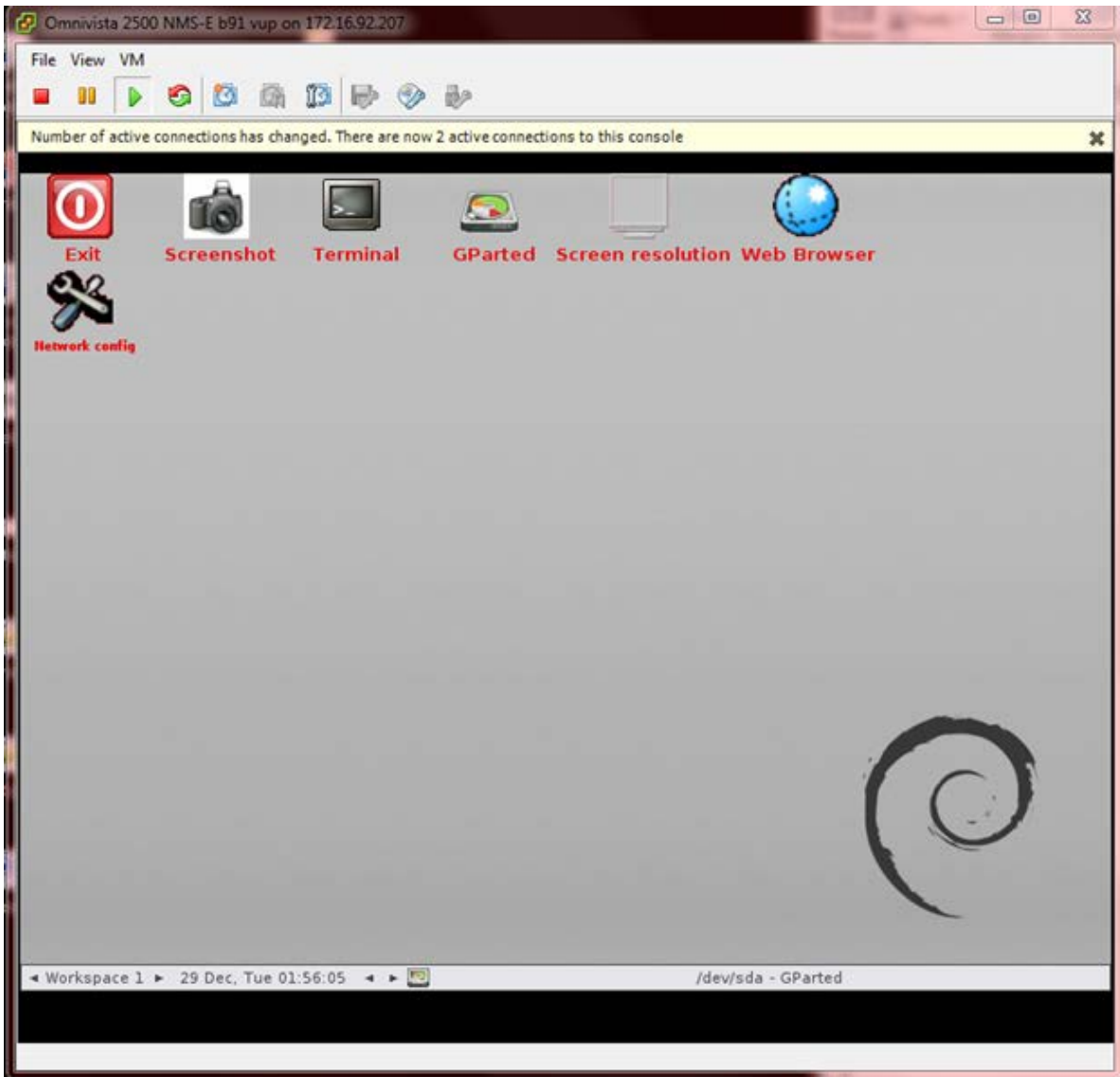


Select **(0)** Continue to start X to use GParted automatically.



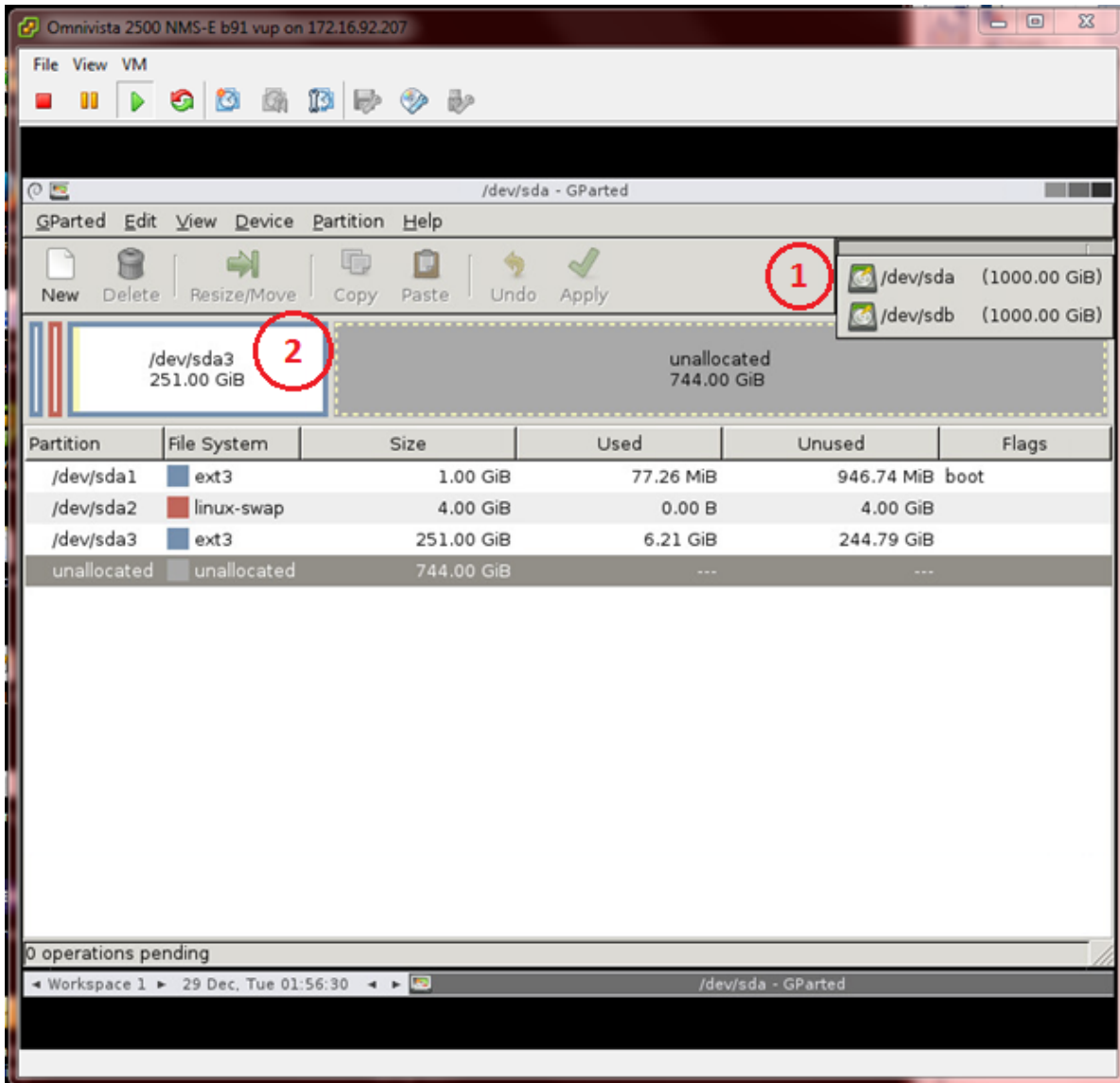
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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



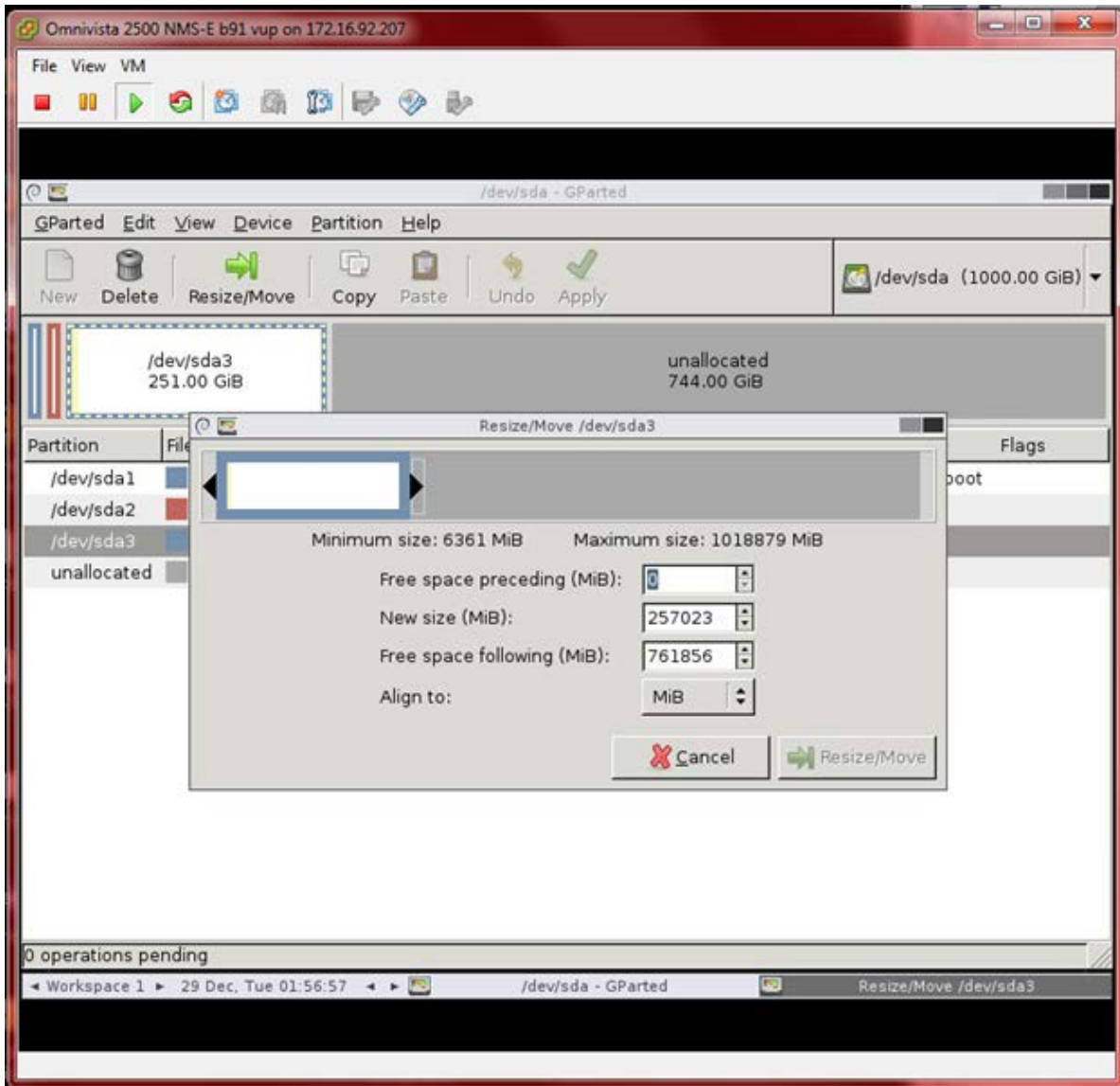
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

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

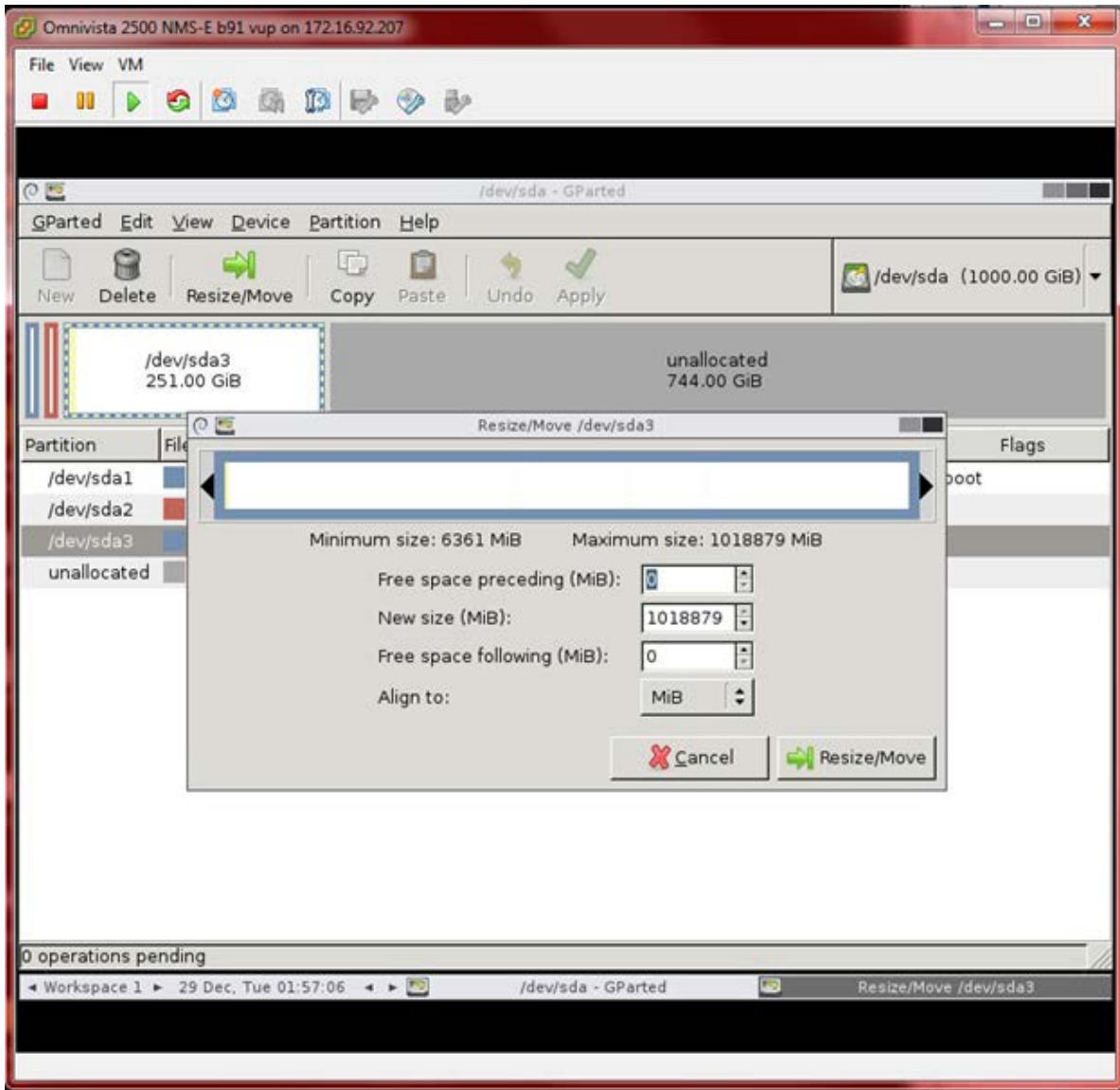


Use the UI menu to change the partition size. Or use the input menu below to enter the size for the partition. When complete, click on the **Resize/Move** button.

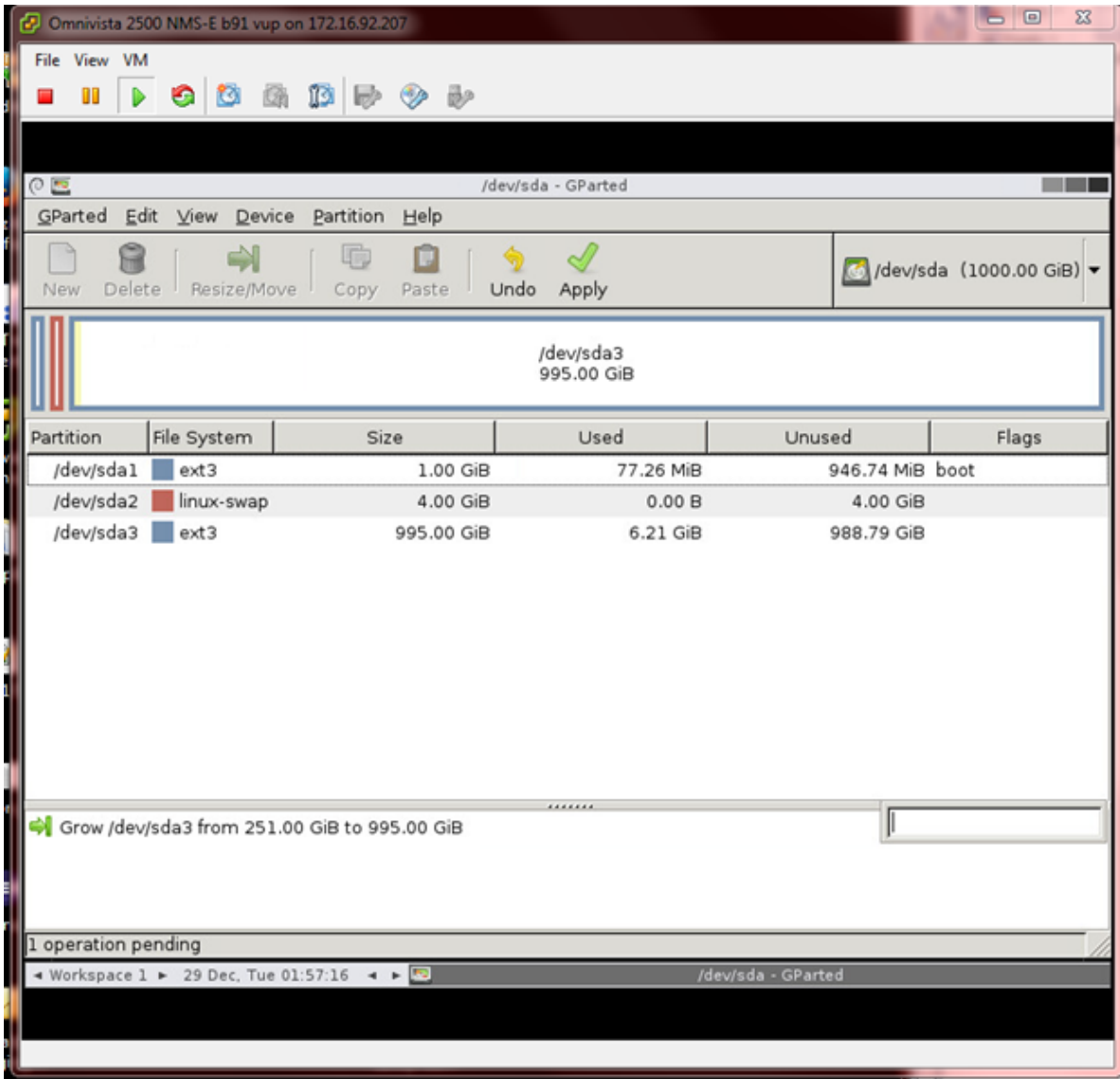
Before



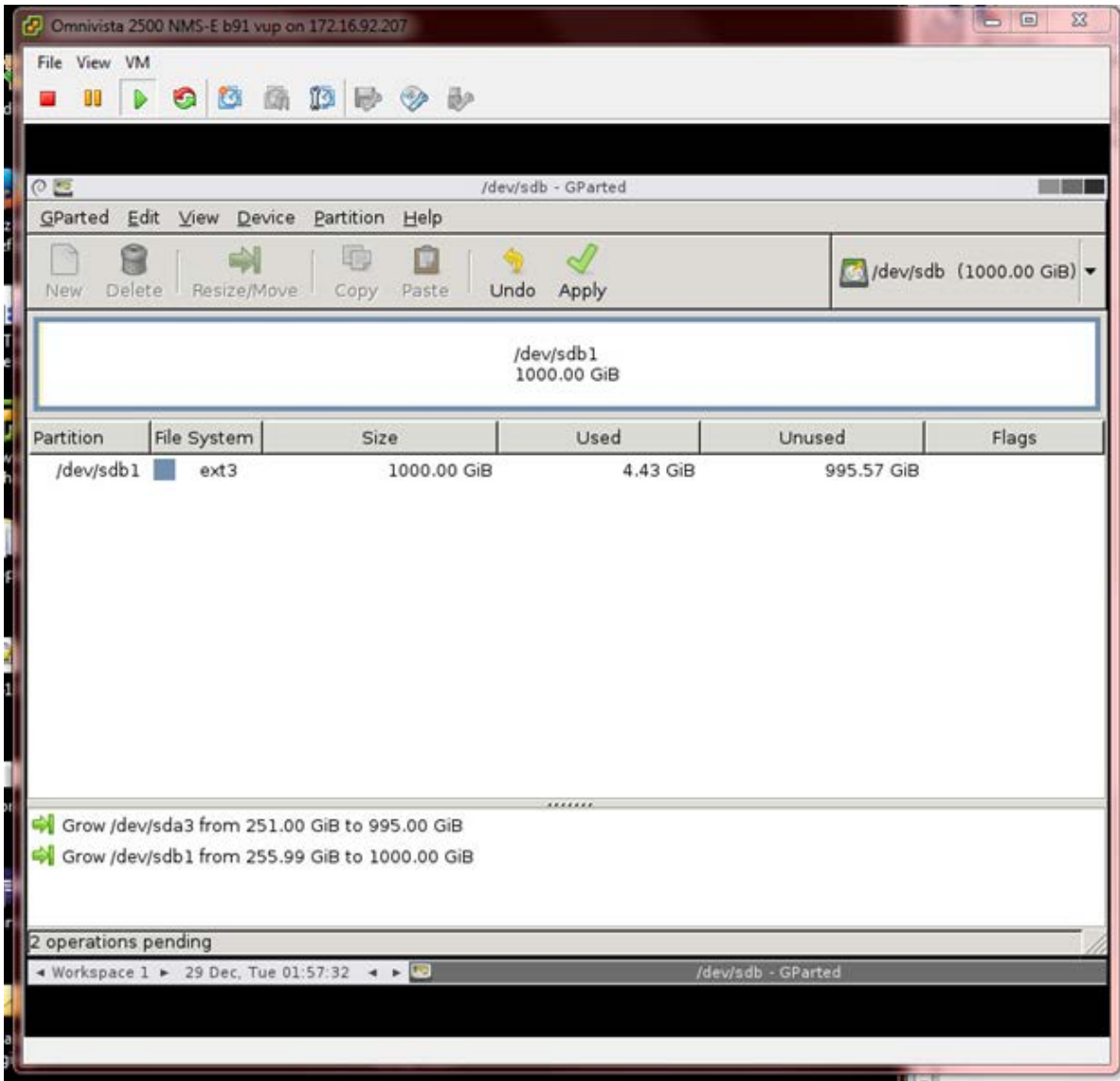
After



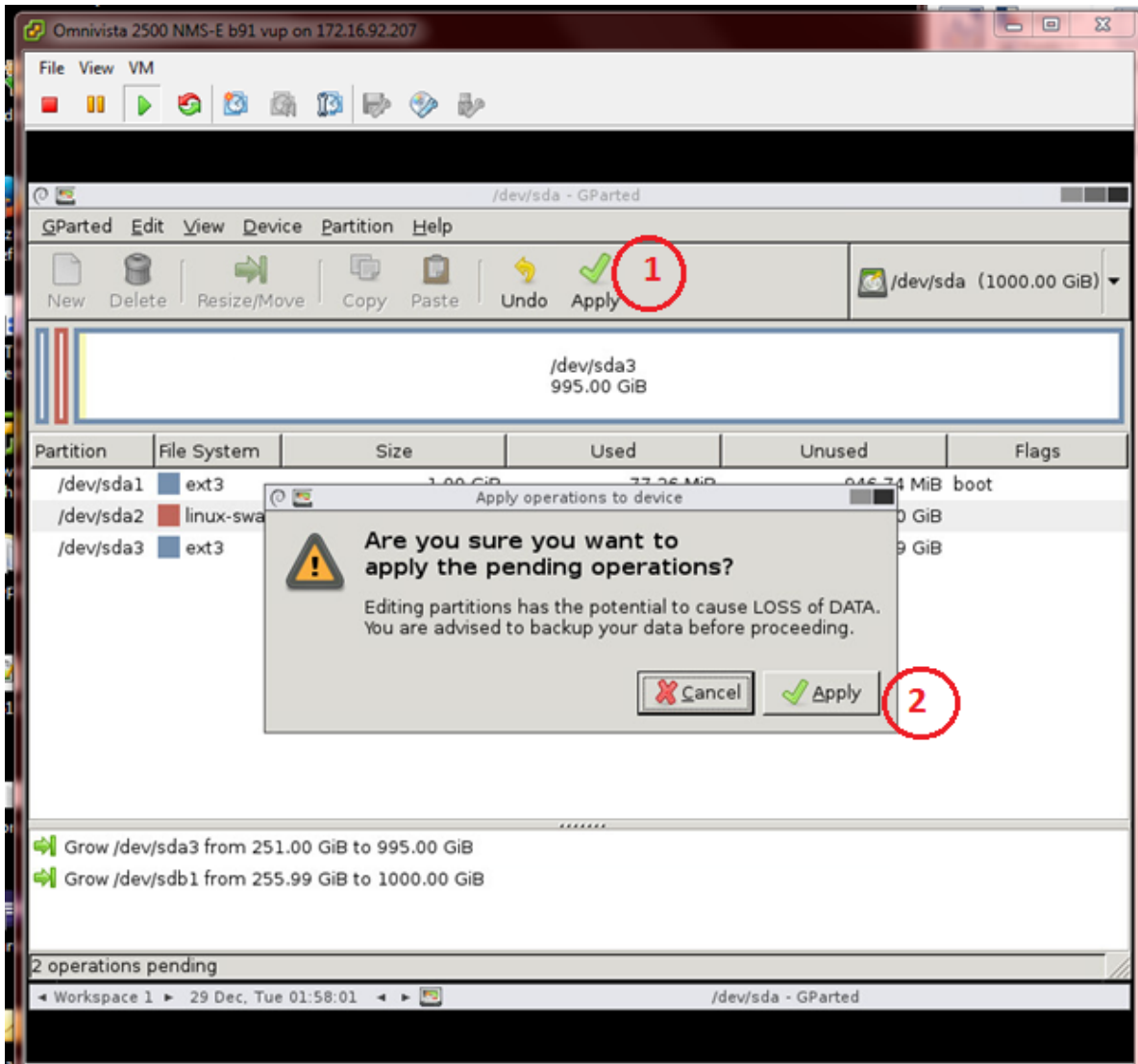
OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



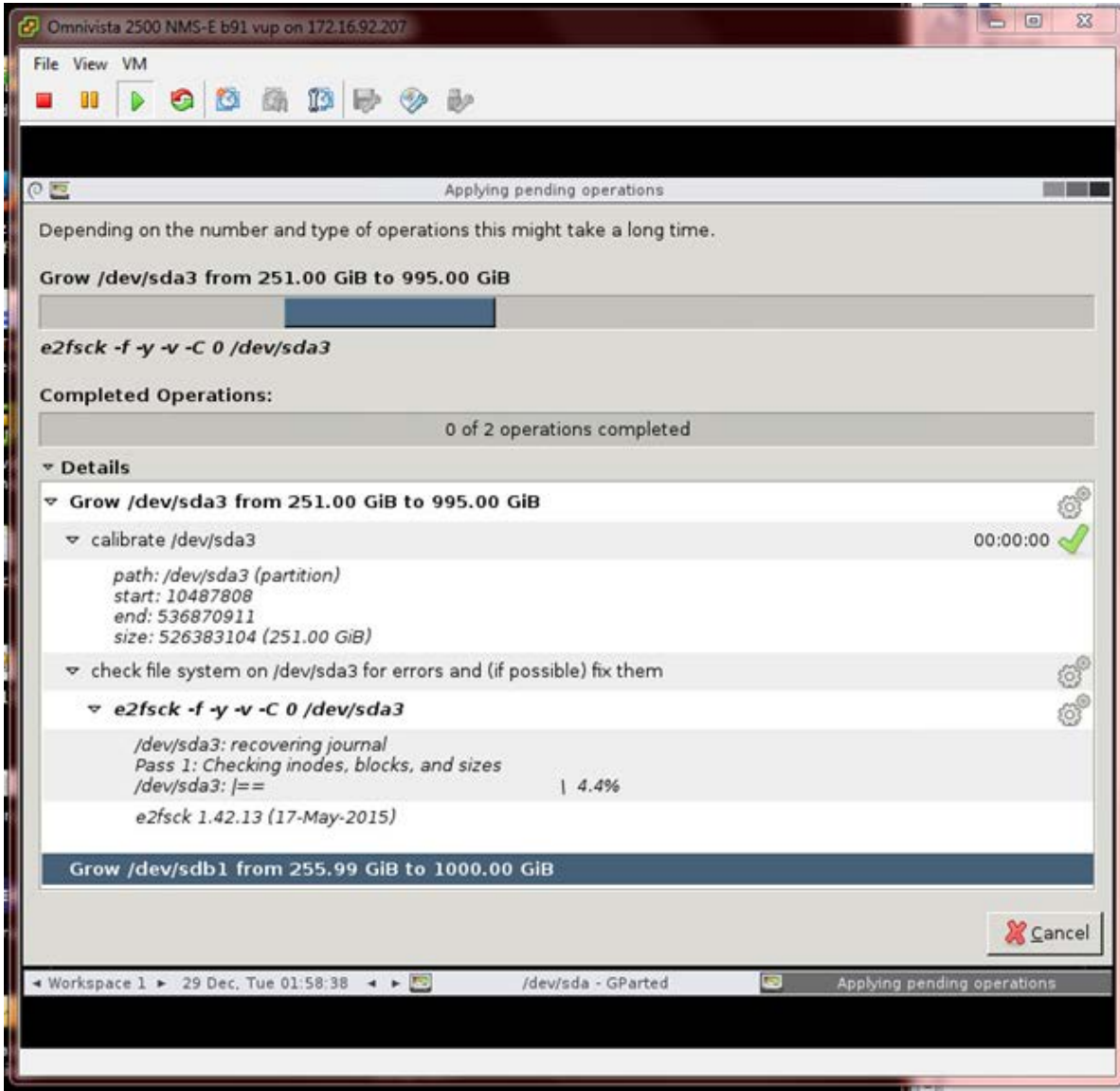
Step 9: Extend the disk size for /dev/sdb and /dev/sdb1.



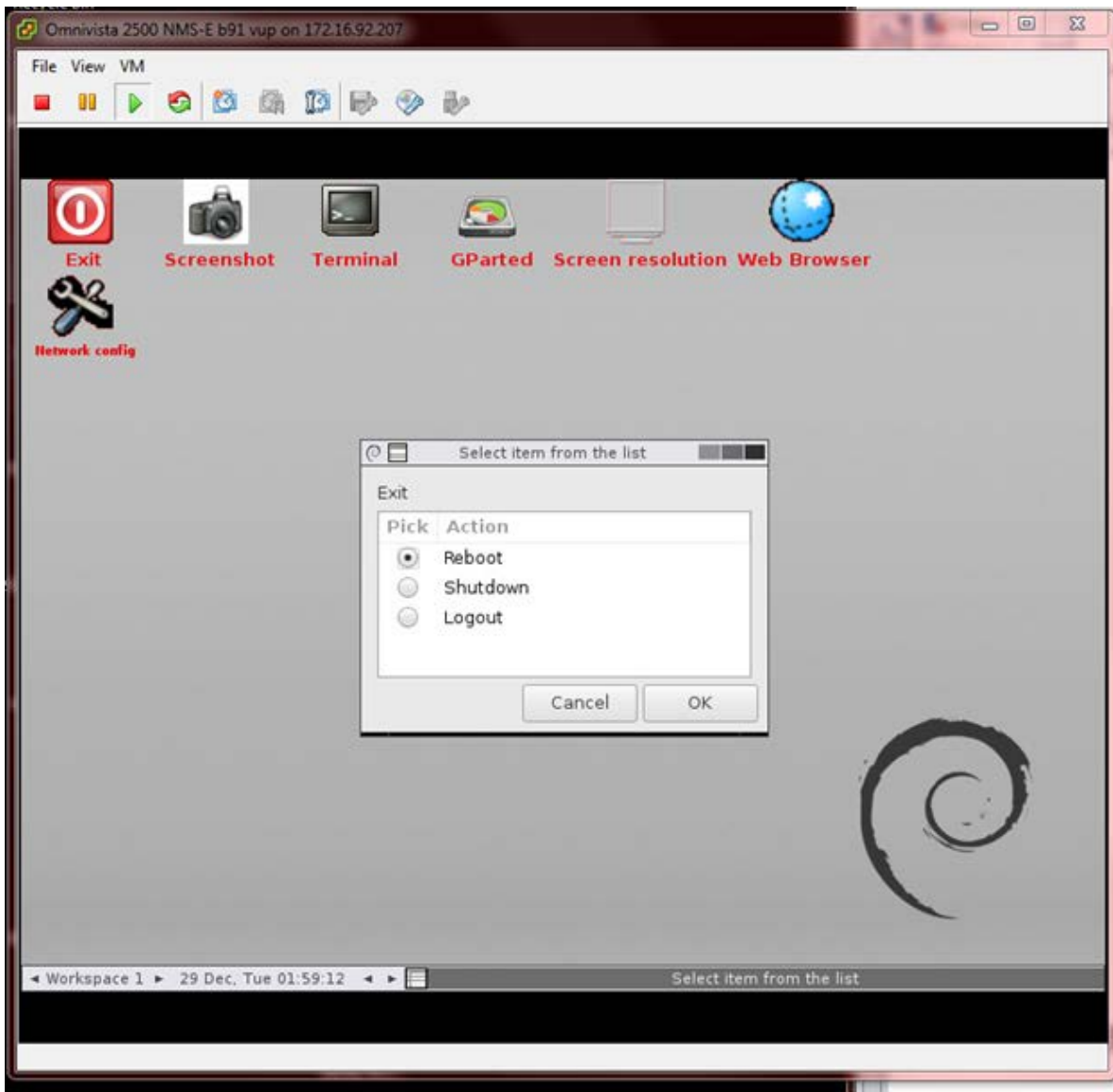
Step 10: Select **Apply** and confirm.



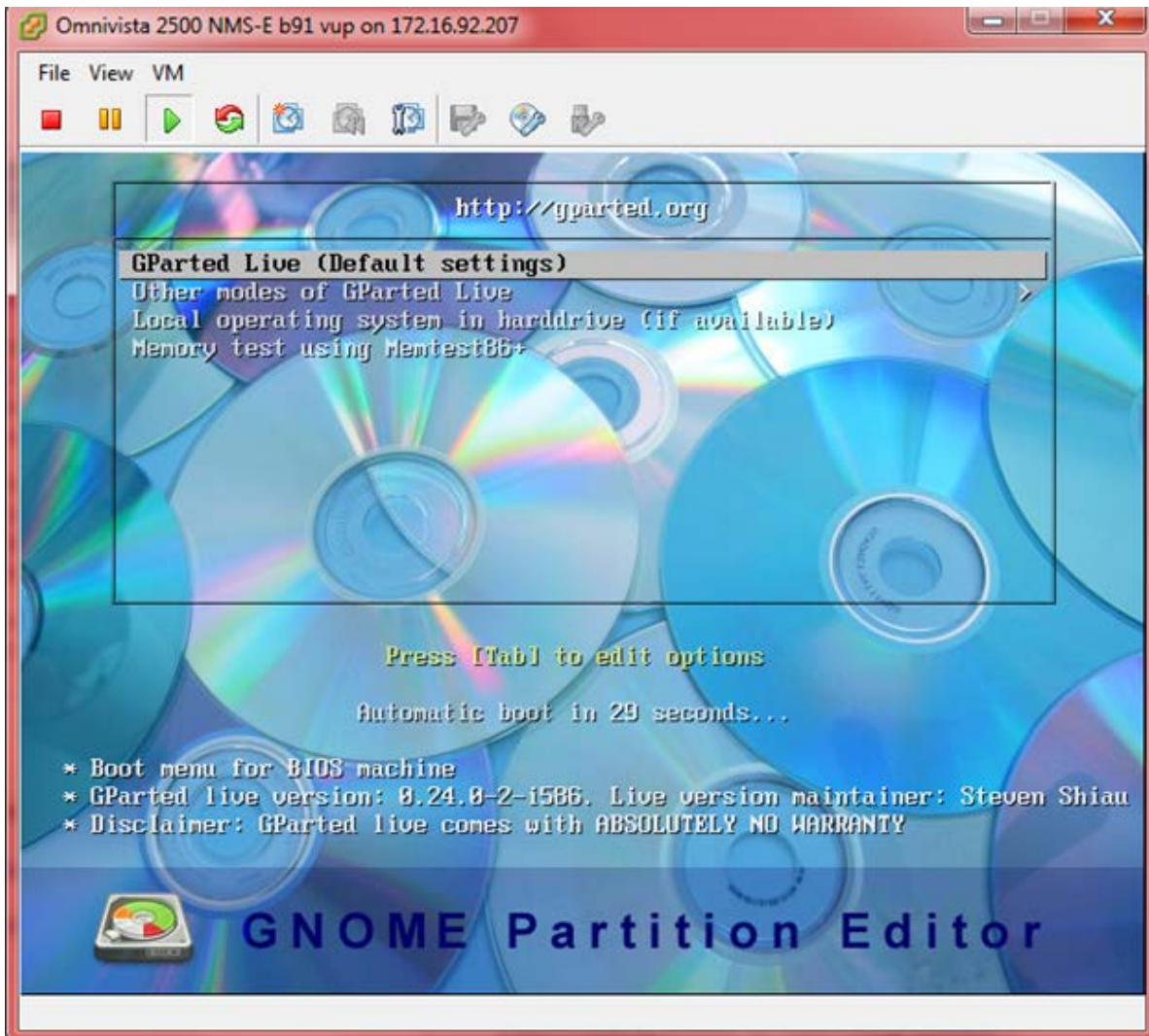
Step 11: Wait for the process to finish, then reboot the VA.



OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide



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 D – Generating an Evaluation License

An Evaluation License provides full OV 2500 NMS-E 4.2.2.R01 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.

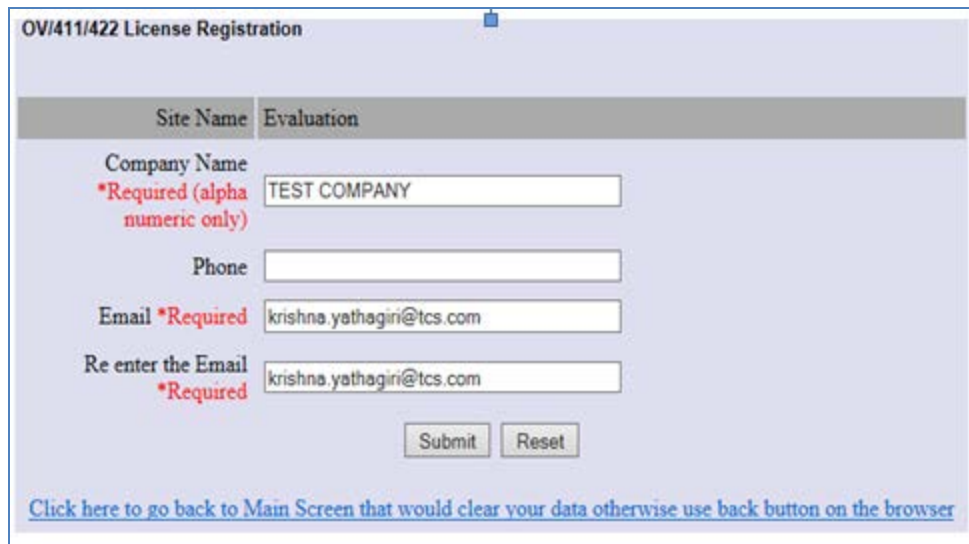
1. Go to <https://support.esd.alcatel-lucent.com/ov25411/enterLicenseData.jsp>.

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.

OmniVista 2500 NMS Enterprise 4.2.2.R01 Installation and Upgrade Guide

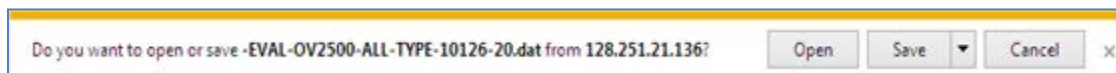


The screenshot shows a web browser window titled "OV/411/422 License Registration". The form contains the following fields and labels:

Site Name	Evaluation
Company Name *Required (alpha numeric only)	TEST COMPANY
Phone	
Email *Required	krishna.yathagiri@tcs.com
Re enter the Email *Required	krishna.yathagiri@tcs.com

At the bottom of the form are two buttons: "Submit" and "Reset". Below the form is a blue hyperlink: [Click here to go back to Main Screen that would clear your data otherwise use back button on the browser](#).

5. Complete all of the required fields on the License Registration Form and click **Submit**. A download prompt (shown below) will appear.



6. Click **Save** at the confirmation prompt to download the license to your computer.

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